KPMG

MeghEA- Detailed Architecture Requirements

Whole of Government

Government of Meghalaya
Planning Department

August 2021

KPMG.com/in

Disclaimer and Notice to Reader

The information contained herein is of a general nature and not intended to address the circumstances of any particular individual or entity. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

We have prepared this report solely for providing select information on a confidential basis to the management of the Planning Department, Government of Meghalaya in accordance with the agreement dated 4 September 2019 executed between Planning Department, Government of Meghalaya and KPMG Advisory Services Private Limited. The document has been prepared with contributions and inputs from National e-Governance Division (NeGD), State Departments and National Informatics Center (NIC) Meghalaya Unit.

This report is confidential and for the use of management only. The distribution of this report should be limited to concerned and appropriate officials of the Planning Department, Government of Meghalaya on need basis only.

This report sets forth our views based on the completeness and accuracy of the facts stated to KPMG Advisory Services Private Limited and any assumptions that were included. If any of the facts and assumptions is not complete or accurate, it is imperative that we be informed accordingly, as the inaccuracy or incompleteness thereof could have a material effect on our conclusions. We have not performed an audit and do not express an opinion or any other form of assurance.

While performing the work, we assumed the genuineness of all signatures and the authenticity of all original documents. We have not verified the correctness or authenticity of the same. While the information obtained from the public domain or external sources not verified for authenticity, accuracy or completeness, we have obtained information, as far as possible, from sources generally considered reliable. We assume no responsibility for such information.

Our views are not binding on any person, entity, authority or court, and hence, no assurance is given that a position contrary to the opinions expressed herein not asserted by any person, entity, authority and/or sustained by an appellate authority or a court of law.

In accordance with its policy, KPMG Advisory Services Private Limited advises that neither it nor any partner, director or employee undertakes any responsibility arising in any way whatsoever, to any person other than Planning Department, Government of Meghalaya in respect of the matters dealt with in this report, including any errors or omissions therein, arising through negligence or otherwise, howsoever caused.

In connection with our report or any part thereof, KPMG Advisory Services Private Limited does not owe duty of care (whether in contract or in tort or under statute or otherwise) to any person or party to whom the report is circulated to and KPMG Advisory Services Private Limited shall not be liable to any party who uses or relies on this report. KPMG Advisory Services Private Limited thus disclaims all responsibility or liability for any costs, damages, losses, liabilities, expenses incurred by such third party arising out of or in connection with the report or any part thereof.

By reading our report, the reader will be deemed to have accepted the terms mentioned hereinabove.

Document Control

Revision History

Version	Author	Date	Revision Remark
0.1	Titash, Ramandeep, Aurobind	07-05-2020	First version submitted for review
1.0	Titash, Ramandeep, Aurobind	12-05-2020	Review comments incorporated
1.1	Titash, Ramandeep, Aurobind	04-06-2020	Review comments incorporated
2.0	Titash, Ramandeep, Aurobind	11-06-2020	Review comments incorporated
2.1	Titash	23-06-2020	Review comments incorporated
3.0	Titash	30-06-2020	Review comments incorporated
4.0	Titash	15-01-2021	Modifications basis changes in other pillars
4.1	KPMG Team	02-06-2021	Modifications basis changes in other pillars post department reviews
5.0	KPMG Team	02-08-2021	Review comments incorporated

Review History

SL No.	Reviewer	Date Reviewed	Comments
0.1	Prasad Unnikrishnan	08-05-2020	Review comments provided
1.0	Dr. Pallab Saha	15 & 20-05-2020	Review comments provided
1.0	NeGD	20-05-2020	Review comments provided
1.0	NIC	20-05-2020	Review comments provided
1.1	Prasad Unnikrishnan	07-06-2020	Review comments provided
2.0	Dr. Pallab Saha	12-06-2020	Review comments provided
2.1	Prasad, Ramandeep	24-06-2020	Review comments provided
4.1	NeGD, NIC, Dr. Pallab Saha	15-06-2021	Review comments provided

Approval Note

SL No.	Name	Date Approved	Comments
1			

Release Note

SL No.	Released To	Release Date	Comments

Contents

List of Tables

List of Figures

1. Introduction

Project Brief

Government of Meghalaya envisions to deliver services that meets the evolving expectations of the citizens of Meghalaya, in-turn facilitate the citizens of Meghalaya realize their true potential. The Government has set an ambitious plan to be among the "**High-Income States by 2030**". The State Government recognizes the transformation potential of digital technologies, hence, looks to embark on digital technologies while it drives towards its vision. While there had been significant effort and investment towards adoption of digital technologies, lack of coordination and a **Whole-of-Government** approach has hindered desired outcome. To avoid such a pitfall and ensure a holistic approach, Government of Meghalaya intends to adopt a framework for digital technology adoption that facilitates service delivery and accelerates the transformation.

Ministry of Electronics and Information Technology(MeitY) notified IndEA framework, and entrusted National E-Governance Division(NeGD) to popularize and implement IndEA across States, Union Territories and PSUs. Government of Meghalaya, decided to adopt IndEA , as its guiding framework for service delivery enhancement and transformation. The initiative has been termed as **MeghEA** (Meghalaya Enterprise Architecture), a flagship and pilot implementation of IndEA. The responsibility of MeghEA project was assigned to Planning Department, Government of Meghalaya along with the able assistance from NIC Meghalaya and guidance from NeGD. As part of the procurement process, KPMG Advisory Services Private Limited was selected as the consulting organization to prepare Blueprint for Implementation of MeghEA.

MeghEA project had a wide area of focus , hence there was a need for a structured and planned approach. MeghEA intended to progress to the envisioned state in a phased methodology:

- Initially MeghEA had to derive its **Vision and Scope** – what to achieve and why to achieve?
- The core, to derive **Detailed Architecture Requirements** – Discover the problems and conceptualize the solutions.
- Preparation of **Finance Solution Architecture** – Deep dive on the solutions and make it implementation ready for pilot implementation by the State.
- Derive the **MeghEA Blueprint** – Plan, estimate and facilitate training.

The initiation phase derived the MeghEA Vision, Mission and scope. The Vision hinges upon the State Government's strategy, which is based on the **four strategic pillars** – **Human Development, Primary Sector, Infrastructure Development and Entrepreneurship with two cross-cutting pillars – Environment and Governance.** Additionally, all these strategic and cross-cutting pillars were mapped to Sustainable Development Goals (SDGs) and its indicator, to measure the progress in these sectors. The responsibility of achieving the desired targets under each of these indicators were assigned to selective departments. Thus, MeghEA Vision and Scope accomplished following critical actions:

- A total of **235** indicators spanning across **17** SDGs were derived, these are required to be monitored for success measurement. These indicators were mapped to each of the **6** pillars.
- State departments were assigned the responsibility to achieve targets for each of the **235** indicators whereas as part of study for preparation of Blueprint, **19** Departments were shortlisted.

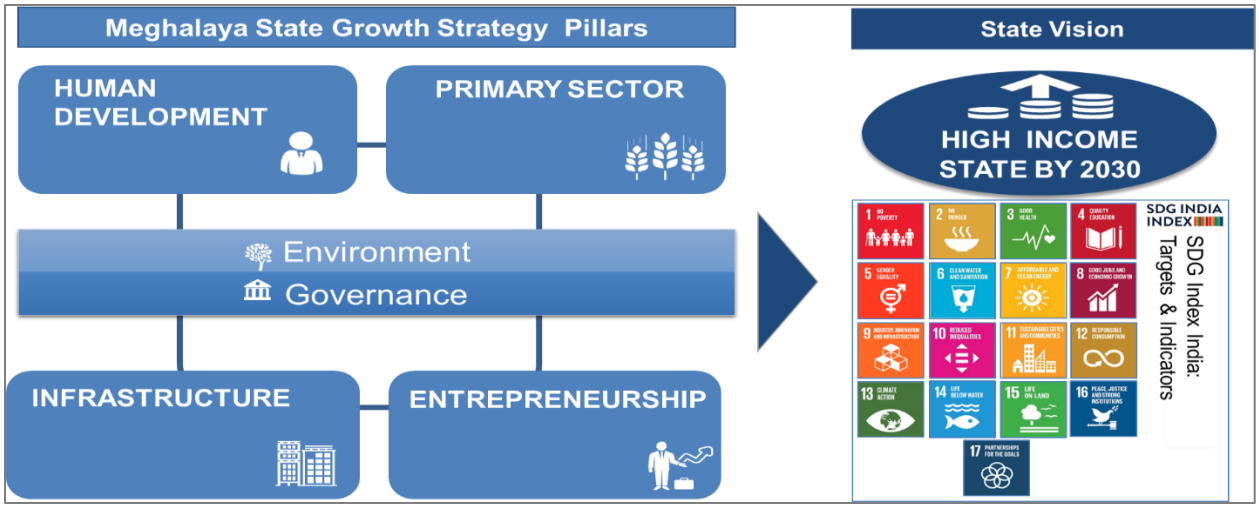


Figure 1: State Growth Agenda and Vision as MeghEA Vision and Scope

In the next phase – Detailed Architecture Requirements, MeghEA focuses on enabling service delivery aspects of the Government of Meghalaya. The shortlisted 19 departments were consulted to understand – what service they deliver? Whom do they deliver those services? How do they deliver those services? What (people, process and technology) enables the service delivery?

To collect the service delivery details, NIC Meghalaya developed **MeghEA Online Questionnaire** tool, enabled with set of assessment questionnaire. The tool facilitated smooth and efficient collection of information across the departments. MeghEA Project Coordination committee, NEGD and steering committee assisted the data gathering and review activity through timely interventions.

The key outcome of the exercise is listed below :

- **732** services pertaining to shortlisted departments were identified
- Step-by-step service process were documented for most of the key services
- **50**+ IT systems along with details were documented

The services were analyzed for enhancement following **IndEA** and **DSS** guidelines. Basis MeghEA service prioritization framework – considering the value services deliver to its stakeholders, the complexity of implementation and service maturity as per Digital Service Standard (DSS) assessment, a set of services along with new services were prioritized for implementation using digital technologies. Below diagram illustrates the services under prioritized under each pillar:

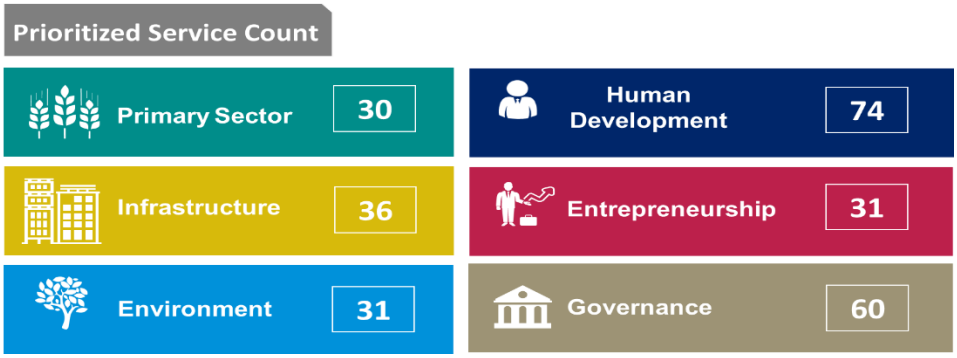


Figure 2: MeghEA Prioritized Services Overview

The service assessment and architecture requirements are elaborated in the detailed architecture requirement.

Below is the journey roadmap for the stages of the project:

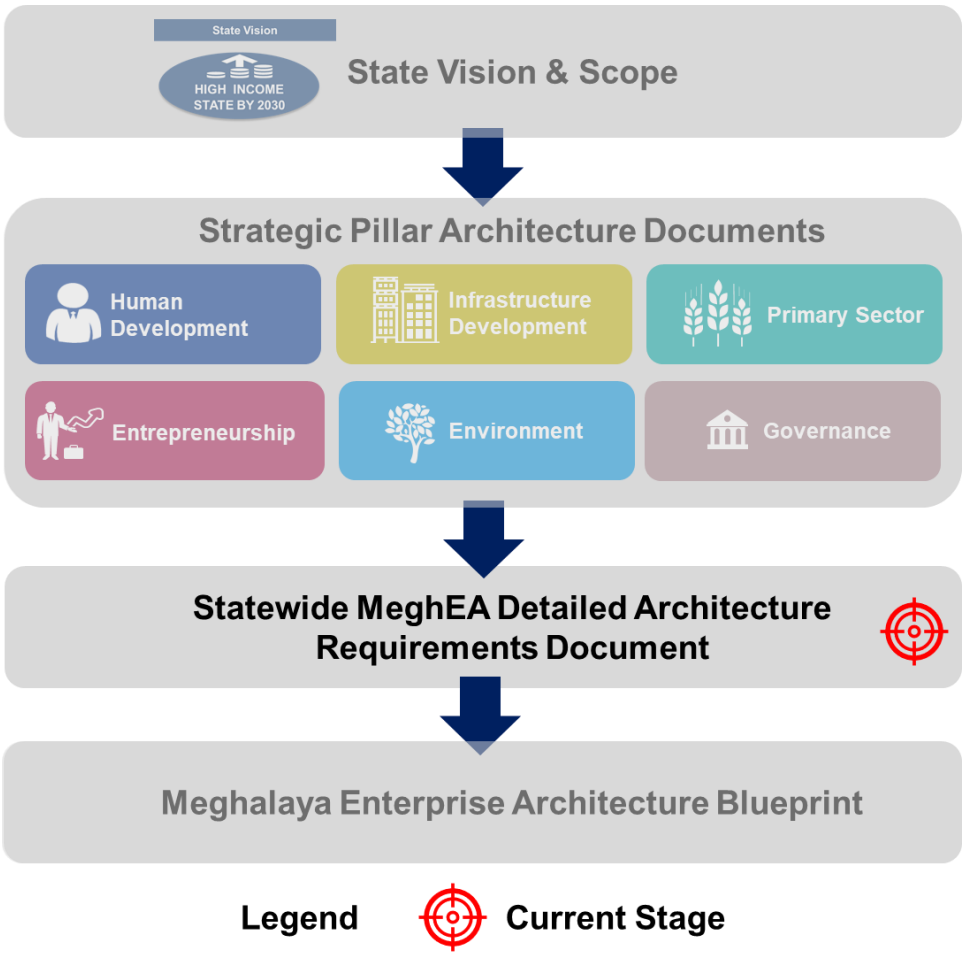


Figure 3: Project Journey Roadmap

Purpose of the Document

The current document is a brief summary of the detailed architecture requirements documents of SIX pillars along with overarching components that are applicable for all the pillars. The document serves multifold purpose:

- Enlist the various goals(SDG), indicators , vision and mission that are planned to be achieved. Thus, provides Government of Meghalaya a snapshot of the performance assessment plan
- Provides an overview of services, systems, data, technology and security architecture requirements to facilitate implementation planning, however, the detailing of the requirement is deliberately provided in the detailed architecture requirement of each pillar documents
- Provides the architecture implementation framework and change impact analysis to enable State Government to undertake key actions before and during implementation
- The document also provides architecture realization model along with an illustrative example that describes the sequence of activities and how the desired objectives are planned to be achieved

MeghEA detailed architecture requirements is further elaborated in following documents:

- Primary Sector Detailed Architecture Requirements
- Human Development Detailed Architecture Requirements
- Infrastructure Development Detailed Architecture Requirements
- Entrepreneurship Detailed Architecture Requirements
- Governance Detailed Architecture Requirements
- Environment Detailed Architecture Requirements

Target Audiences

The details referred or mentioned in document shall be reviewed and deliberated in discussion with the following stakeholders:

- All in-scope department's stakeholders
- NIC Meghalaya
- Project Coordination Committee
- National E-Governance Division (NeGD)

The Detailed Architecture Requirement documents and incorporated artifacts would be input for overall project plan with measurable business success metrics post stakeholder agreement.

This document is organized as per below Sections

Chapter 1 – Introduction.

Chapter 2 – MeghEA alignment to Government of Meghalaya's growth agenda and MeghEA' s architecture segmentation

Chapter 3 – Detailed Architecture Requirement along the domains of IndEA.

Chapter 4 – MeghEA implementation framework and action plan

Chapter 5 – MeghEA change impact analysis.

Chapter 6 – MeghEA Value Realization Model

Chapter 7 – Annexure

Exclusions

The detailed architecture requirements cover 19 in-scope departments as illustrated in Vision and Scope phase and State-wide common and cross-cutting components. While every effort was made to ensure all services, systems, data and technology are assessed and analyzed, there were few departments or directorates that were considered out of scope because of the unavailability of timely and specific information. These department or directorate are - Stamps and Registrations under ERTS department.

The service and system information provided in the MeghEA Online Questionnaire portal were deemed to be accurate and inclusive . Any service or system details beyond the information provided in the portal were considered out of scope and not included in the detailed architecture document. Exceptions were made in cases, where departments had key modifications to the information provided basis discussions with MeghEA team.

All systems for which the system ownership is beyond the purview of Government of Meghalaya, were assessed basis information provided in public websites and documents. Detailed analysis of those systems may significantly differ from existing analysis.

2. Government of Meghalaya Growth Agenda: MeghEA Architecture Alignment

2.1 Current State

Government of Meghalaya over the years had several initiatives, schemes and projects to deliver benefits to the people of Meghalaya through enhanced service delivery, while some efforts had delivered results other effort has fallen short of the expectation. Several national assessment frameworks such as SDG ranking, EoDB ranking, NESDA assessment indicate Meghalaya has not reached to its potential. While the reasons for the lower than expected results are many, there are few common issues which MeghEA would target to resolve:

- Lack of collaboration among departmental units and departments
- Fragmented development plan
- Department centric approach
- Skill gap of service delivery agents
- Reactive governance
- Non flexible service rules and regulations
- Redundant service process steps
- Manual mode of service delivery
- Limited flow of information across units of the Government of Meghalaya

2.2 MeghEA Resolution

MeghEA would look to provide resolution to all the above challenges to enable Meghalaya to achieve the required targets. Below is pictorial description of the resolution to the above problems as envisioned by MeghEA project.

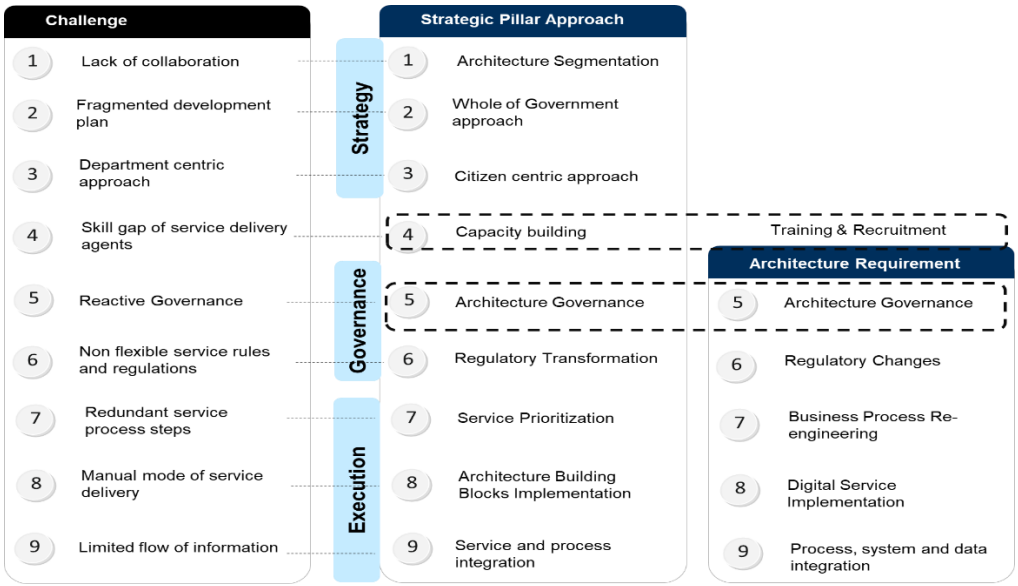


Figure 4: Government Wide Challenges and MeghEA Resolution

The above diagram illustrates the challenges (on the left) and how MeghEA looks to resolve through Strategic Pillar approach (on the middle) and Architecture Requirements (on the right).

2.2.1 Strategic Pillar Approach

The State Government has identified various priorities, the state's growth agenda is based on the four strategic pillars – Human development, Primary Sector, Infrastructure and Entrepreneurship with cross-cutting pillars – Environment and Governance.

Architecture Segmentation

MeghEA architecture would primarily be segmented in alignment with State's growth agenda. The architecture would comprise of:

- Whole of Government Architecture aligned to Agile IndEA Minimum Viable Architecture
- Strategic Pillar and Cross-cutting Pillar Architecture

While each of the strategic pillar and cross-cutting pillar architectures would comprise of seven architecture domains as per IndEA (with integration being covered in business, application, data and technology). Below is a pictorial illustration of the same.

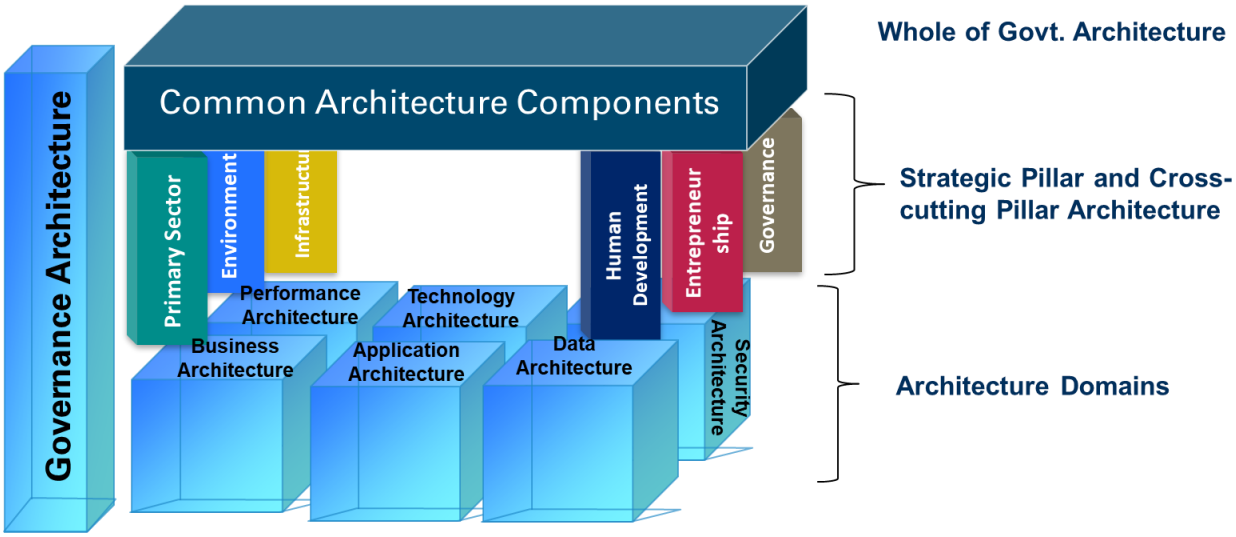


Figure 5: Architecture Segmentation

Whole of Government Architecture : Minimum Viable Architecture (MVA) , would be followed to derive the architecture. The concept of MVA is derived from the Agile methodology, to construct an incremental architecture implementation plan instead of a big-bang approach. In the context of the stakeholders of the Government of Meghalaya, MVA is the phase driven implementation of MeghEA to the final future state. The phases are described below:

- Phase 1: The mandatory building blocks are built; this would primarily include core building blocks implementation and few common solution implementation.
- Phase 2: The common solution building blocks would be focused along with few of the remaining core building blocks.
- Phase 3: The emerging technology related common solution building blocks would be implemented.

- Continuous Implementation: Certain building blocks needs to be continuously built as part of every phase activities OR has multiple components which needs to be built over few phases.

The whole of Government detailed architecture requirements illustrates the building blocks required for proper functioning of all the pillars and Common Architecture Components. The common architecture components comprise of services, systems to implement the common services in digital channels, core platform that enables common and department centric systems to deliver whole of service experience and supporting technology. The common components are arranged as per IndEA architecture domains :

- Performance Architecture - Whole of State Vision
- Business Architecture – Cross-cutting services
- Application Architecture – Common systems and core platform
- Data Architecture – State Digital Registries
- Technology – Technology platforms requirements to implement core and common systems
- Security Architecture – Lists the common components required to meet the security architecture design

Strategic Pillar and Cross-cutting Pillar Architecture: Basis State's Growth Agenda, the pillar architectures comprise of sector specific architecture requirements aligned to performance centric approach with goals mapped to indicators, indicators mapped to services, services enabled by systems, data and infrastructure.

The Strategic Pillar and Cross-cutting Pillar are:

- Primary Sector: The pillar focusses on growth and development in agriculture and allied sectors:
    - Agriculture
    - Animal Husbandry
    - Textiles
    - Fishery
- Human Development: The Government of Meghalaya is committed to its people and their development. This strategic pillar focuses on Human Development through various schemes, programs and services in the following sectors:
    - Education
    - Health
    - Social Awareness & Inequality
    - Food and Nutrition
- Infrastructure: Infrastructure development includes several key sectoral developments including:
    - Roads, urban transport, air transport and railways
    - Power
    - Industrial Estates or parks
    - Water Supply and Sanitation
    - Network Connectivity
- Entrepreneurship : The pillar aims to build a simplified and conducive ecosystem to set up a new business. It also aims to facilitate small scale businesses to help them grow and prosper.
    - Tourism

  - Labour Reforms
  - Rural employment
- Environment: The government of Meghalaya is committed and remains focused to reduce the adverse per capita environmental impact of cities, improving universal access to safe, inclusive and accessible, green and public space for all. Mining activities have been limited and being carried out on a sustainable basis.
- Governance: In terms of governance, Meghalaya is one of the few states where traditional institutions also exist. this allows people to have a greater stake and ownership in the governance of the state. Effective governance is the priority of the Government of Meghalaya, it has a wide area of focus from planning to security and implementation monitoring. Governance would look to cover all sectors.

Architecture Domains: The strategic and cross-cutting pillar architecture would be detailed as per IndEA architecture domains. The domains are area of architecture such as performance, business, application, data, technology, security and governance.

Current Document Coverage

This document (Whole of Government – Detailed Architecture Requirements) details the following areas:

- Common components architecture requirements at Statewide level, detailed under each architecture domains that would be required to ensure pillar architectures work in the manner that has been envisioned
- Provides an overview of services, systems, data, technology and security architecture requirements of all the pillars

Refer section MeghEA: Detailed Architecture Requirements for details. Refer individual pillar architectures for details around each pillar along the six domains of architecture

2.2.2 MeghEA Approach Value and Outcome

MeghEA intends to transform Government of Meghalaya by facilitating collaboration among units, implementing digital services following "Whole of Government" approach and introducing a Governance mechanism that measures performance through both outcomes and progress.

Strategic Pillar approach as described earlier is intended to achieve the following objectives:

Architecture Segmentation: The six pillars are a transformation change from existing department structure, the pillars are organized as per strategic focus of the Government and departments within a pillar incorporated to ensure the holistic coverage of service benefits across the beneficiary's lifecycle.

Illustration: Agriculture and Farmers Welfare department is focused to deliver services to a category of farmers. The same farmers would look to leverage animal farming and fishing opportunities, the current structure inhibits value delivery in an integrated manner. Farmers has to initiate service application on a fresh note. With the Strategic Pillar approach the need of the farmer would be assessed across all possible benefits and would be offered (proactively in the future state) to the farmer. Similarly, a pregnant woman identified by ASHA workers would be benefited from Health & FW department with prenatal care, institutional delivery and would be benefited by education admission of child from education department.

Whole of Government Approach: Aligned to the international best practices, strategic pillar

approach would benefit service design and assessment using Whole of Government approach. This approach targets to solve existing problem of departmentalism within the rigid structures of Government of Meghalaya , that hinders the use of existing resources and incentives. The strategic pillar approach would break these silos enabling effective collaboration in a structured manner.

Illustration: The strategic pillars are assigned Goals and indicators that needs to be achieved in a defined time frame. Aligning the group of departments to work together in a coordinated manner to deliver sector specific services, while the common services gets delivered centrally in factory setting.

The envisaged outcomes are:

- Realization of the Sustainable Development Goals and its associated indicators set in the vision through collaborative effort.
- Governance of the performance – from department centric to outcome oriented.
- Citizen centric and beneficiary specific services – from department centric services.
- Efficient use of resources – from department specific resources.

The diagram below illustrates the overview of each pillars:

- **Goals** – The number of sustainable development goals assigned to the pillar.
- **Departments** – The number of in-scope departments under the pillar.
- **Indicators** – The number of indicators assigned to in-scope departments under the pillar.
- **Services** – The number of services prioritized and recommended for new addition under each pillar.

Figure 6: MeghEA Architecture Segmentation Overview

3. MeghEA : Detailed Architecture Requirements

MeghEA detailed architecture requirement is categorized as per IndEA to the following architecture domains:

1. Performance Architecture
2. Business Architecture
3. Application Architecture
4. Data Architecture
5. Technology Architecture
6. Security Architecture

Integration architecture is covered in business, application and data domains. Governance Architecture would be detailed in MeghEA Blueprint document.

3.1 Performance Architecture

Performance Architecture has the objective of deriving architecture requirements aligned to achieve specific and measurable Goals. MeghEA has identified Goals and KPIs around following areas:

- **Vision**: All pillars have been assigned Specific, Measurable, Achievable, Realistic, and Timely goals as part of vision. The targets need to be further set to near term targets (such as 2022, 2024, etc.) for better monitoring.
- **Qualitative Objectives**: Each pillar has mission, that is a qualitative parameter to measure the success of service delivery. This mission statements are mapped to stakeholder benefits (envisaged).
- **Sustainable Development Goals (SDGs) Indicators**: Each pillar has been assigned multiple Sustainable Goals. These Goals has indicators mapped, as part of the State SDG framework and aligned to the MeghEA Vision (refer *MeghEA: Vision and Scope* Document for details).

3.1.1.1 Key Concepts

- **Sustainable Development Goals**: The SDGs are a collection of 17 global goals designed to be a "blueprint to achieve a better and more sustainable future for all". The SDGs are mapped to targets and indicators. As part of the Government of Meghalaya's SDG initiative, there are 17 goals mapped to the State's Growth Agenda.
- **Indicator** or **KPI** is a metric designed to evaluate the success of an organization or of a particular activity - such as a project, program, scheme or initiative undertaken by it. As part of the Government of Meghalaya's SDG initiative, there are 235 indicators mapped to the State's Growth Agenda.

3.1.1.2 Key Principles

Following are the common principles under Performance Architecture domain of MeghEA:

- ✓ **PP1 – Performance measurement must be linked to Goals and Indicators aligned to State's Growth Agenda**

Refer Performance Architecture principles in annexure for details.

3.1.2 Vision: Whole of State and Strategic & Cross-cutting Pillars

All strategic pillars and cross-cutting pillars have been assigned with a vision for the purpose to set **specific** and **measured** aspirational state for all the pillars to achieve. The State Vision to be in the **"Top ten states in India in terms of GSDP per capita"**

Below are the visions for each of the pillars

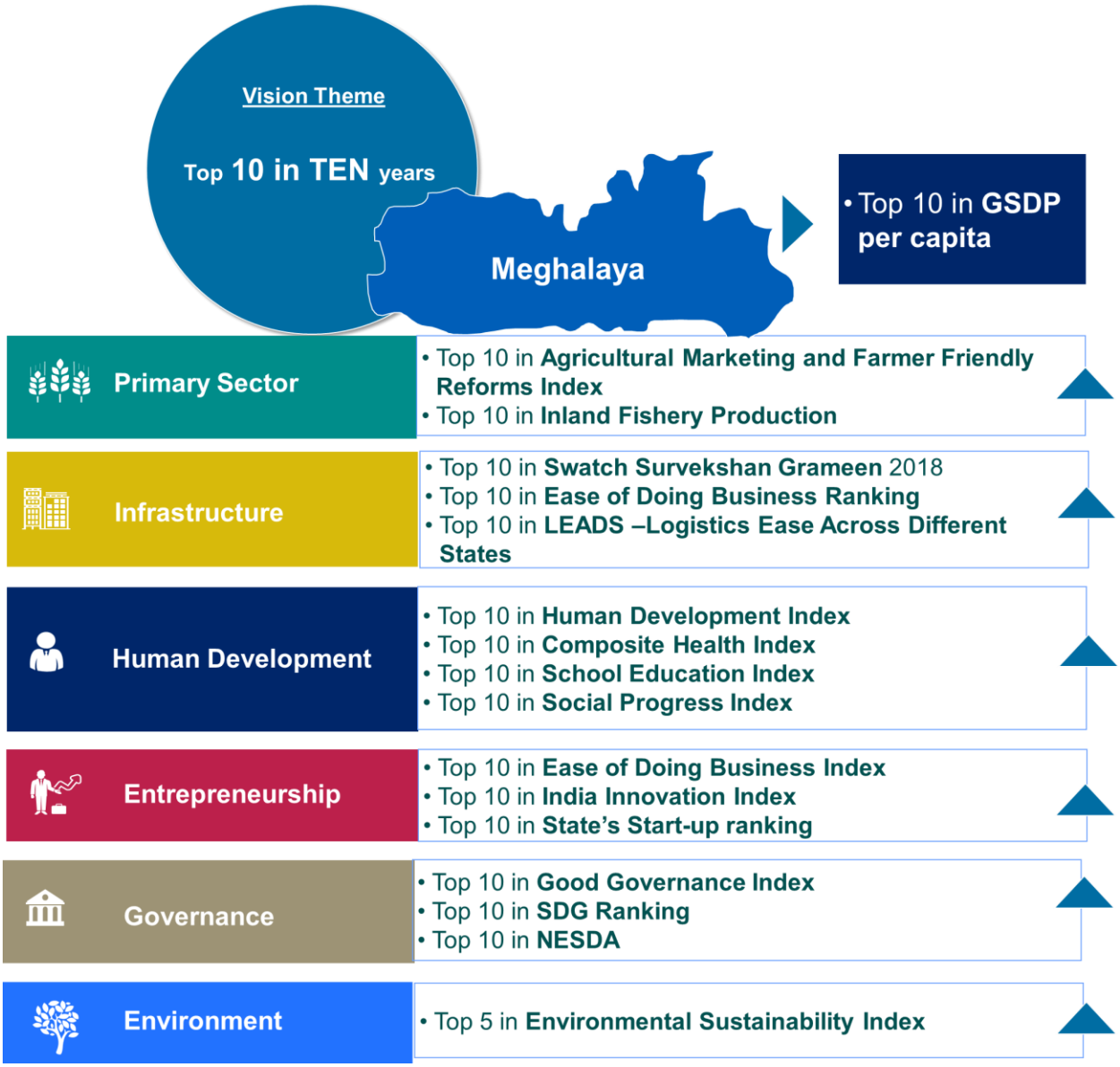


Figure 7: MeghEA Pillar Vision

3.1.3 Mission : Qualitative Success Measure

The graphical representation of the mission for all strategic and cross-cutting pillars are below:

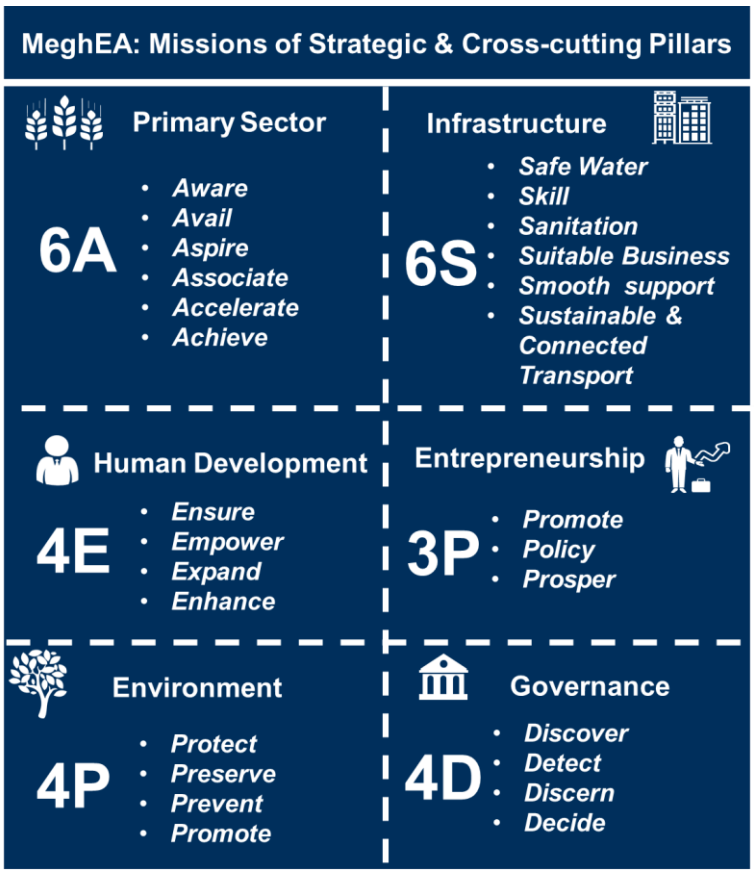


Figure 8: MeghEA Pillar Missions

As detailed in the Strategic Pillar and Cross-cutting Pillar documents, the mission for each pillar is defined considering the key stakeholder expectations from the departments. Below is a consolidated list of the same:

Mission of **Primary Sector**: Achieve the **6 A**s

- ***Aware:*** *Build Awareness About the Services Being Provided to The Farmers.*
- ***Avail:*** *Empower Farmers to Apply for Services at Their Convenience.*
- ***Aspire:*** *Aspire to realize Food Security in terms of Production and Productivity.*
- ***Associate:*** *Connect Buyers and Sellers and Enhance Supply Chain.*
- ***Accelerate:*** *Accelerate the innovations to Improve Food Supply Chain.*
- ***Achieve:*** *Achieve higher yield and improve Economic Livelihood of Farmers.*

Mission of **Human Development**: Achieve the **4 Es**

- ***Ensure:*** *Ensuring Education, Healthcare and Nutrition for all.*
- ***Empower:*** *Empowering people with Empathy.*
- ***Expand:*** *Expanding opportunities available to people.*
- ***Enhance:*** *Enhancing quality of life for people.*

Mission of **Infrastructure**: Achieve the **6 S's**

- ***Safe and Sufficient drinking Water****: Adequate safe drinking Water Supply to Rural and Urban population.*

- ***Skill enhancement of uninformed section**: Initiatives to excel the local craftsmen/artisan skills and their work.*
- ***Sanitation and Hygiene**: Improving the levels of cleanliness and sanitization through Solid and Liquid Waste Management activities and making State Open Defecation Free (ODF).*
- ***Suitable Business Environment**: Single-window system in Meghalaya for trade facilitation.*
- ***Smooth and conducive industrial support**: Adopted and implemented Industrial reforms.*
- ***Sustainable infrastructure**: Sustainable and reliable connectivity and communications, such as transport services and network across state.*

Mission of **Entrepreneurship**: Achieve the **3 Ps**

- ***Promote**: Create better infrastructure for the tourist destinations and Investment Ecosystem in the state.*
- ***Policy**: Effectively and efficiently, implement the Labour policies and Labour welfare programmes.*
- ***Prosper**: Uplift the socio-economic life of rural people.*

Mission of **Governance**: Achieve the **4 Ds**

- ***Discover**: Discover information from the all sections of society on stakeholders need.*
- ***Detect**: Detect actual problems and resolve through effective change management.*
- ***Discern**: Predict key policy changes that can assist government in resolving issues.*
- ***Decide**: Take swift and holistic decision through thorough analysis.*

Mission of **Environment**: Achieve the **4 Ps**

- ***Protect**: Protect forest flora and fauna through a sustainable model.*
- ***Preserve**: Preserve rich biodiversity, heritage, endangered species and culture.*
- ***Prevent**: Prevent and eliminate revenue leakages.*
- ***Promote**: Promote empathy for wildlife and restricted tourism.*

3.1.4 Aspirational State – Vision 2030

While Government of Meghalaya continues to drive forwards its growth agenda, it is necessary to set an aspirational target and monitor the progress in equal intervals to understand the next steps in accordance to the plan. Below is an aspirational plan for pillar specific visions

Strategic/ Cross-cutting Pillar	Departments	Index	2019	2030-Aspirational State
Primary Sector	• Agriculture & FW • Animal Husbandry & Veterinary • Fisheries • Textiles	Agricultural Marketing and Farmer Friendly Reforms Index	Rank - **26** out of 30 States Rank - **3** out of 5 NE small States	Top **10** rank **#1** in NE
		Inland Fish Production (Measured in metric ton per capita)	Rank - **18** out of 35 States & UTs Rank - 5 out of 7 NE States	Top **10** rank **#1** in NE
Infrastructure	• Transport • Public Health & Engineering • Commerce & Industries	Swatch Survekshan Grameen 2018	Rank - **10** out of 28 States & UTs Rank - 5 out of 8 Small States	Top **10** rank **#1** among small states
		Ease of Doing Business Index	Rank **34** among 36 states; **6** out 7 states in NE	Top 10 rank **#1** in NE

Strategic/ Cross-cutting Pillar	Departments	Index	2019	2030-Aspirational State
		LEADS –Logistics Ease Across Different States	Rank - **30** out of 32 States & UTs Rank - **3** out of 5 NE small States	Top **10** rank #1 in NE
Human Development	• Health & Family Welfare • Education • Social Welfare • Food & Civil Supplies	Human Development Index	Rank - **26** out of 36 States & UTs Rank - **6** out of 7 NE States	Top **10** rank **#1** in NE
		Composite Health Index	Rank **5** among 8 small states, categorized as "**Achievers**"	Top **10** among all states
		School Education Index	Rank **35** among 36 states, **7** out 8 small states	Top **10** rank **#1** among small states
		Social Progress Index	Rank **21** among 28 states, **6** out 8 small states	Top **10** rank **#1** among NE states
Entrepreneurship	• Labour • Tourism • Community & Rural Development	Ease of Doing Business Index	Rank **34** among 36 states; **6** out 7 states in NE	Top 10 rank **#1** in NE
		India Innovation Index	Rank 11 out of 11 NE & Hill States	**#1** in NE
		States' Start-up Ranking 2018	Meghalaya has not been ranked	Top 10 rank **#1** in NE
Governance	• Planning • Finance • Excise Registration Taxes Stamps	Good Governance Index	Rank **18** among 36 states & UTs; **5** out 8 states in NE & Hill states	Top **10** among 36 states; **#1** in NE & Hill states
		SDG India Ranking	Rank **25** among 29 states; **6** out 7 states in NE	Top **10** among 29 states; **#1** in NE
		National e-Governance Service Delivery Assessment 2019	Rank **20** among 26 states; **7** out of 9 states in NE & Hill states	Top **10** among 26 states; **#1** in NE & Hill states
Environment	• Forest & Environment • Mining & Geology	Environmental Sustainability Index	Rank (7^{th} -11^{th}) among all states and UTs,	Top **5** among states;

Table 1: Vision – Aspirational and Current State

3.1.5 Sustainable Development Goals

As part of State Government's SDG initiative, 235 indicators have been assigned to the 6 strategic and cross-cutting pillars. Pillar wise SDG Goal to Indicator mapping is illustrated below:

Figure 9: SDG Goals and Indicators mapped to Pillars

Each of the above indicators are further mapped to one or multiple services from the in-scope departments depending on its relevance to the service.

3.2 Business Architecture

Department's perform several functions to complete their mission. In order to achieve success in the performance of these functions a single view or blueprint of the department is required. This view or visualization encompasses services offered by the department, processes needed to deliver the services, people associated with the service delivery – their skills and tools and the regulations associated with it. The Business architecture referred to here is in fact, the creation of these visualizations.

3.2.1.1 Key Concepts

- **Government Services:** Government Service is one that is provided by a government agency to its citizens, businesses, employees or other government agencies, in any form of delivery. A service may have several components, process steps, service levels and performance metrics. A service should have ONE beneficiary (Citizen, Business, Employee or Other Government Agency) and only ONE key outcome such as:
    - Certificate, License, Information, NOC, Approval letter (Digital Outcomes)
    - Sanitation, Enough water, Industrial Education, Employment, public transport service, etc. (Physical Outcome)

- **Service Rationalization:** This is the process in which services that were initially identified were merged with other service that provides the same output to the stakeholder. Considering whole-of-service approach MeghEA intends to define a service in the entirety of its value delivery cycle. In rationalization activity services were also rationalized if that were a process step in an already identified service or were just a system level activity.

3.2.1.2 Key Principles

Following are the common principles under Business Architecture domain of MeghEA:

- ✓ **BP 1 - Integrated Services**
- ✓ **BP 2 - Maximization of Benefit**
- ✓ **BP 4 - Government Process Re-Engineering**
- ✓ **BP 5 - Inclusive Services**
- ✓ **BP 6 – Unique State Digital ID**
- ✓ **BP 7 – Digitally Deliver Payment related services**
- ✓ **BP 8 - Enable Digital Certificates for all Services**

Refer annexure on Business Architecture Principles for details around each of the business architecture principles

3.2.1.3 Standards

Standards Code	Standards	Recommendations
BS.1	**Business Process Modelling** 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 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 that can be used with all major object methods and applied to all application domains.	Future state recommendations post 1st phase roll-out of MeghEA. The UML/other modelling standards require socializations before acceptance
BS.3	**Digital Service Standard** To ensure departments are planning delivery of e-services in a consistent way, digital service standard compliance would be mandated across the Government of Meghalaya Departments.	Must be adhered for service designing, all service would go through MeghEA Service Assessment Framework for approval for implementation

Table 2: Business Architecture Standards

3.2.2 Pillar Specific Services and Cross-Cutting Services

3.2.2.1 Approach

The approach towards business architecture is current state service identification, rationalization of services, prioritization of services, service catalogue finalization and plan for implementation of the re-engineered services.

- **As-Is State Service**: Various stakeholders from all in-scope departments were facilitated to provide department specific services in a detailed format. NIC Meghalaya developed a portal MeghEA Online Questionnaire, this enabled digital mode of data collection
- **Service Rationalization**: Services were subsumed under relevant service domains and were deleted (owing to various issues)
- **Service Prioritization** : The parameters identified are elaborated below:
  - ✓ **Maturity Level of service as per Digital Service Standards (DSS):** Basis DSS assessment framework. Please refer framework in Annexure Section 7.7
  - ✓ **Complexity of Implementation**: The viability of delivering the service value completely through digital technologies.
  - ✓ **Value to Stakeholders**: The value to stakeholders is derived from the indicator mapping with the services.

The assessment framework is graphically depicted below – the blue blocks are categorized as medium priority, the green boxes categorized as low priority and the dark blue boxes categorized as high priority

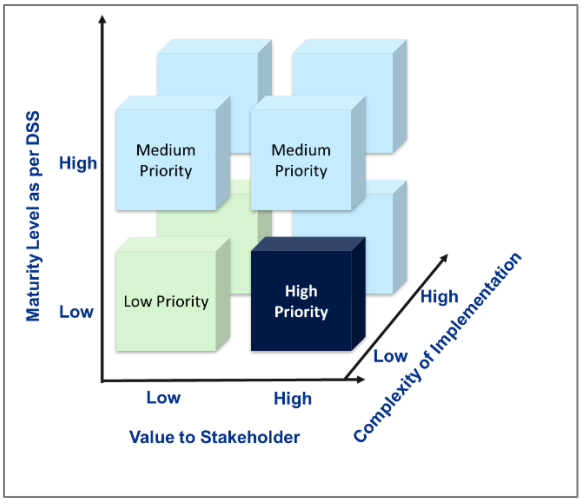
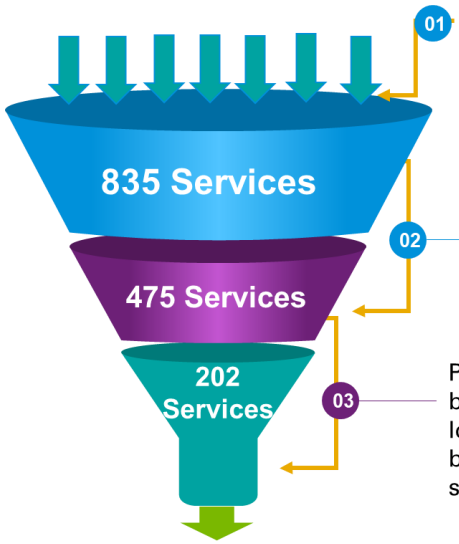


Figure 10:MeghEA Service Prioritization Framework

Below is the representation of steps taken for services captured from the in-scope department to the prioritization.



01 Service Portfolio from the department stakeholders. **835** services identified with regards to the service delivery channel, service type, locations of service delivery, and several other details regarding the service.

02 Detailed analysis, subsume, de-duplication: 360 services were merged/ subsumed within an existing service or marked as duplicate. Post this **475** services were mapped to Indicators

03 Prioritization based on Service Assessment against DSS basis digital maturity- categorized to high, medium and low maturity. **202** services identified as priority services basis "value to stakeholders", degree of complexity in service transformation

Accomplishments:
202 services prioritized for First Phase consideration for Implementation
60 services are planned for New Implementation

Based on above the above three criteria, service prioritization is illustrated below:

Figure 11: MeghEA – Prioritized and New - Service Portfolio

3.2.3 Cross-Cutting Services

Cross-cutting Services are services which are designed such that a single workflow cuts across multiple departments and provide the end result to the service beneficiary, who could be an

employee, citizen or a business entity. Basis, IndEA there are 12 horizontals that represents high-level service groups or in MeghEA' s parlance service domains. These service domains could comprise of multiple services or one service. These services are delivered by multiple departments, i.e. the service process cuts across multiple departments – mostly the line departments and Finance department. Below is the list of the service domains.

The table below describes the services within each of the domains.

Function	Service	Description
Human Resources Management	Recruitment	Recruitment service provides in-take of employees in various government departments
	Post & Allotment	The service deals with posting of different employees in districts, branches and offices under a department or within the government
	Annual Property Return	The service deals with submission and validation of annual property of designated government employee
	Pension	The service deals with application, disbursement and computation of pension.
	Service Book	The service deals in record keeping of employee performance and details on litigation
	Medical Claims	The service deals in application, processing and approval of medical claims of government of Meghalaya employees
	PF & Gratuity	Service to withdraw, compute and record keeping of PF and Gratuity of employee
	Leave	The service deals in attendance, leave application and leave approval of employees. It also deals in leave encashment
	Travel	The service deals in travel allowance approval, travel management of employee and other travel related activities
	PayScale	The service deals in employee salary management, salary slip generation, salary fixation, salary anomaly reporting and other salary related activities
	Training	The employee trainings and skill development are largely dealt by this service
	Promotion	Employee promotion related service, also deals in upgradation of posts
	Facilities	The service deals in facility management of employees and elected candidates
Financial Management	Budgeting	The service deals in planning and budgeting expenditure for the line departments within the departments
	Revenue	The service deals with collection of revenue on different head of accounts

Function	Service	Description
	Expenditure	Service deals with billing and managing expenditure under different head of accounts
	Loans	The service deals in loans and financial assistance that department seeks from various financial bodies
	Audit	Auditing service deals in audit of local institution's financial transactions, bills and other financial bodies affiliated to it
Right to Information	RTI Services	Service provides responses to various petition raised under RTI Act
Land & Resource	Government Land Resource Management	Service deals with registration, update and subsequent access to use of government land
Unified Contact Centre	Management of service delivery from citizen service centres	The service is about management of CSC(rainbow centres) , tracking service feedback, maintenance of service SLAs by CSC's
	Technology based response management	The service is about implementation and support of service response from technology tools
Litigation Management	Litigation Case Management	Management of various litigations against concerned department and department officials
Performance Management	Scheme & Project Performance Tracking and governing	Service deals with tracking the progress of projects and schemes – both physical and financial progress
Procurement Management	Procurement and vendor assessment	Procurement of goods and services adhering to the necessary regulatory norms. The service also deal with the assessment of the vendor
Grievance Management	Grievance Redressal	Service manages responses to grievances raised by citizens or employees and deals with tracking of pending grievances as well
Asset Management	Access to Government Office resources	Service to provide access to government buildings, resources including technology resources and travel related services for employees
Communication & Collaboration	Message Exchanges	The service deals with implementing technical tools to exchange messages between various stakeholders of GoM
	Work Collaboration	Service intends to provide and support unique collaborating tools that enable exchange of knowledge among stakeholders
Service Delivery Management	Service delivery channel management	Service is about managing various delivery channels of the services and intends to ensure services are delivered through all possible delivery channels
	Service Governance	Governance of service SLAs, service feedback and other service related KPIs
	Service workflow	Service is about enabling workflow of approvals or review through technical solutions

Table 3: List of Cross-Cutting Services

Service Delivery Management is an Administrative Capability which would be used to deliver end user services by the departments. Below would be the steps for the same:

- Identification of service to be delivered
- Define workflow and stakeholders for the service
- Define SLAs and KPIs to be achieved
- Identify service delivery channels

- Replication of workflow in a digital tool which will be called as workflow engine of the core platform.

Refer section application architecture building blocks for corresponding system that would look implement the above services using digital systems.

It is recommended to **standardize** the service processes across all departments to ensure optimum usage of resource while maximum outcome from the services. The standardization would need following set of activities:

- Assessment of services process from all departments to understand the variability and impact of standardization.
- Derive future state process for all above services basis business process re-engineering and comparative study of other states.

3.2.4 Business Interaction Matrix

This matrix illustrated the inter-pillar service – with two segregation:

Consuming Business Services : Pillars act as a beneficiary by consuming business services provided by other pillars.

Providing Services : Pillars acts as the service provider by providing services to other pillars.

How to read below matrix. Horizontally – Traverse horizontally for each record to understand the services that consumed by the respective pillar(refer column header), for ease of reading the

Providing Business Services	Consuming Business Services					
	Primary	Human Development	Infrastructure Development	Environment	Entrepreneurship	Governance
Primary		1. Food grain, meat & fish from farm produce 2. Registered farmers list for health insurance 3. Food samples for food safety testing 4. Stipend/ scholarship in higher studies in Agri/veterinary fields 5. Provide grains (Rice & Wheat) for distribution		1. Forest Trees Saplings	1.Demands of agriculture and allied products 2. Jobs to Textile Designers	1. Vegetable Statistics 2. Land Usage Statistics 3. Irrigation Statistics 4. Price Statistics 5. Agriculture Statistics Crop Report 6. Funds by sale of Products from Government farms
Human Development	1. Social Security schemes related to Farmers 2. Health Insurance to Farmers 3. Capacity building of Farmers 4. Food contamination points in the supply chain 5. Demand for farm produce in FCS&CA 6. Social Security schemes related to Farmers 7. Health Insurance to Farmers 8. Capacity building of Farmers 9. Help in distribution of Inputs (Seeds, Fertilizers, Pesticides, Saplings etc.)		1. Procurement order for food in FCS 2. Building construction fund 3. Trained manpower for industries 4. Health insurance for private transport operators	1. Scholarships to local student for higher studies in Mining, Geology, Environment protection etc. 2. Health checkups for mining workers 1. Manpower Educated in Mining Sector 2. Health Schemes	1.Verification of educational qualification 2. Supply of trained work force 3. Apply for Financial Assistance under socio economic development schemes 4. Financial Benefits for Entrepreneurs Programs 5. Register for Employment 6. Registration for empowerment programs	1.Utilization of funds 2.Progress of schemes 3.Care for orphan child 4. Rehab of drug addicts 5.De-addiction programs 6. Monitoring of Health Schemes 7. Housing Statistics 8. Monitoring of Mothers and Child 9. Monitoring of Food Distribution Schemes

Providing Business Services	Consuming Business Services					
	Primary	Human Development	Infrastructure Development	Environment	Entrepreneurship	Governance
Infrastructure Development	1. Transport Facilities	1. Power to institutes, hospitals 2. Building development for schools and hospitals 3. Road connectivity to schools and hospitals 4. Air-ambulance 5. Licenses for food transportation 6. Permits for FCS&CA goods 7. Infrastructure for Anganwadi center		1. Road Facilities 2. Transportation Facilities	1. Registration Under Labour Laws 2. Employer Registration 3. Amendment in Registration 4. Vacancy Reporting	1. Monitoring of Funds provided for Infrastructure Creation 2. Monitoring of Physical and Financial progress of Projects and Programs
Environment		1.Recreational and educational tourism spots, zoo and parks			Business Opportunities to Small Entrepreneurs (Furniture, Stone Crushers units etc.)	1. Specific Projects Programme 2. Improve Environment with Science & Technology Projects 3. Sustainable Green Agriculture 4. Investigate the possibilities of augmenting and improving resources of the state 5. Revenue from Mining
Entrepreneurship	1. Apply for Skill Trainings 2. Field Trainings 3. Candidate Registration 4. Skill Hands Registration Update 5. Skill Hands Citizen	1. Skill demand in job market 2. Candidate Registration 3. Skill Hands Registration Update	1. Registration of Hotels Guest houses/ tourist Accommodation units/ etc 2. Registration			1. Monitoring of MGNREGA Schemes for Job Creation 2. Monitoring of

Providing Business Services	Consuming Business Services					
	Primary	Human Development	Infrastructure Development	Environment	Entrepreneurship	Governance
	Registration 6. Apprenticeship 7. Market Linkages - Agri Business 8. Demand for Agriculture Inputs and alied services like warehousing and cold storage to increase Agri capacity 10. Policy and Law Support - Import, Export, Trade Policy 11. Sector Development Roadmap 12. Supply of Machinery	4. Skill Hands Citizen Registration 5. Apprenticeship	of contractors 3. Development and Management of Tourist Spot			different C&I Schemes
Governance	1. Vegetable Statistics 2. Land Usage Statistics 3. Irrigation Statistics 4. Price Statistics 5. Agriculture Statistics Crop Report 6. Financial regulations - Minimum Support price, etc. 7. Scheme Funding 8. Sanction of Funds 9. Approval on Scheme Annual Action Plan 10. Issuance of LOA 11. Scheme monitoring and Evaluation 12. Sectoral Strategy and Planning	1. Financial regulations 2. Scheme Funding 3. Sanction of Funds 4. Approval on Scheme Annual Action Plan 5. Issuance of LOA 6. Scheme monitoring and Evaluation 7. Sectoral Strategy and Planning 8. National Sample Survey	1. Monitoring of Funds provided for Infrastructure Creation 2. Monitoring of Physical and Financial progress of Projects and Programs	1. Specific Projects Programme 2. Improve Environment with Science & Technology Projects 3. Sustainable Green Agriculture 4. Investigate the possibilities of augmenting and improving resources of the state 5. Scheme Funding 6. Sanction of Funds 7. Approval on Scheme Annual Action Plan 8. Issuance of LOA 9. Scheme monitoring and Evaluation	1. National Income (NI)	

Table 4: Business Interaction Matrix

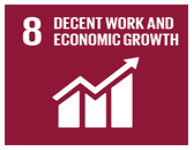
3.2.4.1 Digital Service Implementation: DSS Alignment and Next Steps

Digital Service Standard has been extensively referred to derive the architecture requirements and service design. The services prioritized above has several components that is critical for implementation.

Service Objective

The objective of the Digital Service has been mapped with all the goals and indicators identified in the vision phase. Refer Pillar documents section – *Service Indicator mapping* for details.

Illustrative Example:



Goal 8. Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all

Indicator: ***Farmers with surplus crop production, enabled to be an entrepreneur***

Service Code	Service Name
AFW.06	Distribution of Seeds to Farmers
AFW.16	Distribution of Soil Health Card to Farmers
AFW.20	Testing of seed samples collected from the farmers
AFW.21	Providing Inputs to Farmers
AFW.01	Provide Training and Awareness to Farmers
AFW.02	Financial Assistance for Establishment of Agriculture Infrastructure
AFW.37	Distribution of Machineries and Equipment
AFW.91	1917 iTEAMS Agro Advisory, Market Connect and Transport Logistics

Service Catalogue

The service catalogue comprises of various aspects of the service taking into consideration that the purpose of the catalogue was to define the services that are planned for implementation. Refer 9.7 Future State Service Catalogue in each pillar documents for clarifications.

Illustrative Example:

Service Code	Service Name	Service Description	Service Type	Service Frequency	Service Delivery Channel	Service Level (Days)
FCS.01	Issuance/ Renewal/ Cancellation of FPS/ SK Dealer License	The citizen applies for New FPS/SK Oil dealer License. Basis eligibility criteria and details provided, department approves licensing or renew license	G2B	As per request	Digital – Mobile, State Service Delivery Portal, Rainbow Centre, Umang App, State Service App	Service will be delivered in **5 days** from data of application submission

Service Design

Digital Services are planned to be designed taking into consideration the precise needs of the

targeted Users. Refer Pillar Document – (Beneficiary) *Service Life Cycle* for details around what stage services, which services deliver benefits. Further, beneficiary life cycle has been mapped to service delivery challenges and bottlenecks to facilitate architecture requirement finalization.

Illustrative Example:

Stage	Sub- stage	Service	Indicator
Birth	Institutional Delivery	Treatment - Pregnancy and related care	• Reduce Neonatal mortality rate(NMR) per Lakh • Reduce maternal mortality ratio (MMR) per lakh • Percentage of home births compared to total number of births

Additionally, Service design needs to be based on DSS Assessment framework with the objective of scoring maximum marks as per the framework.

Whole-of-Government Approach

The service listing has taken into consideration – "Whole-of-Government Approach" to design the end-to-end services. Refer application architecture, data architecture, technology architecture and security architecture for requirements on the Whole of Government approach.

Illustrative Example:

- Refer *Service Application Module Mapping* section in pillar documents for details on application requirements for digital service implementation.
- Refer *Service and Data Mapping* section in pillar documents for details on role of services in the data life cycle stages.
- Refer technology architecture section and security architecture in pillar documents for specific requirements around technology and security.

Service Classification

Services have been classified under following categories:

- **Strategic Pillars** – Services have been mapped to pillars and departments; please note the basis is department – service mapping, multiple departments relate to more than one pillar.
- **Service Domains** – Aligned to National Government Services Portal, services are mapped to service domains.
- **Type of services** – Services are classifieds to Government to citizens, Government to business, Government to employees and Government to Government.

Basis architecture requirements, there are specific next steps that the Government of Meghalaya needs to undertake to implement the services.

3.2.4.2 Next Steps

Business Process Re-engineering

Refer following key sections in the pillar documents to execute Business Process Re-engineering for prioritized services.

The Use Cases for Services:

The architecture use cases for prioritized service is detailed in section " Service Realization Model", these use cases would form the basis of system and process design.

The System flow illustration:

The implementation of services would need a specific system flow, this is detailed in section

"Illustration of Use Case Realization". Please follow the section for details on how to design the system basis of high-level process flow.

Service Design

User Experience (UX) – Refer Digital Service Standard to design UX for services.

System Requirements

Refer application architecture section for pillar documents for applications, modules, functionality and infrastructure requirements.

Regulatory Changes

Refer pillar documents section " Regulatory Changes" to understand the regulatory change requirements considering digital service implementation. Following are the key activities:

- Form committee within the department to undertake regulatory changes
- Draft required changes and present to committee
- Approve modifications, new order post approval

3.3 Application Architecture

MeghEA Application Architecture defines the blueprint for the IT Systems to be deployed, their interactions with each other, and their relationships to the Government services. IT systems would essentially support key processes in a service to be delivered with or without manual interventions.

The purpose of application architecture is defining the guiding strategy behind implementation of IT systems in the State IT ecosystem, provides the inventory of existing systems (referred as As-Is Portfolio) and the transformation plan. This section describes the application architecture of MeghEA:

- List out the current state systems that are used
- The application architecture building blocks
- The Future State application architecture
- The application transformation plan

3.3.1.1 Key Concepts

- **Legacy Application**: Legacy application is an IT system developed in the past in (currently) outdated technology. These applications may be commercial of the shelf(COTS) or bespoke(customized in-house developed) application as well.
- **Application Integration**: The inter-application transfer of information using technology in an automated and most convenient way that enhances collaboration among Government units.

3.3.1.2 Key Principles

Application Architecture principles are used to capture the very basis of how Government of Meghalaya will use and deploy applications. The principles are used in several different ways:

- To provide a framework within which the State Government(Meghalaya) can start to make conscious decisions about systems and apps.

- As a guide to develop a relevant evaluation criterion, thereby exercising influence on the selection of products, solutions, during the later stages of managing compliance with reference to the enterprise architecture.
- Support activities related to architecture governance in terms of providing a rule book' for the standard architecture compliance assessments.

Following are the common principles under Application Architecture domain of MeghEA:

- ✓ **AP1 – One User Interface**
- ✓ **AP2 – Sharing & Reusability**
- ✓ **AP3 – Technology Independence**
- ✓ **AP4 – Loosely Coupled Architecture**
- ✓ **AP6 – Adherence to Non-Functional Requirement**
- ✓ **AP7 – Applications to interoperate using integration platform**

Please refer annexure on Application Architecture Principles for details

3.3.1.3 Standards

Below is the list of standards that needs to be followed for all application design, development and testing:

Standards Code	Standards Name	Description	Recommendations
AS.1	User Interface Standards	Adherence to GIGW standards for user interface design	Must be followed
AS.2	Code Readability	Indent and comment on code for better readability	Must be followed
AS.3	Web Service Standard	Follow latest standard of protocols for • SOAP • JSON • XML	Must be followed
AS.4	Code Naming Convention	Use of Camel Case and business relevant name in declaring all classes, entities and variables	Must be followed
AS.5	Software and system engineering	Follow ISO/IEC/IEEE 24765 standard for systems and software engineering	Recommended
AS.6	Software testing	Follow ISO/IEC/IEEE standard 29119 for software testing	Recommended

Table 5: Application Standards

3.3.2 MeghEA Application Portfolio

As part of National E-Governance Service Delivery Assessment, Meghalaya has achieved an overall score of 0.44, ranking 7th out of 9 NE and hill states. Following are the key insights from the assessment:

- Emerged as a leading State in NE States and Hill States category for the **Ease of Use**
- Significantly fallen behind in Accessibility, Content Availability, Information Security and Privacy, leading to a low overall score
- Meghalaya has good assessment scores in Finance, however low scores in sectors such as Health, Education, Labour & Employment and Local Government sectors.

All applications have been grouped to following categories:

- **Department Applications**: Applications currently performing one or more business operations of a single department.

- **Strategic Pillar Applications**: Applications currently performing one or more business operations of a single Strategic Pillar.
- **Common Applications**: Applications currently performing one or more business operations all pillars.
- **Core Applications**: Applications currently supporting common, Strategic Pillar or department applications to deliver whole-of-a-service experience.

3.3.2.1 As Is Portfolio

State Applications: The applications that have been deployed and customized for the state and deployed in the State Data Centre or on cloud under the sole purview of the State Government of Meghalaya.

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.

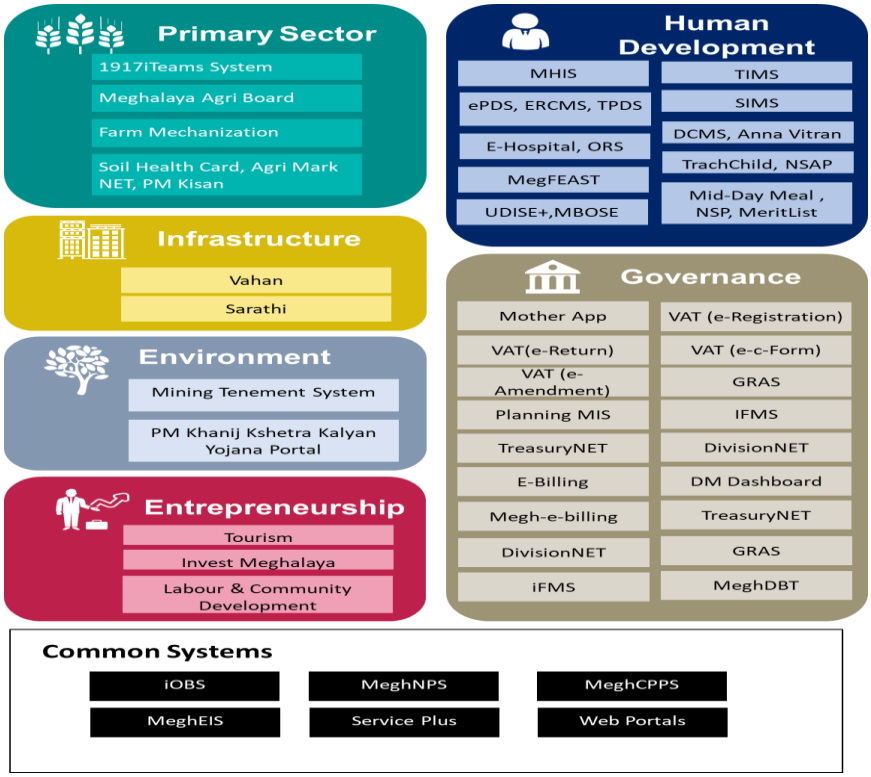


Figure 12: As-Is Application Portfolio

Please refer " *As-Is State Application Architecture*" in Pillar documents for details about each of the above applications.

3.3.3 Application Architecture: Building Blocks

The services derived for each strategic pillars or cross-cutting pillars need to be delivered through digital channels to enhance efficiency in service delivery. The building blocks described above would be realized through existing applications considering the principal of re-use in mind.

Application Type	Building Block	Solution	Functional Description	Required Functional Capability
Common System	Financial Management	Budgeting	The budgeting system would facilitate budget estimation, budget distribution, LOA issuance, and various other services such as supplementary demand, re-appropriations, etc.	Budget Estimation LOA/LOC Supplementary Demand Re-appropriations Budget Distribution Scheme Financial Management Savings & Utilization Deposit Account
		Expenditure	The expenditure system would facilitate digital billing from departments (DDOs) for expense management	Digital Billing Challan Processing Bill Auditing Bill Audit Allotment Reports Ways & Means Alert Economic Measures
		Revenue Management	System for Digital payment for Government revenue, generalized application for all departments.	Revenue Target Revenue Reports Revenue – Bank Integration Revenue Status Reporting e-Challan Generation
		GST Accounting	Reconciliation system, to reconcile data from GSTN and RBI-e-Kuber system	Rate Notifications e-Way Bill Registration Refund Statement and Return Payment of Tax
		Direct Benefit Transfer System	Direct Benefit Transfer (DBT) intends to transfer benefits to individuals' bank accounts electronically, minimizing tiers involved in fund flow thereby reducing delay in payment, ensuring accurate targeting of	Schemes (DBT) Reports Aadhar Seeding(Beneficiary Registration) Integration with NPCI PFMS Integration

Application Type	Building Block	Solution	Functional Description	Required Functional Capability
			the beneficiary and curbing pilferage and duplication.	Authentication for in-kind transfer
	Land & Resource Record Management	Land Record Management System	System to modernize management of land records, minimize scope of land/property disputes, enhance transparency in the land records maintenance system, and facilitate moving eventually towards guaranteed conclusive titles to immovable properties in the state.	Digital Land Map Land Records Database Online Mutation of Land Records New Registration Government Property Records
	Content Management, Document Management and Citizen Locker	Content Mgmt.	Content Management System is a software application that automates the administration, tracking and download of Government policies, acts, rules, SOPs, and other key knowledge related documents. The system is also about web-based content management and image capture	Indexing of documents Search – Document metadata Search – in Documents Upload and download facility Integration facility with state portal Data Visualization – Real-time dashboard on GSDP, Industrial Growth Imaging – Scanning solution of physical records Document & Multi-media Content – Storage and retrieval Web Content – Publishing of documents and content in portals
		Document Management System	The document management system is the digital file handling system enabled by manually driven workflow.	Storage of Service-related documents Storage of templates Index search Workflow File Management (Government files) Receipt, Noting, draft and dispatch on Files Facility to add attachments to files Merging/de-linking of files Indexing of documents Search – Document metadata Search – in Documents Upload and download facility Integration facility with state portal

Application Type	Building Block	Solution	Functional Description	Required Functional Capability
				Data Visualization – Real-time dashboard on GSDP, Industrial Growth
		Citizen Locker	The system would provide facility to store documents from citizens or from Government entities(for citizens)	Aadhar based authentication Document Segregation – Issued by authorities, stored by citizens and request by requestor
	Service Delivery Management	Service Provisioning	System with flexible in-built workflow to implement government services in a digital delivery channel.	Service addition/update/deletion Service workflow design/integration Service implementation Service Form Design Service integration with integration platform
	Project and Scheme Management	Scheme Mgmt. System	Provide Centralized monitoring and analytics for physical & financial progress, through decentralized data collection.	Scheme Registration Scheme Plan Submission Scheme approval Scheme progress reporting Project data entry Workload management Capital Expenditure Operational Expenditure Scheduling
	HR Management	e-HRMS	HRMS is a standard ICT solution for the Government sector, addressing maximum requirements of Meghalaya Government related to personnel management.	Employee Profile Management Posting Online Leave Attendance Management Recruitment Annual Property Return Digital Service Book Management. ACR Transfer & Promotion Claims
		Pension System	System to regulate pension payment, pension processing and update information from employee related to pension.	Pension Request Pension Approval AG integration

Application Type	Building Block	Solution	Functional Description	Required Functional Capability
				Pension Computation Request Pension Calculation PPO Number Integration Payment processing Reports
	Litigation Mgmt	Litigation Mgmt. System	The Litigation Management System would aim to record all litigation records of the departments and automate courts or other judiciary mechanism within the state	• Case Management • Contract Management • Document/ Content Management • Calendar & Scheduling • Fees & Charges • Profile Management • E-Filling of litigations • Payment of court fees • Virtual Court • Case Status • Court Orders • Case Search Advocate Search
	Grievance Management	Grievance Management System	The system to register and record grievance related to government services. The system must also have the capability to resolve grievances.	Lodge New Grievance Redressal workflow View Status Notifications Reminders SLA monitoring • Reports
	Monitoring & Evaluation	State Integrated Dashboard	The dashboard will enable progress of various government initiatives/schemes/programs.	Design new reports Connect operational database and data warehouse Design business intelligence enabled dashboards Integrate with State Service Bus
	Learning Management	Learning Mgmt. System	Learning management system is a system for the administration, documentation, tracking, reporting, and delivery of training courses, programs, or learning and development programs for all stakeholders of the state.	Upload learning content Create new learning calendar Assign learning activity to stakeholders Publish stored learning content Conduct digital tests Reports

Application Type	Building Block	Solution	Functional Description	Required Functional Capability
	Procurement Management	Procurement Management system	The procurement management system would enable tendering, procurement, vendor empanelment and various other procurement related activities in the system.	Self-certified Registration Catalogue Management Tender Creation/Publishing Publishing of corrigendum Bid Submission Contract Awards & Notification Order Placement and Fulfilment E-Bid/Reverse auction Demand Aggregation Payments Contract Management Reporting Vendor Assessment
Core Platform	Digital Identity	Authentication Gateway	The authentication system to validate and retrieve state digital ID	Validate ID from data Validate ID from biometric authentication OTP Validation Retrieve citizen data Store request/retrieve transactional data
	Digital Registry	State Data Hub	Centrally manage databases that uniquely identify and describe persons, service providers, facilities, assets, procedures, products, sites or other entities related to the organization	State Digital ID mapping Domain ID mapping Ease of retrieval
	Integration Management	Integration Platform	The integration platform would enable interoperability of internal systems through state service bus and API gateway for external integration.	Register new application service Choreograph several application services Ensure exchange of information with external systems Events routing
	Messaging	SMS Gateway	SMS gateway delivers notifications from systems to intendent recipients and transfers SMS to the backend application database using SMS Gateway APIs. The data can then be processed by the applications.	Store SMS templates Publish SMS Integrate with systems for data exchange

Application Type	Building Block	Solution	Functional Description	Required Functional Capability
	Geographical information	GIS Platform	A geographic information system (GIS) is a framework for gathering, managing, and analysing data. Rooted in the science of geography, GIS integrates many types of data. It analyses spatial location and organizes layers of information into visualizations using maps and 3D scenes.	Location based information processing Map and assign unique GIS ID to Government immovable properties Integration with remote sensing imagery for • Emergency operations • Infrastructure monitoring • Utilities • Transportation • Hydrography • Cadastral • Land use and cover • And several others
	Enterprise App Store	Enterprise App Store	The app store for all government mobile based services, apps, acts as an aggregator.	Aggregation of Government services in mobile device
	Payments	Payment Gateway	The State Government payment gateway that receives fund from digital channel through collaboration with agency banks.	Integration with banks Status reporting from banks Payment status notifications
	Security & Access	Single Sign On	Authentication and authorization of user requests for any system within the purview of Government of Meghalaya	Refer Single Sign On strategy in section 3.6.6
	Data Warehouse	Business Intelligence, Analytics and Data Warehouse	The capability to derive results from a large set of varied data, the capability would extend to derive business centric decisions from the data.	Technical product with flexibility to integrate with state system's databases, systems through API Execute analytical processing Derive business intelligence from analytics process results Perform data transformation, extraction and load in state data warehouse Store data in data marts

Application Type	Building Block	Solution	Functional Description	Required Functional Capability
	Workflow Management	Workflow Tool	The system provides capability to automate, measuring and optimizing business processes using tools	Business Process Analysis (BPA) capability - used to 'capture' process descriptions - so that they can be understood and analysed Design process models using low code feature Analyse process models Business Process Management capability - used to automate processes into working applications Implement designed business process model using low code feature Integrate with systems to implement necessary workflow
	Artificial intelligence & Block Chain	Chatbot, Block Chain	State chatbot to facilitate service application for the state, the chatbot would have artificial intelligence capability. Block Chain system would implement distributed ledger format that can be leveraged to support an array of government and public sector applications, including digital certificates, payments, land registration, identity management, supply chain traceability, health care, corporate registration, taxation and legal entities management.	Chatbot – AI supported response to service-related queries Service status query Service process queries Block Chain – Digital Certificate Land Registration Food Supply-chain
	Collaboration	Chat Platform	Enhance collaboration among employees by providing them easy to use chat platform, secured document sharing, secured group-based notification	Integration with employee database Integration with web contents, documents storage Centralized administration Security
	Consent Manager	Consent store and management system	System to store and manage citizens consent on information shared with the government	Store consent Integrated with SSO and Digital Identification gateway
	Data Quality Management	Data Quality Management	Quality management tool to assess data quality issues and address the same.	Data Quality Threshold Data Quality reporting Data quality actions and Status

Table 6: Application Architecture Building Blocks

Systems for the above set has been chosen based on secondary research and data provided NIC Meghalaya and NeGD.

Below is a tabular representation of common solution building blocks and core platforms listed above along with the (tentative) choice of systems along with the existing Business and Technical Owners of the chosen systems.

Application Type	Solution	Choice of System (Tentative)	Business Owner	Technical Owner
Common System	Financial Management	Integrated Financial Management System	Finance Department	NIC Meghalaya
	Land Record Management System	Meghalaya Computerized Land Record	Revenue & Disaster Management	NIC Meghalaya
	Content Management	Not Identified	Multiple Departments	Not Applicable
	Document Management System	e-Office	Finance Department	NIC Meghalaya
	Citizen Locker	DigiLocker	Various Departments	NeGD
	Service Provisioning	Service Plus	IT & C Department	NIC Meghalaya
	Project & Scheme Mgmt. System	Not Identified	Planning Department	Not Applicable
	HRMS	e-HRMS & MeghEIS	Finance Department	NIC Meghalaya
	Litigation Mgmt. System	e-Courts	Law Department	NIC
	Grievance Management System	MegPGRAMS	Administrative Reforms & Public Grievances	NIC
	M&E Dashboard	Not Identified	All Departments	Yet to be Identified
	Learning Mgmt. System	LMS	Various Departments	NeGD
	Procurement Management system	GePNIC & GEM	Multiple Departments	NIC Meghalaya
Core Platform	Digital Identity	Aadhaar Gateway	Planning Department	UIDAI
	Digital Registry			
	Integration Platform	State Service Bus, Bharat API, API Gateway	Finance Department	NIC Meghalaya
	Messaging Gateway	Meghalaya SMS Gateway, Email Gateway	Various Departments	NIC
	GIS Platform	NCoG	Various Departments	NeGD
	Enterprise App Store	Umang	Various Departments	NeGD
	Payment Gateway	GRAS	Finance Department	NIC
	Artificial Intelligence	Chatbot	Planning Department	Yet to be Identified
	Block Chain	Not Identified	Various Departments	NIC
	Security & Access	Parichay	Finance Department	NIC
	Data Warehouse (Analytics & BI)	To be Developed	IT & C Department	NIC Meghalaya
	Workflow Management	To be Developed	IT & C Department	NIC Meghalaya
	Data Quality Management	To be Developed	IT & C Department	NIC Meghalaya
	Collaboration	NIC SANDES	Various Departments	NIC
	Consent Manager	Not Identified	Yet to be Identified	Yet to be Identified
Cloud & SDC Infrastructure	Data Adaptors	As per Technology	IT & C Department	NIC
	Reporting	Not Identified	IT & C Department	Yet to be Identified
	Software Development Platform	OpenForge	IT & C Department	NeGD
	Software License Management	Not Identified	IT & C Department	Yet to be Identified
	Data Encryption Tools	Not Identified	IT & C Department	Yet to be Identified

Table 7: Building Blocks to System Mapping

The pictorial representation for of common solution building blocks and core platforms listed above along with the (tentative) choice of systems is as shown below:

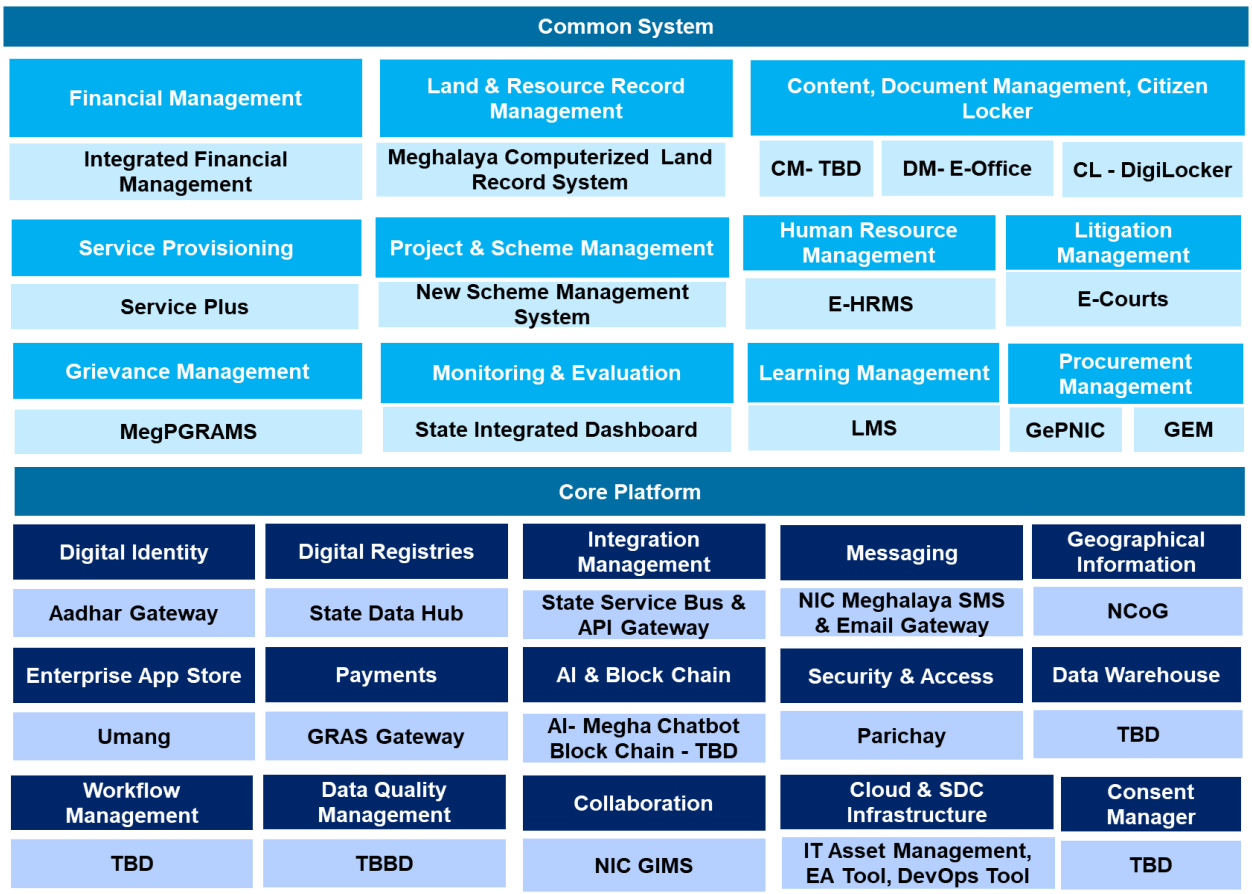


Figure 13: Common Systems & Core Platform Portfolio

3.3.4 Common Systems and Core Platform Readiness Assessment

Considering that many of the core platform components and common systems are planned to be procured or sourced from different organizations, there is a need for a maturity model that focuses on details of the technical aspects of information systems interoperability and met the requirements of MeghEA common systems and core platform.

The parameters of assessment are illustrated below:

Integrability

The solution **MUST** be able to integrate with any system of the State Government using APIs or web services. Different types of integration levels are as below:

- **Level 1**: The integration to other systems mainly happens through File, CSV or Manual mode.
- **Level 2**: The application has APIs or web-services developed to perform integration.
- **Level 3**: The integration to other systems mainly happens through REST APIs and there is detailed API documentation available for API integration.
- **Level 4**: The enterprise has APIs integration user interface

Scalability

The solution MUST be able to support the expected range of user, processing, and communications loads both initially and over time.

- **Level 1**: Load testing statistics are not available; but solution claims to cover user load.
- **Level 2**: The solution can support 75% of current peak user load.
- **Level 3**: The solution can support 100% of current peak user load.
- **Level 4**: The solution can support 100% of future(3 years) peak user load.

Reliability

The solution MUST be able to remain functional using failure recovery techniques, in alignment to the project team requirements.

- **Level 1** :No mean time to recover (MTTR) published.
- **Level 2**: MTTR> Application SLA.
- **Level 3**: MTTR~ Application SLA.
- **Level 4**: MTTR significantly less than Application SLA.

Modularity

The solution **SHOULD** provide a modular design that allows activation and deactivation of capabilities without disruption.

- **Level 1**: No modular design exists.
- **Level 2**: Components can be de-coupled and integrated.
- **Level 3**: The application has components that have independent APIs.
- **Level 4**: Micro-service architecture oriented/SOA with availability of registered service.

	Level 1	Level 2	Level 3	Level 4
Integrability	File, CSV, FTP, Manual entry	APIs/ Web Services	REST API + API Interactive docs	Integration UI Orchestration
Modularity	No modular design exists	Components can be de-coupled and integrated	Components have independent APIs	Micro-service architecture oriented/SOA with availability of registered service
Performance	The solution does not meet the desired criteria of response time	The solution occasionally meets the desired criteria of response time	The solution meets the desired criteria of response time	The solution meets desired criteria in low network bandwidth
Scalability	Load testing statistics are not available; but solution claims to cover user load	The solution can support 75% of current peak user load	The solution can support 100% of current peak user load	The solution can support 100% of future(3 years) peak user load
Reliability	No mean time to recover (MTTR) published	MTTR> Application SLA	MTTR~ Application SLA	MTTR significantly less than Application SLA

Figure 14: Core Common Platform Readiness Assessment

Basis the above integration assessment framework, all proposed systems are assessed under the framework to derive the final results. The proposed systems assessment results are as below:

System Name	Integrability		Modularity		Scalability		Reliability	
	Remarks	Level	Remarks	Level	Remarks	Level	Remarks	Level
iOBS	Few Web Services exist, no proper API documentation is available	2	System modules are tightly coupled along with the database as per design	1	Currently the application has no issues in supporting existing user base apart from Crystal reporting module	2	MTTR is not documented as no DR drills have been carried out in the recent past	1
TreasuryNET/ DivisionNET	Few Web Services exist, no proper API documentation is available	2	System modules are tightly coupled along with the database as per design. Application design is primitive	1	Application frequently faces issues due to legacy design or poor network, but no report of causal analysis exist that may point out the true cause of slow response	1	MTTR is not documented as no DR drills have been carried out in the recent past	1
Megh-GRAS	Web services exists, no proper API documentation is available	2	System has APIs for different key functions	2	No scalability issues reported; application's capability to handle future load is not documented	2	MTTR is not documented as no DR drills have been carried out in the recent past	1
State DBT	No web service exists	1	System modules are tightly coupled along with the database as per design	1	No scalability issues reported; application's capability to handle future load is not documented	2	MTTR is not documented as no DR drills have been carried out in the recent past	1
Meghalaya Computerized Land Record	No web service exists	1	System modules are tightly coupled along with the database as per design	1	Application may not support peak load, currently it supports only a fraction of the planned user base	1	MTTR is not documented as no DR drills have been carried out in the recent past	1
e-Office	24 web service exists in e-office, along with required documentation	1	Modules are available independently; however, no APIs exists to extract or transfer document files as per API documentation. This is a key challenge as e-office is the planned document and knowledge management tool	3	e-office does not have specific documentation on scalability but basis other larger states implementation findings, e-office seems to be scalable for Meghalaya Government	4	Cloud hosted instance may have scheduled maintenance timeline. No MTTR documentation exists	2
GePNIC	Web services exists but no documentation is provided	1	Modules are tightly coupled	1	Supports a large user base in several states	3	MTTR is not published	1
GEM	Web services exists but no documentation is provided	1	Modules are tightly coupled	1	Supports a large user base in several states	3	MTTR is not published	1

System Name	Integrability		Modularity		Scalability		Reliability	
	Remarks	Level	Remarks	Level	Remarks	Level	Remarks	Level
Service Plus	Several APIs exists and can be built in. No API documentation available	2	Modules are tightly coupled	1	No details provided; other similar implementation in states such as Haryana, Assam needs to be reviewed for any scalability issues	2	Cloud hosted instance may have scheduled maintenance timeline. No MTTR documentation exists	2
e-HRMS	Few APIs/web services exist	1	Modules are tightly coupled	1	No documentation has been obtained; the scalability depends on implementation planning	2	MTTR may vary basis implementation.	1
CPPS	Few APIs/web services exist	1	Modules are tightly coupled	1	As per information obtained from discussions with NIC Meghalaya stakeholders – system has no scalability issues.	3	MTTR may exceed SLA, no failure report has been obtained as there were no DR drill has been conducted in the recent past	1
MeghNPS	Few APIs/web services exist	1	Modules are tightly coupled	1	As per information obtained from discussions with NIC Meghalaya stakeholders – system has no scalability issues.	3	MTTR may exceed SLA, no failure report has been obtained as there were no DR drill has been conducted in the recent past	1
e-Courts	No APIs/web service exists	1	Modules are tightly coupled	1	Implementation in Meghalaya has been restricted to few district high courts only. System may have limited capability of handling peak user load post full scale implementation	2	MTTR may exceed SLA, no failure report has been obtained as there were no DR drill has been conducted in the recent past	1
MegPGRAMS	No APIs/web service exists	1	Modules are tightly coupled	1	Legacy system, may have scalability issues	1	Not assessed	1
LMS	No APIs/web service exists	1	Modules are available independently; however, no APIs exists to extract or transfer learning content files	3	No documentation has been obtained; the scalability depends on implementation planning	1	MTTR may depend upon implementation model	1
DigiLocker	Several APIs exists along with detailed documentation. REST APIs are supported	3	Modules are loosely coupled, with high integration capability	4	Currently supporting a user base of 1 Cr+, no scalability issues	4	Cloud hosted with zero MTTR	4

System Name	Integrability		Modularity		Scalability		Reliability	
	Remarks	Level	Remarks	Level	Remarks	Level	Remarks	Level
Meghalaya SMS Gateway, Email Gateway	APIs exists along with documentation	2	Not Applicable	4	No information found; this may depend on existing contract with NIC	1	MTTR is not reported	1
NCoG	APIs exists along with documentation. REST APIs are supported	3	Modules are loosely coupled, with high integration capability	4	No information obtained	1	MTTR is not reported	1
Umang	APIs exists along with documentation. REST APIs are supported	3	Not Applicable	4	Not applicable as this would act as an aggregator	3	MTTR is not reported	1
GRAS	Few APIs/web services exist	1	Modules are tightly coupled	1	No information obtained	1	MTTR may exceed SLA, no failure report has been obtained as there were no DR drill has been conducted in the recent past	1
OpenForge	Few APIs/web services exist	1	Not Applicable	4	Not applicable as this would act as an DevOps platform with limited user base	4	Not applicable	4

Table 8: Proposed Systems Assessment Results

The graphical representation of the system assessment is represented below:

Figure 15: System Assessment

3.3.4.1 Recommendations

1. iOBS, TreasuryNET, DivisionNET has several functional and technical gaps, these systems are NOT fit for purpose. Instead an Integrated Financial Management System has been proposed as per Finance Solution Architecture assessment
2. Meghalaya Computerized Land Record System needs business functional and architecture enhancement
3. E-Office may not meet requirements of Document Management or Knowledge Management system. Detailed analysis is required to arrive at a conclusion. There are multiple systems adopted by different states , Government of Meghalaya must execute necessary due diligence covering Government of India notification, e-office re-architecture possibility and evaluation of other systems before adoption
4. Service Plus would be the Service provisioning system, Workflow component (part of core platform) would require COTs product, Service Plus is not fit for purpose of a Workflow platform.
5. Grievance Management system needs to be re-developed as the current system is not considered fit for purpose.
6. e-HRMS system needs detailed architecture review before adoption is planned.
7. Land Record system needs replacement/re-architecture.

8. Proposed systems – Parichay has not been assessed as there are no documentation available. There is a need for detail assessment before adoption.

3.3.5 Application Architecture: Future State

The future state of application architecture comprises of several modules under each pillar, while each module enabling one or more services. These services would be initiated from the module interface however would require one or more common and core systems to work in order to deliver a whole of service experience.

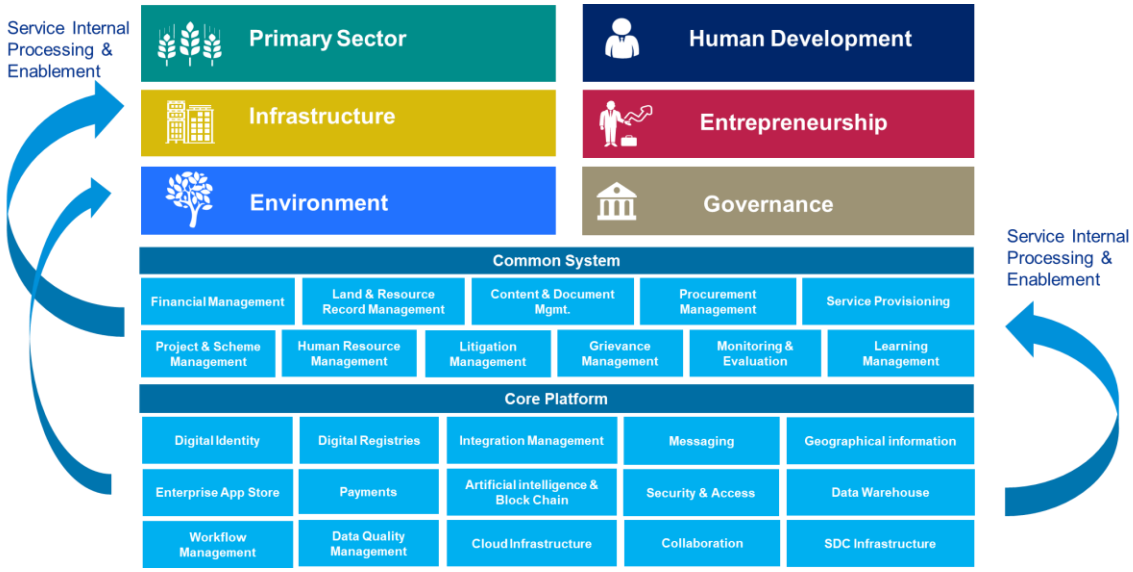


Figure 16: Application Taxonomy

Primary Sector

The Primary Sector system would include functions to cater all prioritized business services :

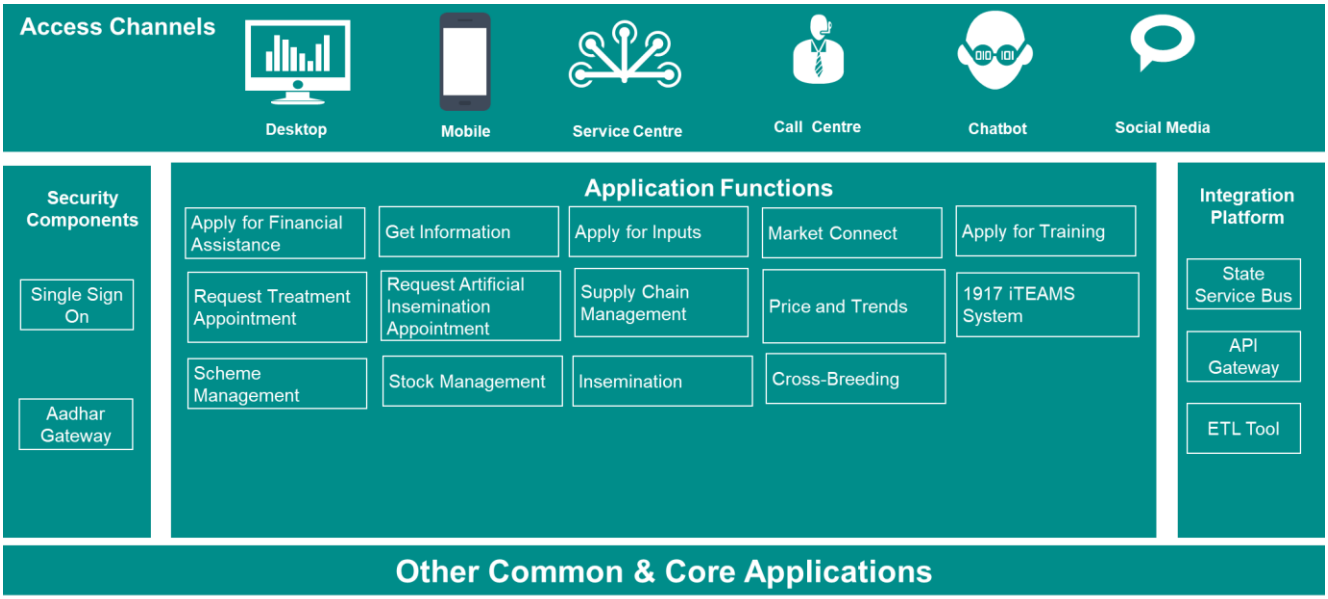


Figure 17: Primary Sector – Application Functions

Please refer Detailed Architecture - Primary Sector Document – " Application Architecture: Future State" for details about each of the above functions

Human Development

The Human Development system would include functions to cater all prioritized business services :

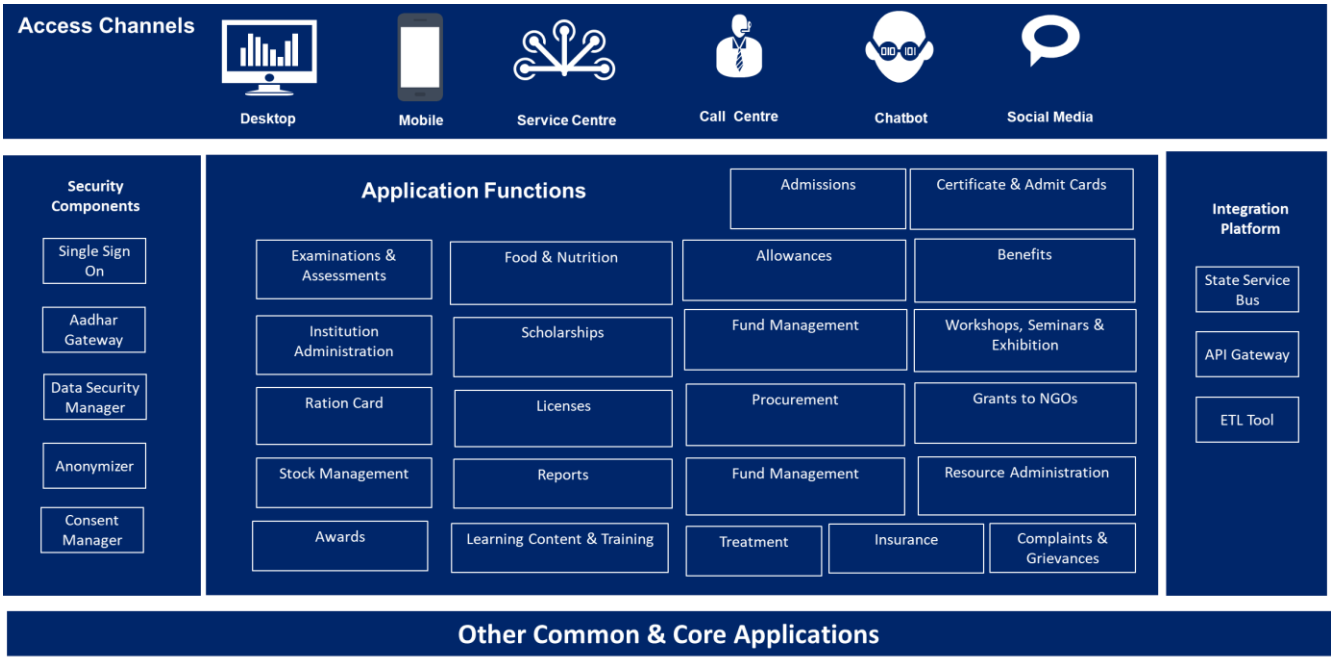


Figure 18: Human Development – Application Functions

Please refer Detailed Architecture – Human Development Document – " Application Architecture: Future State" for details about each of the above functions.

Infrastructure

The Infrastructure Sector system would include functions to cater all prioritized business services :

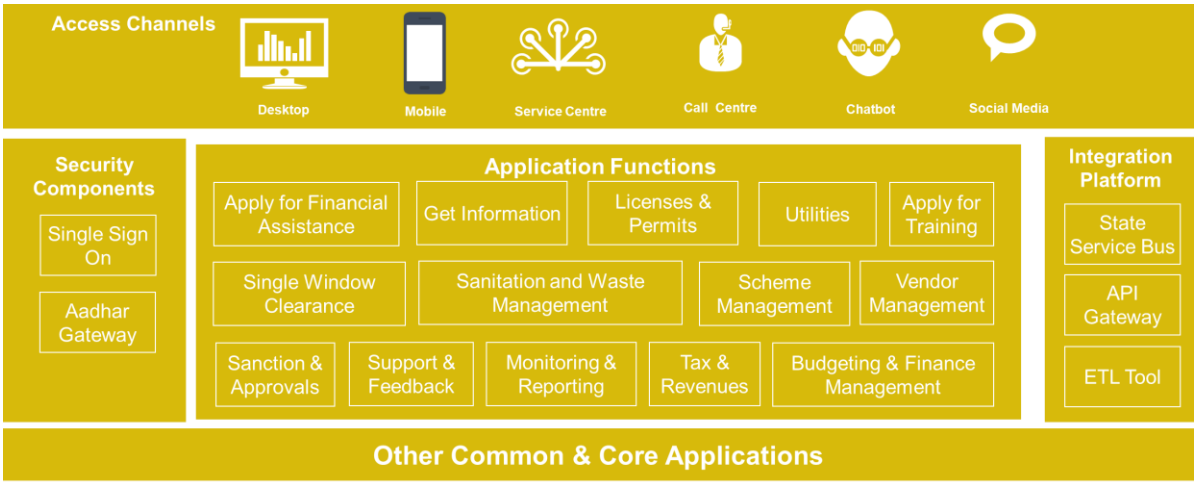


Figure 19: Infrastructure Development Application Functions

Please refer Detailed Architecture – Infrastructure Development Document – " Application

Architecture: Future State" for details about each of the above functions.

Entrepreneurship: The Entrepreneurship sector system would include functions to cater all prioritized business services :

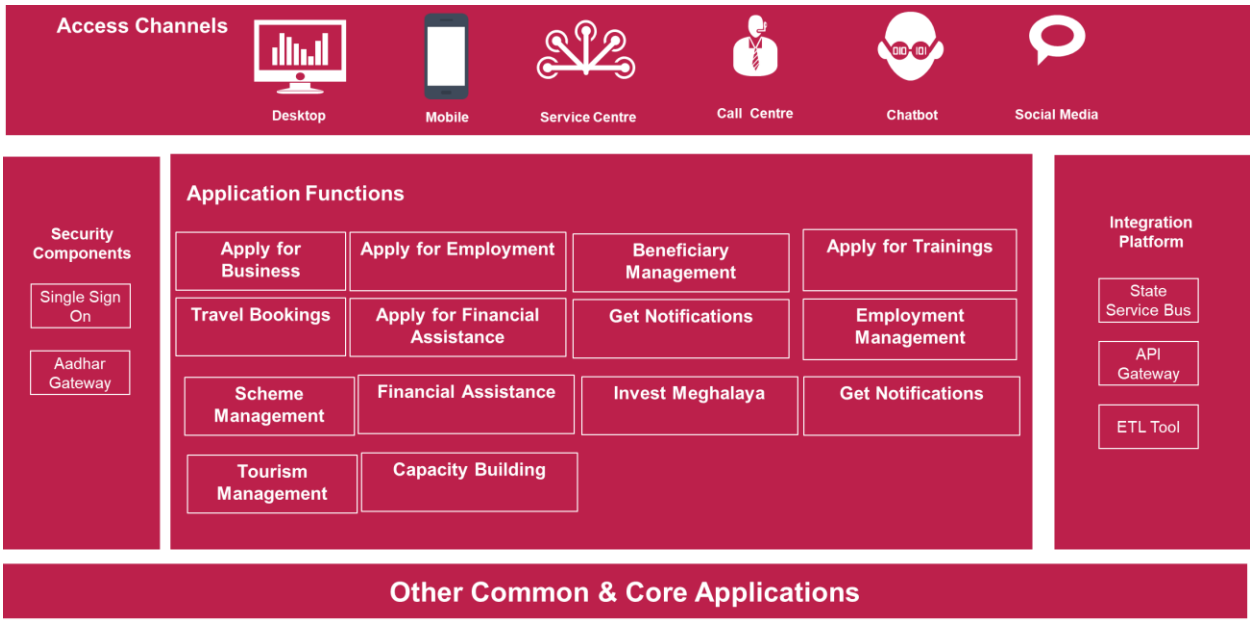


Figure 20: Entrepreneurship Pillar – Application Functions

Please refer Detailed Architecture - Entrepreneurship Document – " Application Architecture: Future State" for details about each of the above functions

Environment

The Environment pillar system would include functions to cater all prioritized business services :

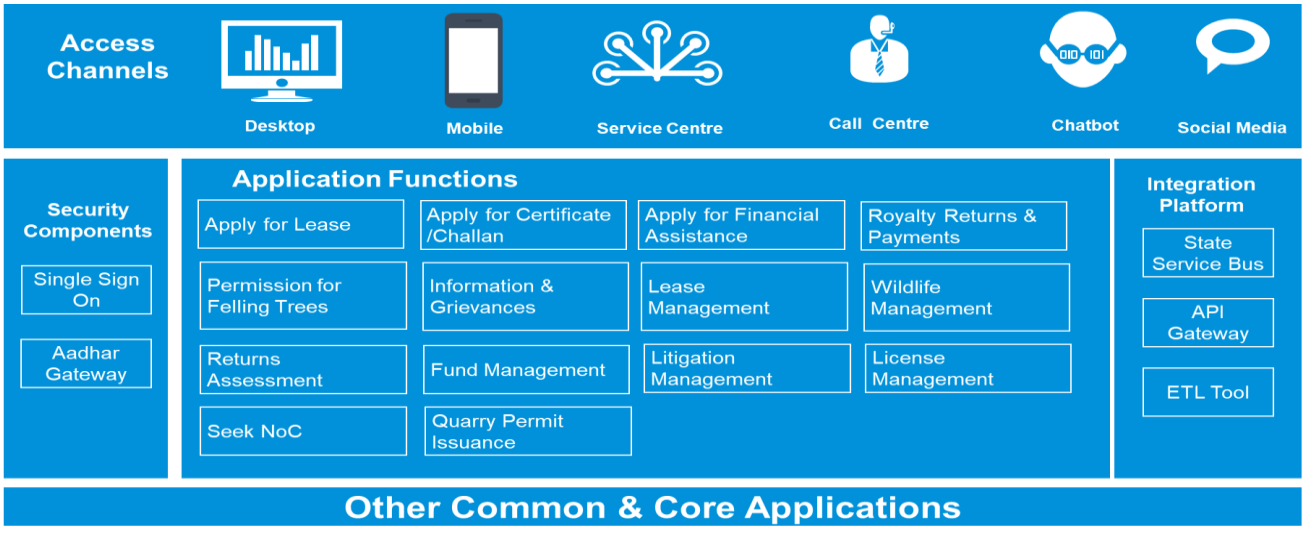


Figure 21: Environment Pillar – Application Functions

Please refer Detailed Architecture – Environment Pillar Document – " Application Architecture: Future State" for details about each of the above functions.

Governance

The Governance pillar system would include functions to cater all prioritized business services :

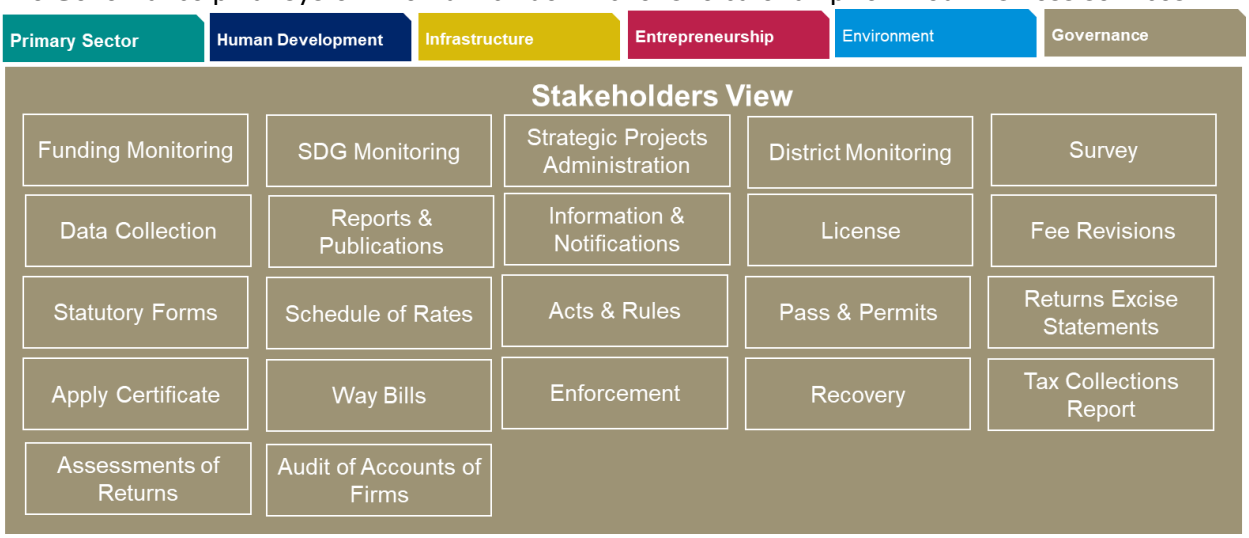


Figure 22:Governance Pillar – Application Functions

Please refer Detailed Architecture - Governance Document – " Application Architecture: Future State" for details about each of the above functions

3.3.6 Application Transformation Plan

Basis study of business architecture and the derived business transformation plan, it is evident that few of these systems needs to be re-architected while few would need to be decommissioned as proposed system would subsume the application service.

Following categories of changes are planned for the applications:

1. **Business Functionality Addition/Elimination**: This would be applicable for systems which have limited capability, existing functionality would be transferred to existing/ new system to ensure better service delivery or new functionality would be added to enhance service delivery
2. **Application Architecture Enhancement**: The application may have been supporting critical functionality with low technical fitment. It is imperative that the application needs to be modified to incorporate necessary architecture enhancement.
3. **Decommission**: Systems that have duplicate or redundant functionality would be decommissioned to rationalize the portfolio and enhance efficiency.
4. **New Introduction**: System to be added in the portfolio to facilitate digital delivery of services, the functionality of the system would be new to the application portfolio.
5. **Re-Interface**: Provide a citizen centric interface and integrate the external system from existing portal

Basis gap assessment study and analysis, below table represents the plan:

Application Name	Business Functionality Addition/ Elimination	Application Architecture Enhancement	Decommission	New Introduction	Re-Interface
Primary Sector System				✓	

Application Name	Business Functionality Addition/ Elimination	Application Architecture Enhancement	Decommission	New Introduction	Re-Interface
1917iTeams System	✓				
Meghalaya Agri Board		✓			
Farm Mechanization			✓		
Farmers Registration			✓		
Soil Health Card					✓
AgMarknet					✓
PM ✓Kisan					✓
Human Development System				✓	
Megha Health Insurance Scheme Portal (mhis.org.in)			✓		
e-Hospital (http://ehospital.gov.in/)		✓			
UDISE Plus					✓
Mid-Day Meal Automated Reporting and Management System					✓
Teachers Information System (TIMS)	✓	✓			
National Scholarship Portal					✓
Rapid Reporting System of ICDS (MIS for ICDS)					✓
Computerized Disability Certificates					✓
Track CHILD 3.0					✓
ePDS	✓	✓			
End-to-End Computerization of TPDS			✓		
MegFEAST (Food & Essential Commodities Assurance & Security Target)			✓		
Existing Ration Card Management System (ERCMS)		✓			✓
Stakeholder Identity Management System (SIMS)		✓			✓
Depot Code Management System (DCMS)		✓			✓
Anna Vitran					✓
Meghalaya Board of School Education		✓			
Merit List of Students undergoing MBBS, BDS and other Allied Courses			✓		
Infrastructure System				✓	
NSAP					✓
Vahan					✓
Sarathi					✓
Entrepreneurship System				✓	
Mesmerizing Meghalaya Portal (Tourism)	✓	✓			

Application Name	Business Functionality Addition/ Elimination	Application Architecture Enhancement	Decommission	New Introduction	Re-Interface
Invest Meghalaya Portal	✓	✓			
Labour & Community Development	✓	✓			
Pradhan Mantri Khanij Kshetra Kalyan Yojana Portal					✓
Governance System				✓	
Mining Tenement System		✓			
Mother App		✓			
Planning Department Portal			✓		
MIS			✓		
VAT (e-return)		✓			
Computerized Value Added Taxes (e-Registration)		✓			
VAT (e-c form)		✓			
VAT (e-amendment)		✓			
DM Dashboard		✓			
Integrated Budget Information System (iOBS)	✓	✓			
TreasuryNET	✓	✓			
Megh-e-billing			✓		
DivisionNET			✓		
Central Pension Payment System		✓			
MeghNPS		✓			
MeghEIS (Meghalaya Employee Information System)		✓			
GRAS (Government Receipt Accounting System)		✓			
State DBT	✓	✓			
Integrated Financial Management System	✓	✓			

Table 9: Applications Transformation Plan

3.3.7 Application Communication Model

The future state application communication model would not be based on point to point integration rather be enabled by State Integration platform. The interaction and communication between components are across the platform, which has a similar function as a physical computer bus to handle data transfer or message exchange between services without writing any actual code.

Follow the below table for detailed description of the integration functionality:

Feature	Description
Virtualization	Virtualization is about using tool that creates a virtual copy of production APIs/services, this can be used for testing and development purpose. Virtualization would not mean mocking, the virtualized APIs will not be context-specific, or a specific behavioural response specific to fulfil a certain development need at a certain time.

Feature	Description
Transformation	Data Transformation is the processing of data from one format, such as XML or SOAP, or even currencies and time formats, into another such as REST. It needs to have bi-directional transformation (for example, REST-to-SOAP, XML-to-JSON, and HTTP-to-JMS) capability
Routing	Routing capability of a messaging system is used to fundamentally connect different message channels. A router consumes a message from one message channel (as an example TreasuryNET) and republishes it to a different channel based on specified conditions (Service Plus Mobile App)
Orchestration	Orchestration or Choreography capability is for coordination of application service request, when multiple application service requests would lead to a single outcome
Load Balancing	Capability needed to load balance API calls among the API gateways in a cluster to optimize the utilization of gateway resources
Error Handling	Ability to handle error, provide incoming requests a desired business response in case of an error, also to enable retry for initial failures
Throttling	Capability to manage steady-state rate and burst rate to manage API traffic

Table 10: Application Integration Platform Features

Read below matrix considering the following:

Application Service Provider : Applications that provides information post processing the information through specified business logic

Application Service Consumer – Applications that consume services in the form of information from other applications.

	Application Service Provider									
Application Service Consumer	Strategic Pillar/Cross-Cutting Pillar Modules	Financial Mgmt. System	Communication Tools	Procurement System	Service Plus	HRMS	M&E System	DigiLocker	Chatbot	Single-Sign-On
Strategic Pillar/Cross-Cutting Pillar Modules	Refer Business Interaction Matrix	Scheme status & funding Payment Status	Email/SMS based Service Request	Procurement Status Stock Fulfilment	Service Status Service workflow	Service Resolution Officer	Threshold Parameters	Issued Certificates	Service Request Service Number Requestor ID	Identity Authority
Financial Mgmt. System	Digital Bills Bank Account of Beneficiary Revenue Amount			Vendor Account Details	Payment Request Details	Salary Bill Allowance Payment details	Target Revenue		Pension Request ID PPO Number Service Request ID	Identity Authority
Communication Tools	Email ID Mobile Number (SMS)	Email ID Mobile Number (SMS)		Vendor Email Vendor Phone No.	Email Content Email ID SMS Content Mobile No	Email Content Email ID SMS Content Mobile No		Issued Certificate Metadata Aadhar Number	Email Content Email ID SMS Content Mobile No	Registration Details
Procurement System	Stock Requirement Tender Payment Details	Payment Status			Stock Requirement	Stock Requirement			Tender Status Payment Status	Identity Authority
Service Plus	Service Details Service Data Stock Information	Service Details Service Data Budget Funding		Tender Status Approved Vendor List Stock Information		Employee ID Employee Details Salary Information		Issued Certificate Metadata	Service Name Application Form data	Identity Authority
HRMS	Service Actor Requirement	Salary Status			Service Status			Issued Certificate	Service Request Details	Identity Authority
M&E System	Dashboard Data	Financial Data		Procurement Status and Other data	Service Status, Number of service requests	Employee related data		Certificate stored		Identity Authority

	Application Service Provider									
Application Service Consumer	Strategic Pillar/Cross-Cutting Pillar Modules	Financial Mgmt. System	Communication Tools	Procurement System	Service Plus	HRMS	M&E System	DigiLocker	Chatbot	Single-Sign-On
DigiLocker	Issued Transcripts, Certificates, NoC, Licenses			Quality Certificate	Aadhar Number Citizen Consent	Aadhar Number Employee Consent				Aadhar Number
Chatbot	Information Services	Service Metadata		Procurement Status Stock Fulfilment	Service Status Service workflow	Employee related data				Identity Authority
Single-Sign-On	User Authority data	User Authority data								

Table 11: Application Communication Matrix

3.4 MeghEA: Data Architecture

Data is an asset and a key to provide services to the stakeholders in the state, the true realization of the value of data and its management is probably the most important differentiator in providing best in-class services to stakeholders. Data architecture defines boundary less information flows within and across departments and external agencies, and how they are controlled. In other words, it **Connects** all departments at data layer, facilitates increased **collaboration** among departments/agencies keeping security and technical requirements of individual data elements so that they are implemented and managed appropriately.

MeghEA Data Architecture defines the data entities, their interactions with each other, and their value in delivering government services.

The goal of data architecture is to introduce structure, control and consistency to the fragmented data landscape found in State Government Departments. This section describes the data architecture of MeghEA:

- List out the current data entities that are used.
- The data architecture building blocks.
- Key finding and recommendations.
- The Future State data architecture.

3.4.1.1 Key Concepts

- **Digital Data Resource:** A Digital Data Resource is a digital container of information. A Digital Data Resource may correspond to three types of data: "Structured Data Resource", "Semi-Structured Data Resource", and "Unstructured Data Resource". It acts as a container for the metadata about the data resource.
- **Structured Data Resource**: Structured Data Resource is a type of Digital Data Resource containing only structured data. A Database Schema is used to define/describe a Structured Data Resource, it is that data that is highly organized and easily understood by machine language.
- **Semi-Structured Data Resource**: A Semi-Structured Data Resource is a Digital Data Resource containing semi-structured data. A Semi-Structured Data Resource contains partly structured and partly unstructured data.
- **Un-structured Data Resource:** An Unstructured Data Resource is a type of Digital Data Resource that contains only unstructured data. Unstructured data is collection of data values that are likely to be processed only by specialized application programs.
- **Conceptual Data Model:** The conceptual data model represents the overall structure of data required to support the business requirements independent of any software or data storage structure.
- **Metadata :** Metadata is data about data, it defines and describes data or information. Metadata is the structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource.
- **Data Taxonomy:** Data Taxonomy is a collection of data definitions that organized into a hierarchical structure. Each term in taxonomy is a topic. Taxonomy provides a means for categorizing or classifying information in a domain of discourse (invariably a department in

the Government). Each term/topic in taxonomy is related to one or other terms/topics in the taxonomy in a parent child relationship.

3.4.1.2 Key Definitions

- **Entity:** An Entity is an abstraction for a person, place, object, event, or concept described (or characterized) by common Attributes. For example, "Employee" and "Department" are Entities. An instance of an Entity represents one occurrence of the Entity, such as a specific employee or a specific department. An entity has one or more attributes. An entity may have relationships with one or more entities.
- **Data Stewards:** A data steward are department/sector experts in their respective data domains and responsible for monitoring compliance to MeghEA data management policies and standards, addressing data related issues and governing data belonging to their data domain. Data Stewards also play a critical role in data standardization and metadata definition tasks.
- **Data Custodian:** Data custodian is the agency that is delegated the role to manage the data (e.g. Information Technology Authority and 'Establishment' data).
- **Data Models:** A data model is an abstract model that organizes elements of data and standardizes how they relate to one another and to the properties of real-world entities.

3.4.1.3 Key Principles

- ✓ **DP1-Data-sharing**
- ✓ **DP2-Data asset**
- ✓ **DP3-Data Trustee**
- ✓ **DP4-Data Privacy and Security**
- ✓ **DP5-Common Vocabulary and Data Definitions**

Refer annexure on Data Architecture Principles for details around each of the principles

3.4.1.4 Standards

Below is the list of standards that needs to be followed for all data acquisition, ingestion , provision, consumption and integration

Standards Code	Standards	Recommendations
DS.1	**Metadata and Data Standards** Refer Metadata section .	State-wide Metadata standards have been illustrated in section 3.4.3
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 classification of data elements based on Open Group Framework – O-DEF.	Refer data.gov.in for data catalogues 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

Table 12: Data Standards

3.4.2 Data Entities

The data architecture capabilities of MeghEA have been mapped to the framework to provide an overview of the system capabilities in place and that need consideration in future. The Framework is divided in to three bub layers.

Data to Information: Data is the unprocessed facts that we capture according to some agreed-upon standards with stakeholders. The data captured via different departmental or central applications is further analysed in order to understand the information and draw conclusions. Those conclusions lead to actions that can be facts for KPIs or indicators or to further improve the service delivery to stakeholders.

Data Processes: The layer includes various processes, mechanisms and frameworks to manage the information and its governance.

Data Objects: The objects of a data model such as citizen name or address. Entities are containers for attributes and relationships between objects. Data entities are the properties inside a data object.

Figure 23: Data Architecture Capability Framework

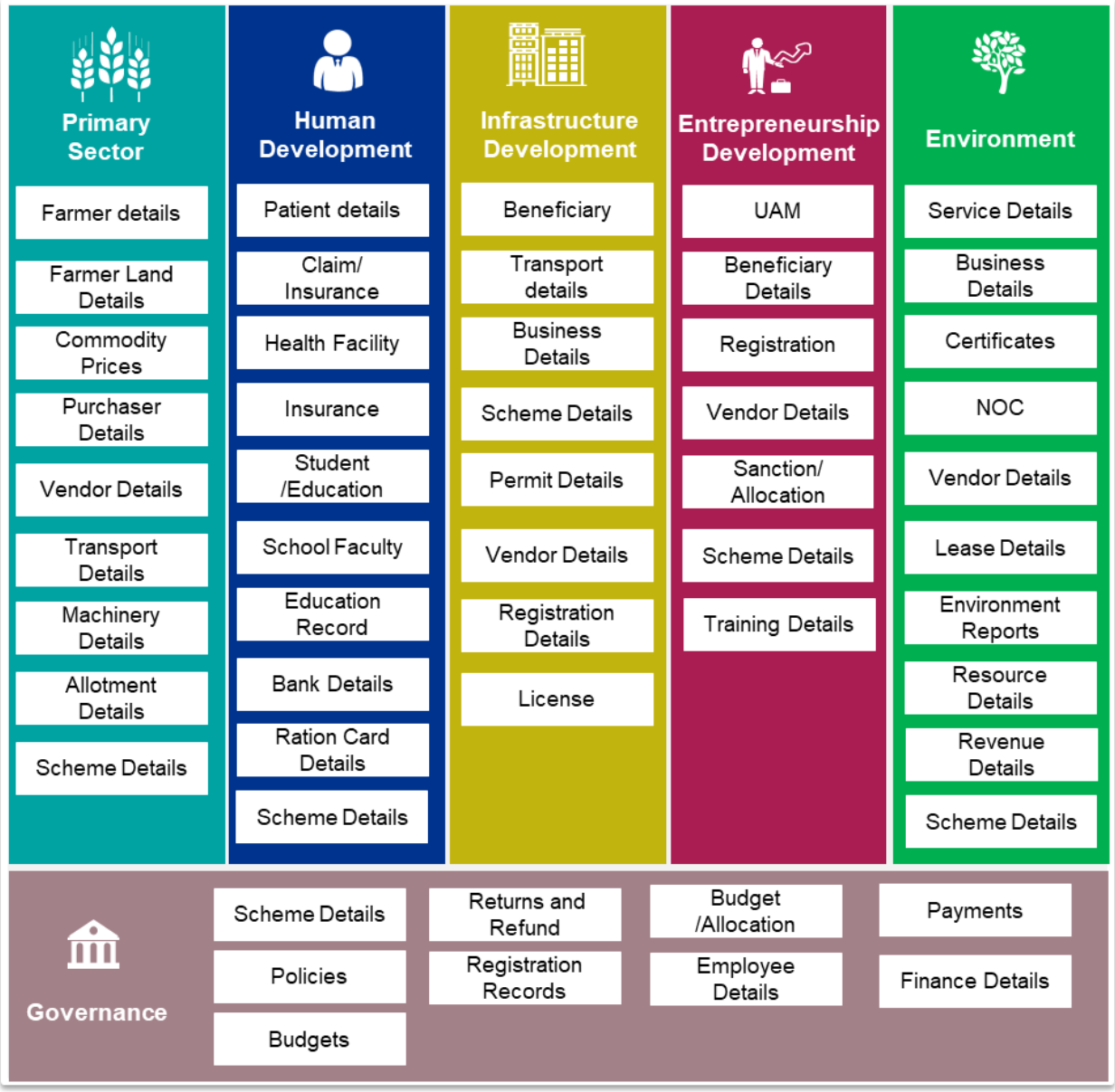


Figure 24: MeghEA Data Entities

3.4.3 Metadata Data

Metadata has been defined as "data describing the context, content and structure of records and their management through time". Metadata is logically separate from the resource it is about, even when embedded within the resource. "Metadata" consists of data elements and values for data elements description and discovery (access, retrieval): data elements that connect users to information resources in a structured, controlled way.

MeghEA: 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 MeghEA, a similar model is planned to be adopted- Minimal Data

Elements.

A minimal set of metadata elements would be designed in MeghEA at the statewide level, while each pillar would have the mandate to follow the model and the flexibility to augment the model as and when required.

Statewide Minimal Metadata Elements

The MeghEA Metadata Structure defines the metadata elements, it also defines the reference metadata to be collected or reported by specifying the concepts required, how these relate to each other, their presentational structure and to 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 (Refer MeghEA Data Classification).
- **Contact Information** – Identification and means to communicate with persons or entities associated with the data.

Metadata Standards

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

Operating Model

The below is the typology of metadata standard along with the statewide standards. The agencies under Government of Meghalaya has to adopt the statewide standards or has to seek architecture exception for adoption. The agencies may add any standard basis , specific need of the domain.

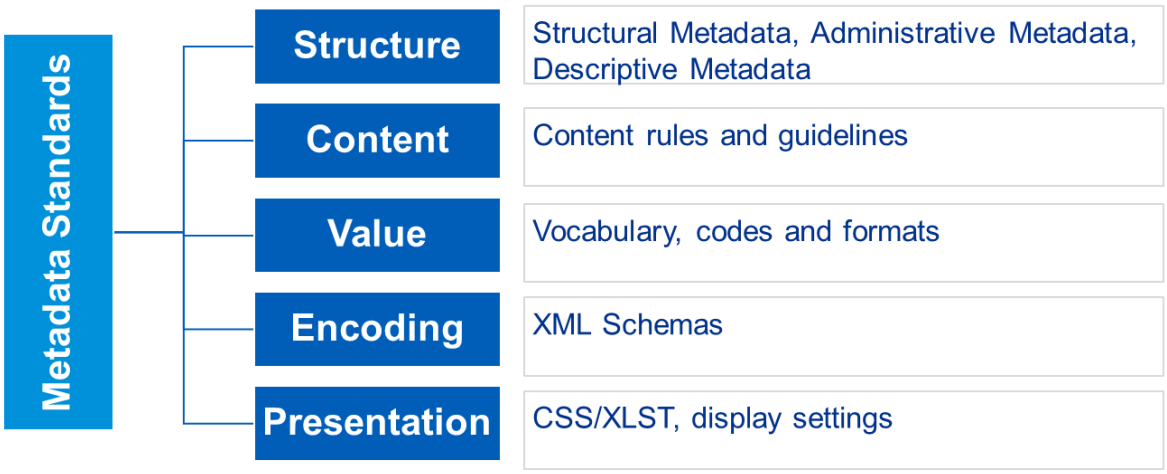


Figure 25: MeghEA Metadata Typology

Structure related Standards

Standard	Mandatory/Optional	Reference Link	Remarks
MeghEA 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	Mandatory	https://ddialliance.org/explore-documentation	Applicable for surveys and other observational methods in the social, behavioural, economic, and health sciences

Table 13: Metadata Structure - Standards

Content related Standards

Standard	Mandatory/Optional	Reference Link	Remarks
National Spatial Data Infrastructure (NSDI) standards	Mandatory	https://nsdiindia.gov.in/nsdi/nsdiportal/images/NSDI MetadataDocument.pdf	Applicable for GIS data definition and exchange format

Table 14: Metadata Content - Standards

Value related Standards

Standard	Mandatory/Optional	Reference Link	Remarks
Local Government Directories	Mandatory	GoI LGD - https://lgdirectory.gov.in/	Applicable for districts, blocks and villages
Agency Codes	Mandatory	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 15: Metadata Value - Standards

Encoding related Standards

Standard	Mandatory/Optional	Reference Link	Remarks
MeghEA Encoding and Transmission format	Optional		Need to define , please refer - http://www.loc.gov/standards/mets/
Extensible Markup Language (XML)	Optional	https://www.w3.org/XML/	

Standard	Mandatory/Optional	Reference Link	Remarks
XML Schema for Generic Data Elements: Specific to Land Region Codification	Mandatory	http://egovstandards.gov.in/xml-schema-for-generic-data-elements-lrc	This standard is aligned with LGD

Table 16: Metadata Encoding - Standards

3.4.4 Data Architecture Building Blocks

For data architecture, building blocks realize capabilities and are the basic elements to design and build data architecture. The data architecture building blocks are defined considering minimalistic approach – to include only those building blocks which are mandatory for the Government of Meghalaya. The building blocks are further arranged to following categories:

- **Data Ingestion:** Accessing and collecting data sources through a variety of channels (for example API, web questionnaires, administrative archives, streaming data, etc.) remain the first step of data production process. The data received from different resources includes,
    - Loading data into a data storage (for example relational database, NoSQL, big data storage, etc.).
    - Connecting the metadata management capability to capture the relevant information about the ingested data.
    - Managing the relationship with data providers (for example respondent management and Service Level Agreements for administrative data sources).
- **Data Transformation:** This involves transforming data in a format that is (re-)usable for the provisioning capability. The capability of building block includes,
    - Cleanse data to conserve internal coherence and consistency of data, check the data coming from metadata system used in the department across.
    - Data harmonization with classifications coming from data standards.
    - Reduce the amount of data, filtering rows and selecting columns.
    - Alter the data following security or statistical significance reasons.
- **Data Integration:** Data integration is a key building block of the target architecture supporting ability to fulfil information needs from different and existing sources.
    - Metadata-driven (schema-driven) data discovery within and across sources.
    - Data mash up and blending of heterogeneous sources (dataset, relational data bases, Linked Open Data, etc.) using different techniques.
    - Access and connection to sources APIs independently from their location (local/remote/cloud environments).
    - Agile acquisition/processing and delivery data workflows with automation / batch features.
    - Agile data modelling and structuring allowing users to specify data types and relationships.
- **Data Provisioning:** The building block can make data and metadata available to Authorized internal and external users and processes. The required capability is:
    - Metadata-driven access to data sets, for example APIs or through a data catalogue.
    - Providing direct access to data through data analysis tools or APIs or query languages.
    - Access and disseminate data using open standards.

- **Data Governance:** This involves clean-up of input data, life-cycle management of data, metadata management, and most importantly security of data. Data Governance requires following building blocks.
    - **Data Life-cycle Management:** The ability to manage the life cycle of data through the implementation of policies, processes and rules in accordance with the Government of Meghalaya's strategic objectives.
    - **Data sharing:** Data dissemination is the distribution or transmitting of GoM, or other, data to users or National Government or Open Data repository. The exchange of data should preferable be done using open standards.
- **Security and information Assurance:** Security and Information Assurance includes granting security and continuity to the information system, and will provide the following controls:
    - Granting access to authenticated and Authorized users and successfully deny access to all others.
    - Applying security to data in transit and at rest, to an appropriate level in line with the relevant official security classifications and Privacy Impact Assessments (if applicable).
    - Ensuring the preservation of the integrity and availability of data.
    - Ensuring the business continuity of the system, putting in place the capability to overcome temporary problems and ensuring the availability of alternative sites in the event of a disaster.
    - Protecting user privacy and use of data encryption techniques where applicable.

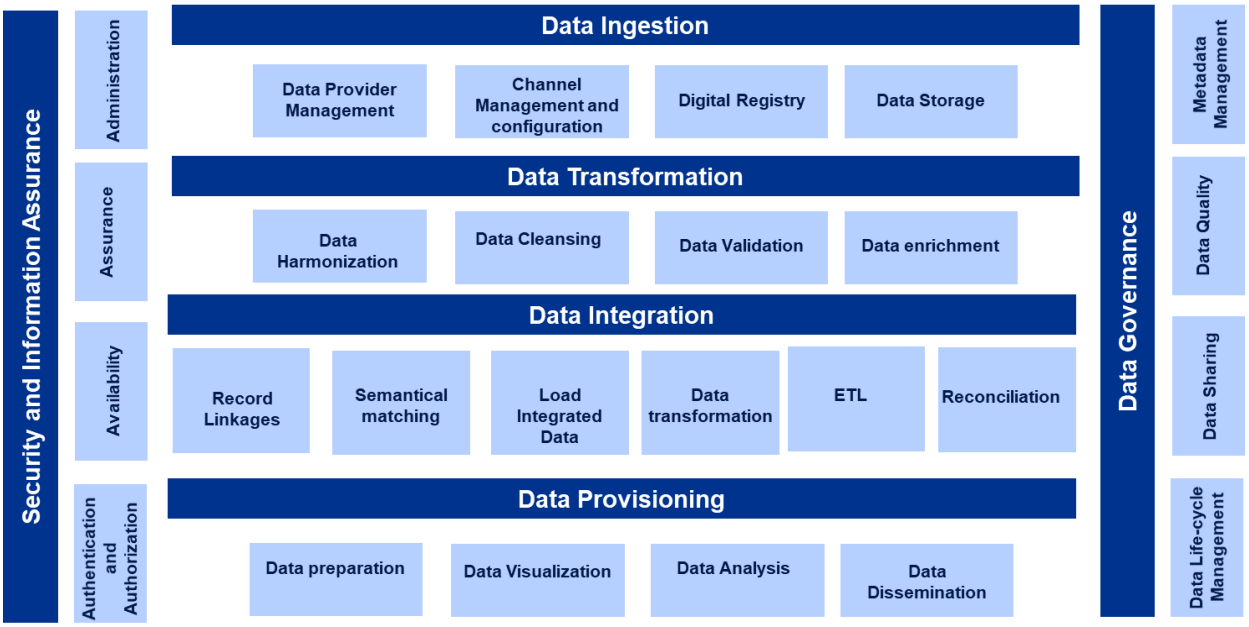


Figure 26: Data Architecture Building Blocks

3.4.5 Data Architecture: Future State

The Future State representation of MeghEA Data architecture comprises of following components

- **Data Transformation**: GoM departments would be enabled to process data in various forms (XML, JSON, Fla File, etc.) from multiple sources.

- **Digital Identity**: Aadhaar and GSTN would be used to create login for the citizens. This ID would be used for access to all Sector services.
- **Data Extraction**: Extraction of data from relational databases to data warehouse for easier and efficient reporting.
- **Data Storage**: Storage, load and design of relational data base for transactional and analytical processing.
- **Data Analysis**: Data analysis would be enabled by both system level processing and business intelligence and data warehousing tools.
- **Data Visualization**: All departments need tools to visualize data analysis through Business Intelligence, MeghEA State-wide architecture would include such capabilities.
- **Data Retention**: Data retention policies needs to be revamped to include necessary retention requirements.
- **Data Life-cycle Management**: Data life-cycle management would include necessary and specific requirements of the sector; however, it would be aligned to MeghEA data life-cycle management.
- **Data Dissemination**: Data dissemination of public data as classified in data classification model, needs to be shared with Government of India or Open Data repository.
- **Data Authentication & Authorization**: The substantiation of the identity, definition and enforcement of permitted capabilities of a user related to the department or system in some way.
- **Metadata Management**: Departments participating under Human Development Sector would contribute to the metadata repository for data that are classified under their ownership.

The various tools and technology required as per MeghEA data architecture and relevant to state-wide implementation are illustrated below:

Tools	Description
Metadata Repository	Metadata is data that is describe and characterise other data, answering the 'who', 'what', 'when', 'where', 'why', and 'how' about the data set that is being described. Metadata repository software would provide the following capabilities: • An embedded repository • Analysis tools
Data Modelling Tools and Repository	The data modelling tools enable easier and sophisticated data modelling for data design. Development and maintenance of Conceptual, Logical and Physical data models would be enabled by this software. The repository used to store this model would be called as Data Model Repository.
Open Data Catalogue	The catalogue is a repository of data that are exposed as part of the open data policy of the Government. Departments respective pillars needs to incorporate the open data from existing data(operational), post which the catalogue would be operational.
Data Governance Tool	The tool required to perform various key functions such as data quality checks, data access audit, etc. Data Security Manager would also be needed to store data at flow information, what data(of citizen) has been shared with whom. Refer "Human Development" Detailed Architecture Requirements document for details
ETL Tools	To automate data integration and transformation operation, through transferring data from operational store to data warehouses. Departments in Human Development Sector would need such a tool to perform is data warehouse operations.
Data Clean up tools	Data cleansing or data scrubbing is a process for removing corrupt, inaccurate or inconsistent data from a database. Regular data-cleansing corrects records containing typographical mistakes, or other errors. Departments in Human Development Sector need the tool to eliminate such erroneous data to

Tools	Description
	facilitate accurate reporting.
Data Encryption Tool	As part of MeghEA, encryption tool is required to enable efficient and secured data sharing. Data classified as confidential, would need such encryption before being shared.
Master Data Management	MeghEA master data management tool would store the digital registry data and other data hub for centralized access for all departments.
Data Warehouse	Data warehouse (DW) is a key component in data architecture to enable effective reporting and decision making. Data Warehouse would be required to keep all the data and reporting purpose. This would also include Business Intelligence and data analytics capability

Table 17: Tools and Technologies

Below is a diagrammatic representation of the core data entities along with the identifying data attribute for each data entity. The diagram also illustrates the relationships between state Digital ID and the corresponding data entity's identifier. The various tools proposed to be used under Data Architecture is also illustrated.

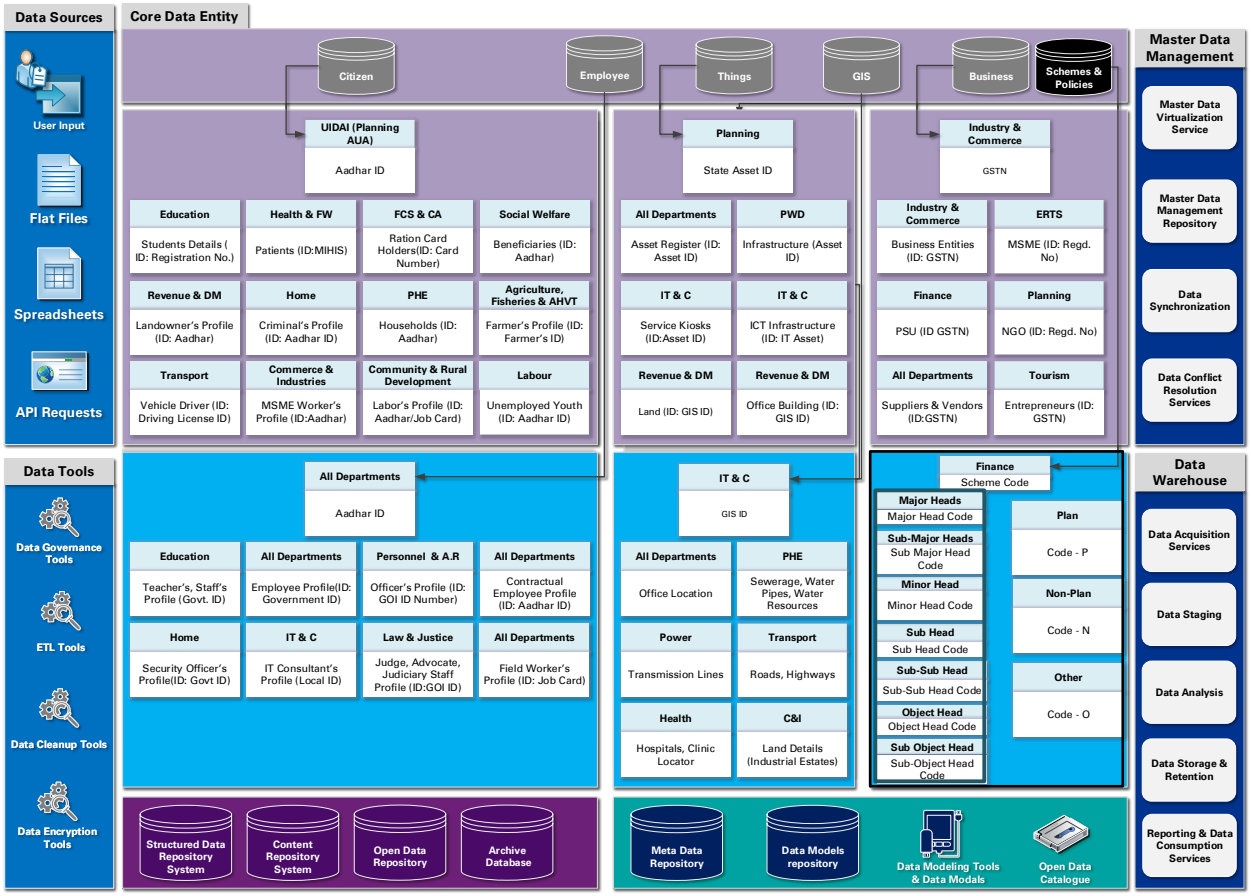


Figure 27: Future State Data Architecture

The above diagram illustrates digital registries in the centre , while all tools and component on the periphery

Data Hub: The data hub for MeghEA comprises of Master data for following key core data entities:

- Citizen

- Employee
- Business
- Things
- Schemes & Policies

The data hubs would comprise of Digital Registries along with key identifier of each of the digital registries. Data hubs are part of the State Master Data Management, the State Master Data Management platform would comprise of other key data, refer the pillar (detailed architecture requirements documents) for details.

The digital registry would contain various details of the entities , refer pillar documents for detailed understanding:

Digital Registry	Reference Identifier	Mapping with State Digital ID	Data Trustee Department
Citizen			
Students	Student Registration Number	Aadhar ID	Education Department
Patients	MHIS ID		Health & FW
Ration Card Holders	Ration Card Number		FCS & CA
Social Welfare Beneficiaries	Aadhar ID		Social Welfare
Landowner's Profile	Aadhar ID		Revenue & Disaster Management
Criminal's Profile	Aadhar ID		Home (Police)
Households	Aadhar ID		PHE
Farmers	Farmer's ID		Agriculture, Fisheries & AHVT
Vehicle Driver	Driving License ID		Transport
MSME Workers Profile	Employment Regd. No		Commerce & Industries
Labour	Aadhar ID, Job Card Number (MGNREGA)		Community & Rural Development
Unemployed Youth	Aadhar ID		Labour
Employee			
Teacher's & Educational Staff Profile	Government ID	Aadhar ID	Finance
Department Officers	Government ID		All departments
Administrative Officer	GOI ID Number		Personnel & A.R
Contractual Employee	Aadhar ID		All departments
Security Officer	Government ID		Home (Police)
IT Consultant's Profile	Local ID		IT & C
Judge, Advocate, Judiciary Staff Profile	GOI ID/Aadhar		Law & Justice
Field Worker's Profile	Job Card No		Community & Rural Development
Business			
Business Entities	GSTN	GSTN	ERTS
MSME	Registration Number		Commerce & Industries
NGO	Registration ID		Planning
PSU	GSTN		Finance
Suppliers & Vendors	GSTN		All Departments
Tourism Entrepreneurs	GSTN		Tourism
Things			
Asset Register	Asset ID	State Asset ID	All departments
Infrastructure	Asset ID	State Asset ID	PWD
Service Kiosks	Asset ID	State Asset ID	IT & C
Land Records	GIS ID	GIS ID	Revenue & Disaster Mgmt
ICT Infrastructure	IT Asset ID	State Asset ID	PWD
GIS			
Office Location	GIS ID		IT & C
Sewerage, Water Pipes, Water Resources	GIS ID		PHE
Transmission Lines	GIS ID		Power
Roads & Highways	GIS ID		PWD
Hospitals, Clinic Locator	GIS ID		Health & FW

Digital Registry	Reference Identifier	Mapping with State Digital ID	Data Trustee Department
Land Details (Industrial Estates)	GIS ID		Commerce & Industries
Schemes, Policies			
Schemes	Scheme Code		Planning

Table 18: Digital Registry List

3.4.6 Data Governance

All departments under MeghEA would have a role to play in each of the stages of the Data Lifecycle for the Scheme (core data entity).

Data, being a key asset of the Government, must be correct, up-to-date, complete and secure (quality data). These requirements are managed by the following roles:

- Data owner
- Data Trustee
- Data custodian
- Data steward

Data owner is the ultimate owner of the data, this could be citizen or business or government department, the owner would be holding the proprietorship of the data.

Data Trustee is from the department or directorate and are responsible for data capture, data accuracy and concurrency.

Data Steward are department/sector experts in their respective data domains and responsible for Metadata management, accountability, security and integrity of data.

Data custodian is assigned specific data management responsibilities by a Data Steward. A Data Custodian typically will control access rights to data that it manages. A Data Custodian implements controls to ensure the integrity, security, and privacy of the data.

Below is RACI matrix for data governance related activities for each roles. R- Responsible, A-Accountable, C-Consulted, I – Informed:

Activity	Sub-Activity	Data Owner	Data Steward	Data Trustee	Data Custodian
Metadata management	Define & Govern	**I**	**R/A**		
	Implement		**A**	**C**	**R**
	Review & Report		**A**	**R**	**C**
Classify data	Classify & Govern	**I**	**R/A**	**C**	**C**
	Implement		**A**	**C**	**R**
	Review & Report		**A**	**R**	**C**
Data capture	Define & Govern	**I**	**A**	**R**	**C**
	Implement	**I**	**I/C**	**A**	**R**
	Report		**A**	**R**	**C**
Review data storage details	Review		**A**	**R**	**C**
	Implement		**A**	**C**	**R**
Back-up and DR	Define	**I**	**A/R**	**C**	**C**
	Implement		**A**	**C**	**R**
	Review and report		**A**	**R**	**C**

Activity	Sub-Activity	Data Owner	Data Steward	Data Trustee	Data Custodian
Data usage details	Define		A/R	C	C
	Govern & Report		A	R	C
	Implement		A	C	R
Data sharing	Define & Govern		A	R	C
	Implement		A	R	R
Data access	Define	I	A/R	C	I
	Review and change	I	A	R	I
	Implement		A	C	R
Data Masking	Identify & Govern	I	A	R	I
	Implement		A	C	R
Data Encryption	Identify & Govern	I	A	R	I
	Implement		A	C	R
Data archival	Define policy		A/R	C	C
	Implement		C	A	R
Data disposal	Define Policy	I	A/R	C	C
	Implement		I	A	R
Data Quality Management	Define completeness, accuracy and consistency thresholds		R	I	I
	Report data quality		A	R	C
	Monitor data quality and Govern		R	C	I

Table 19: Data Governance - RACI

The activities required under the realm of data life-cycle management is provided below:

Lifecycle Stage	Activity Description
Create	Need to approve any new addition or deletion in the attributes of all the data entities within the "scheme" core data entity
	Review data classification as per MeghEA standard data classification framework
	Review all security controls and report assessment every quarter using a dashboard
Store	Review data storage details
	Review and report security adherence of storage
	Define storage back-up policy and report
	Review and conduct DR drills
Use	In the case of data relating to employees, the purpose for which the data would be used should ideally be communicated at the point where the employee is providing the data. This is particularly important in the case of Aadhaar number, bank account details, family details.
	Review and approve report publication in public domain
	Refine and finalize the current access list for the data entities
	Review the datasets planned to be displayed through reports for the government officials to take decisions, what data would be displayed and whether masking of specific fields such as Aadhaar, bank account number etc. are required
	Review and approve data access requests from users
Share	Review and approve data sharing mechanism including encryption
	Review and approve data sharing details among departments on confidential datasets

Lifecycle Stage	Activity Description
	Review and approve request for data from external entities
Archive	Define archival policy
	Define standard operating procedures for data archival including mechanism, security requirements and test procedures
	Review archival reports in a regular basis
	Define access policy for archival data
	Review and approve any requests to view only access in archival data
	Review archival data restoration requests
Destroy	Define data disposal policies
	Develop standard operating procedures for data disposal
	Review data disposal requests

Table 20: Data Life Cycle Management

The Data Steward, Data Custodian and Data Owner for various key data entities are described in the pillar specific detailed architecture documents.

3.4.6.1 Data Quality Management

The Steps for data Quality Management is illustrated below:

Data quality thresholds and rules: As a first step to data quality management, it is critical to set data quality threshold. What data, how much of completeness is required, what is the minimum accuracy threshold. This step requires a threshold to be set by Data Trustees, on the threshold values in a system enabled reporting system.

Assess the quality of data: Data Custodian is responsible to report data quality test results to data trustees in a pre-defined timeline.

Resolve data quality issues: Data Trustee to derive plan for resolving data quality issues with respect to Human Development Sector in consultation with Data Custodians and keep the Data Owners informed of the new processes.

Monitor and control data: This stage is required for regular monitoring using tools and reports. The monitoring would be primarily be done by Data Custodians and overseen by Data Trustees.

Below Table describes the key process and details of the data quality management process.

Data Quality Management Steps	**Who?** Department & Branches	**What?** Data Entities	**How?** Procedures and steps	**When?** Time Schedules
Data quality thresholds and rules	All Departments has following set of roles: • Data Steward - Responsible for setting data quality thresholds • Data Trustee - Responsible for deriving current data quality and define metadata type	All key data entities.	• Set threshold for completeness • Set threshold for accuracy • Set metadata type	• Completeness to be monitored **Quarterly** • Accuracy to be monitored **monthly** • Metadata Type to be set once by data custodian and agreed by Data Trustee
Assess the quality of data	Data Custodian to publish report on data quality	All key data entities.	This will be done through reports	Every month
Resolve data quality issues	• Data custodian to resolve all quality	Entities for which quality issue exists	Data Steward and Data	As and when required

Data Quality Management Steps	Who? Department & Branches	What? Data Entities	How? Procedures and steps	When? Time Schedules
	• issues in the defined time frame • Data Steward to define time frame to resolve quality issues		custodian to get into joint meeting to decide on quality issue resolution timeline	
Monitor and control data	Data Trustee and Steward to monitor	All key data entities.	This will be done through reports	Monthly

Table 21: Data Quality Management

3.4.7 Data Quality Assessment

Data quality of current data set were assessed basis inputs from different stakeholders. Actual quality assessment would require access to the production data set, which needs to be carried out by data custodian. This assessment is based on stakeholder voice and may vary significantly from actual results

What has been assessed – the data set for all the digital registries that are currently being used and basis stakeholder voice – the coverage of the data as a percentage of total data and perception-based quality assessment of the data

Citizen - Digital Registries

- **Students** : There are no single source of truth , each directorate maintain their own data. The registration identification number varies in between MBOSE and universities
- **Patients** : Out of 8,37,283 households, 4,16,041 has enrolled in MHIS. There is a coverage of about 50% of total households
- **Ration Card Holders**: SECC 2011 database is the foundational data, there are several issues in the database. As per the department, close to 60% of data are accurate. The database is not linked with Aadhar; hence, this data is not much of use in its current shape
- **Social Welfare Beneficiaries**: No single source of truth, all schemes have their own data
- **Landowner's profile** : No such database, needs to be built
- **Criminal's profile**: Not assessed
- **Households**: PHE holds the data in electronic format but not in a relational database
- **Farmers**: Only Agriculture farmers data has been captured - the coverage is about 5%. However, Aadhar has not been linked to the data. No other farmers database has been assessed
- **Vehicle Driver**: Sarthi 4.0 system has 100% coverage of Meghalaya vehicle drivers data. But this is maintained at central ministry, obtaining the data may need additional procedural complexities
- **MSME Worker's profile** : No such database
- **Labour**: C&RD maintains the database of MGNREGA employment seeker, Aadhar seeding is 100%. But this is maintained at central ministry, obtaining the data may need additional procedural complexities
- **Unemployed youth**: Employment registration maintains the database for registered candidates only. Aadhar is not seeded in the database

- **Labour**: C&RD maintains the database of MGNREGA employment seeker, Aadhar seeding is 100%. But this is maintained at central ministry, obtaining the data may need additional procedural complexities

Employee – Digital Registries

- **Teacher's & Educational Staff Profile** : Maintained at directorate level in relational database format. The coverage is 100% however, Aadhar seeding may not exist
- **Department Officers**: 100% coverage, maintained in MeghEIS, no Aadhar seeding exists
- **Administrative Officer**: Maintained by central ministry, not assessed
- **Contractual Employee**: No single source of truth exists
- **Security Officer**: Not assessed
- **IT Consultant's Profile** : No single source of truth exists
- **Judge, Advocate, Judiciary Staff Profile** : Not assessed
- **Field Worker's Profile**: Not assessed

Business – Digital Registries

- **Business Entities**: GST Web portal from central government maintains the database. No reports were available to assess the coverage.
- **MSME** : C& I maintain the database, a database of 1400 units exists with the department
- **NGO** : Currently all NGOs has to register from e-district services, however, GSTN is not seeded. GSTN seeding is required.
- **PSU**: Finance department has the registry of PSUs but not in an electronic format.
- **Suppliers and Vendors**: No single source of truth exists, there is a need of GO to mandate registration of all suppliers along with 100% GSTN seeding.
- **Tourism Entrepreneurs** : No such database exists.

Asset – Digital Registries

- **Asset Register, Infrastructure, Service Kiosks**: Each department maintains list of assets but not in digital format. There is a need of single source of truth along with linkage to General Ledger system.
- **Land Records**: Not assessed.
- **ICT Infrastructure**: No single database is maintained, no asset or license management tools.

Maturity of GIS implementation is low and hence, it has not been assessed in detail.

3.4.8 Data Warehouse Strategy

Monitoring and Evaluation is most important aspect of MeghEA with primary responsibility assigned to Governance Pillar and the same is possible through Data Warehouse, Analytics and Business Intelligence. The below picture illustrates the Monitoring and Evaluation of all data pertaining to all six pillars in Meghalaya Enterprise Architecture project.

The data flows through the proposed solution as below:

- For each data source in the state as well as center system, any data which is updated will be exported to Blob Storage through Extract, Transfer, Load (ETL) Jobs.
- The data will be cleansed and transformed and stored into Data Warehouse.
- The Data Factory will load the data incrementally in tables of Data Analytics tool.

- The data analytics tool applies the analytics on business data and relationships.
- Business Intelligence tool analyzes data stored in Data Warehouse via Data Analytic Services.

Operating Model of Data warehouse

The State Government would provide the necessary infrastructure on cloud to departments to develop their own data warehouse solution, dashboard and analytics. The department would request usage and basis defined SOPs, the DW,BI and analytics product would be made available to the department for usage. The data warehouse would require following activities for implementation

1. Identify the data design of the data warehouse
2. Identify the data sources and data extraction methodology
3. Set tracking duration
4. Define and design the analytics on the data requirement
5. Design charts and graphs using BI tool
6. Implement the dashboard on the pillar portals

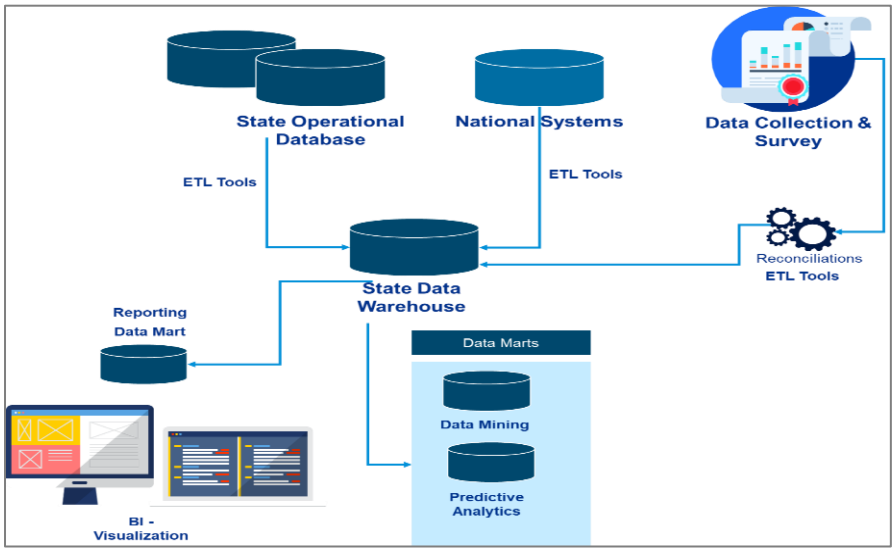


Figure 28: Data Warehouse Illustration

3.4.9 Data Communication Matrix

The data presently residing in silos in different departments would now combine and collaborate to deliver value.

Digital Registries : Digital registries would be used by various departments to perform multiple operations which is currently not viable as data is not shared. Basis data sharing rules , data for digital registries would be shared across the Government for various service delivery activities and events.

Plan Schemes: Basis digital registries Government of Meghalaya would be able to target certain set of beneficiaries who needs Government services the most, estimate total cost of schemes, design outreach plans.

Govern Services: Understand the key outcome of the key benefits delivered through integrated data and take necessary remedial actions.

Integrated Data: Below is a tabular representation of how data would be used across different pillars

to realize the integrated services. The horizontal header represents provider of data i.e. the data steward of the data ; while vertical leftmost row represents the pillar that would benefit from the data or consume the data for various purposes.

Information Consumer	Information Provider					
	Primary Sector	**Infrastructure**	**Human Development**	**Environment**	**Entrepreneurship**	**Governance**
Primary Sector	• Farmer demographics • Fodder information • Advisory	• Transport Facilitation • Permits Approvals	• Training details • Employment details • Health advisory • Medical records • Farmers details	• Land details • Climate advisory • Lease and permits • GIS details	• Market linkage • Trade promotion • Investment • Raw material	• Sanctions and Approvals • Budget requirement • Regulations
Infrastructure	• Transport details • Supply details • Inventory details • Irrigation permits	• Training details • Water body status • Business details • Vendor details	• Transport requirement • Supply details	• Transport requirement • Supply details • Inventory details • Challan details	• Permits /permissions • License • Business details	• Sanctions and Approvals • Budget requirement • Regulations
Human Development	• Commodity Prices • Purchaser details • Stock information • Treatment Requirement	• Employment details • Employment requirement • Insurance details • Location details	• Health advisory • Medical records • Student details • Health facilities • Patient details • Claim details	• Climate Advisory • Resource details • Compliance details	• Medical Records • Insurance • Treatment Requirement • Employment	• Sanctions and Approvals • Budget requirement • Regulations
Environment	• Approval requests • Advisory • Farmer Land details	• Transport details • Supply details • Inventory details	• Advisory details • Medical records • Claim details	• Permits and Approvals • Advisory • Land details • Business details	• Lease requests • Asset details • Compliance	• Sanctions and Approvals • Budget requirement • Regulations
Entrepreneurship	• Service Details • Training/capacity building Details • Market linkages	• Transport details • Transport inventory • Advisory and safety	• Medical records • Claims • Skill development •	• Training/capacity building Details • Employment details • Climate advisory	• Business details • Training/capacity building Details • Beneficiary details	• Sanctions and Approvals • Budget requirement • Regulations
Governance	• Scheme Details • Budgeting details • Funding/Payment details • Implementation details	• Scheme Details • Budgeting details • Funding/Payment details • Implementation details	• Medical Records • Scheme Details • Budgeting details • Funding/Payment details • Implementation details	• Scheme Details • Budgeting details • Funding/Payment details • Implementation details	• Scheme Details • Budgeting details • Funding/Payment details • Implementation details • Compliance details	• Scheme Details • Revenue • Returns

Table 22: Data Communication Matrix

3.5 MeghEA: Technology Architecture

The technology architecture defines the methodology, principles, designs and guidelines for implementation of IT infrastructure for the Government of Meghalaya. It includes all activities to design and implement better technology architecture for digital Meghalaya and provides easy and seamless access to ICT Infrastructure for the departments to operate on.

The objective is to develop the Technology Architecture that enables the Architecture Vision, target business, data, and application building blocks to be delivered through technology components and technology services, in a way that addresses the stakeholder concerns.

Below are the sections described in technology architecture of MeghEA:

- As-Is Technology Stack with Gaps
- Technology Architecture Transformation Plan
- Future State Technology Architecture

3.5.1.1 Key Principles

Following are the principles defined under Technology Architecture and customized for Meghalaya Enterprise Architecture:

- ✓ **TP1 – Technology Independent Architecture**
- ✓ **TP2 – Open Standards**
- ✓ **TP3 – Shared Infrastructure**
- ✓ **TP4 – Resilient Architecture**
- ✓ **TP5 – Optimized Infrastructure**
- ✓ **TP6 – Network and Connected devices at all service delivery centers**
- ✓ **TP7 – Control Technical Diversity**
- ✓ **TP8 – Interoperability**

Refer annexure on Technology Architecture Principles for details around each of the above architecture principles

3.5.1.2 Standards

All standards mentioned in IndEA would be followed in MeghEA, refer IndEA for details on the standards. Additionally, below is the list of standards that needs to be followed for all application design, development and testing:

Code	Standard	Recommendations
TS.1	**Simple Network Management Protocol (SNMP)** For collecting and managing information about managed devices for 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). SNMP is used by network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an Application Layer protocol, a database schema, and a set of data objects. SNMP version 3 would be used for national 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	Must be adhered while developing and implementing new systems

Code	Standard	Recommendations
	• Internet Explorer (IE) • Chrome • Firefox • Safari • Opera	
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 (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	**SSH and SFTP** Network Protocol for information exchange SSH would be used as default standard for information exchange. Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network. SFTP SFT would be used as default standard for content exchange. SFTP (SSH File Transfer Protocol) is a secure file transfer protocol. 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 (IP) v6** 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 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

Table 23: Technology Standards

3.5.2 Technology Architecture Transformation Plan

IndEA – TRM was at the core of the approach. IndEA - TRM depicts the layout of the technology foundation of ICT-based systems to be designed for the delivery of identified business services. The components listed by IndEA in TRM include a technology system on an end-to-end basis, including IT Infrastructure, Applications, Access Devices, Communication Systems and Service Delivery modes. TRM also defines the currently applicable open standards for all the solution building blocks and components and identifies the Open Source Products for each technology component.

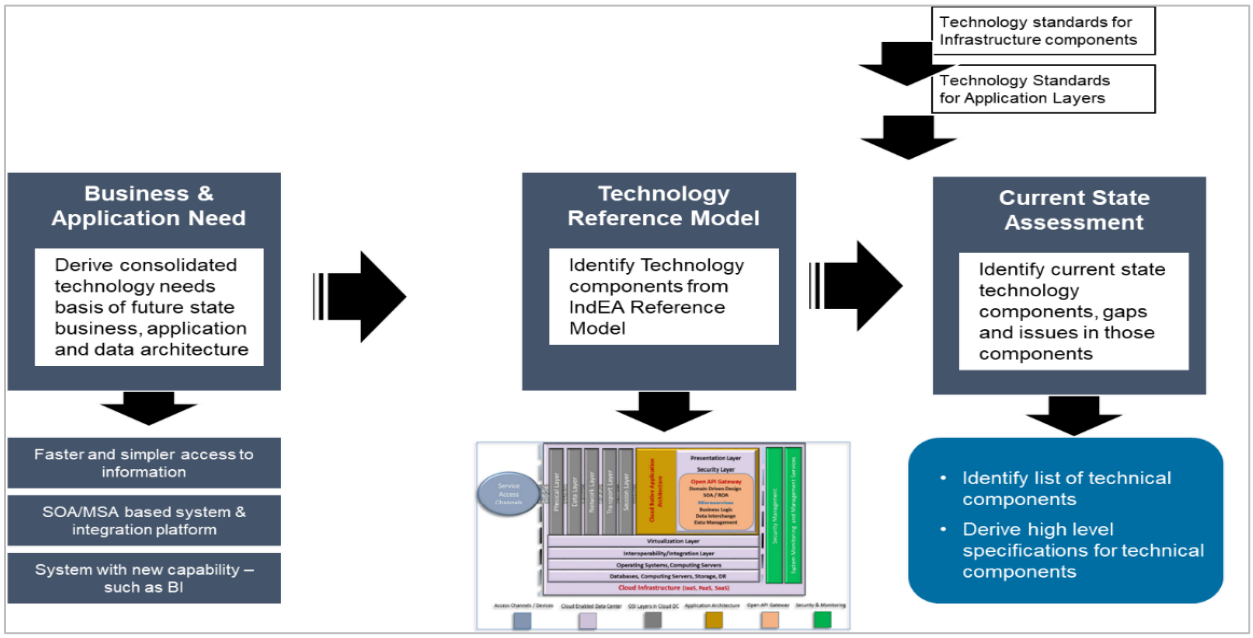


Figure 29: Technology Architecture Approach

Steps to undertaken to derive Technology Architecture:

- Identify business, application, security and data needs for technology infrastructure. Deduce the necessary technical components need to realize the future state.
- Map current state Technology Architecture with IndEA – TRM and perform principle adherence to identify gaps.
- Derive new components required to realize technology architecture.
- Identify Software and Hardware components used in the layers of the architectural patterns diagram.
- For each of the above components, identify the open standards, and use open source products wherever prudent and applicable.

Technology Architecture serves to outline the technology elements that collectively support the adoption and implementation of component-based architectures. The model provides the foundation to advance the re-use of technology and component services across the Meghalaya Government through standardization. Aligning agency capital investments to the architecture leverages a common, standardized vocabulary, allowing inter-department and intra-department discovery, collaboration, and interoperability.

Technology deployment architecture of the MeghEA assembles the assets and capabilities required for all deployments. It defines the logical and physical view of systems identified in the application architecture.

Component Name	Component Description
Single Sign-On	Single sign-on (SSO) is a typical IAM solution that enables users to securely authenticate with multiple applications and web portals by logging in only once using a variety of options such as mobile number as user id, Government email ID, etc. With single sign-on, the application or web portal that the user is trying to access relies on a trusted token to verify the user.
Security Layer	The external security layer shall protect the system from unwanted traffic and provides easy and seamless access with the help of Load balancer, reverse proxy and access gateways.

Component Name	Component Description
Web Portal Server	Web Portal Server shall enable external and internal users to access systems through any web browser from any location.
Internal Security	All internal traffic shall be routed through the internal security layer which shields application clusters from unwanted attacks.
Application Server	The application server consists of business logic and performs the task required for the system.
Database Server	The structured data pertaining to the system shall be saved in the database. For high availability, databases should be configured on the cluster environment.
Centralized Monitoring System	The centralized monitoring system shall manage and monitor all government systems and IT infrastructure components. It shall provide real-time alert/notification and dashboard for analysis and performance management.
Disaster Recovery Site	The DR site would act as the main data centre in case of incidents such as network outages, power failure, etc. It would be enabled by Failover switch

Table 24: Technology Components

The following sections 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 Meghalaya Enterprise Architecture.

- Access Devices
- Peripherals
- Network connectivity
- Network infrastructure
- Platforms
- Software Development Technology
- Computing stack
- Hosting locations

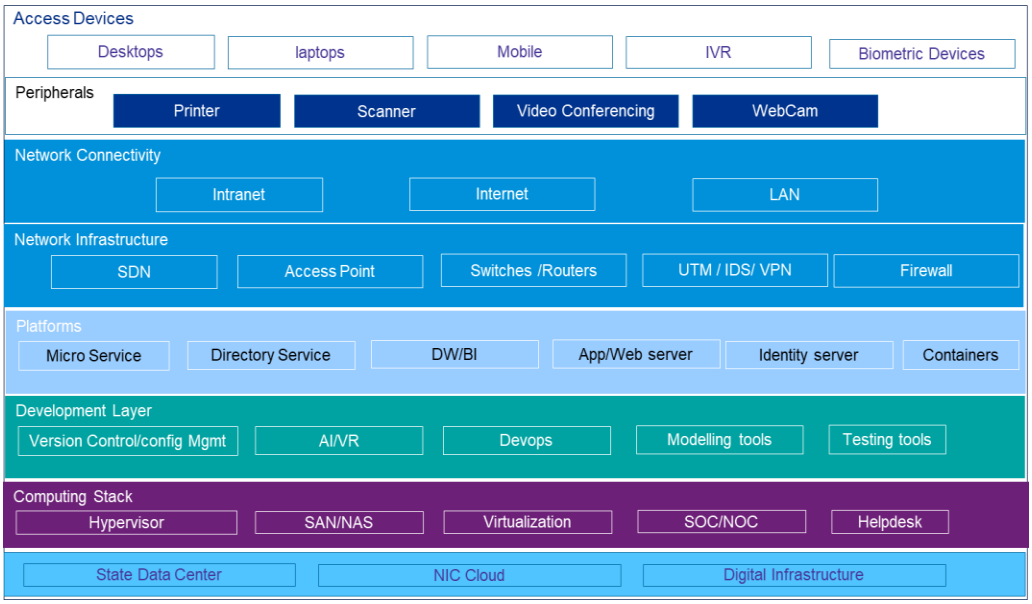


Figure 30: Proposed Technology Architecture Model

3.5.2.1 Access Devices

Access devices allow users to access the Department's ICT systems. In line with the business need to deliver services through multiple channels and enable anytime, anywhere access to its resources as highlighted in earlier Section, Department's systems would need to support a diverse set of Access Devices.

Location	Designation	Recommended Requirement
Secretariat	• Department HoD • Department Joint Secretary • Department Under Secretary • Commissioner • Department UDA • Department LDA • Superintendent • Program/Scheme Director • Research Officer	• Desktop availability at the ratio of 1:1 • Bio-metric device – at least one per floor • Mobile Device at the ratio of 1:1
District Offices	• DDO • Deputy Directors • Superintendent • UDA • LDA	• Desktop availability at the ratio of 1:1 • Bio-metric device – at least one per district office • Mobile Device at the ratio of 1:1
District Offices	• Field Officers	• Mobile Devices at the ratio of 1:1
Block Offices	• Field Officers • Department officers	• Mobile Devices at the ratio of 1:1 • Bio-metric device – at least one per district office

Table 25: Access Device Requirement

3.5.2.2 Peripherals

Peripherals and the devices that attach to Access Devices and allow users to perform additional activities to best leverage the Information Assets and ICT systems of the Department. Appropriate number of:

Printers, scanners and Video conference facilities are required as per need

3.5.2.3 Network Connectivity

Service delivery in Meghalaya suffers significantly due to Network connectivity. Below is the current state assessment

District	NICNET/SWAN/Public	Bandwidth	Type
Shillong	NICNET	100 Mbps	fiber
West Khasi Hills	NICNET	LAN Connection	fiber
Ri-Bhoi	NICNET	LAN Connection	fiber
South West Khasi Hills	NICNET	100 Mbps	fiber
East Khasi Hills	BSNL Broadband	N/A	fiber
West Jaintia Hills	NICNET	LAN Connection	fiber
East Jaintia Hills	NICNET	LAN Connection	fiber
West Garo Hills	NICNET	4 Mbps	fiber
East Garo Hills	NICNET	34 Mbps Speed	fiber

District	NICNET/SWAN/Public	Bandwidth	Type
South Garo Hills	NICNET	10 Mbps connected through NIC by Jio Network	fiber
South West Garo Hills	NICNET	VLAN14 Connection from Core Switch	fiber
North Garo Hills	NICNET	100 Mbps	fiber

Table 26: Current State Network Connectivity

As seen above, the primary network State SWAN is non-operational in most of the districts. NICNET the secondary network, is acting as the primary network for the offices. Below is the mandatory requirement:

Device/Capability	Details
Primary Network	Availability of uninterrupted supply of 100 Mbps internet connection
Secondary Network	Availability of uninterrupted supply of 100 Mbps internet connection from a different network service provider
Access points	Offices with Wi-Fi campuses are required to plan and implement access points to allow employees to connect to the internet/intranet.
Switches	Offices are required to implement switches to connect computers, printers and servers within a building or campus. Each office would require back-up switches
Routers	Routers are used by Offices to connect a LAN hub or Switch to a WAN as per need

Table 27: Network Requirements

Other requirements at State Data Centre:

Device	Requirements details
Firewalls	Firewalls are required to monitor traffic to or from the network. It allows or blocks traffic based on a defined set of security rules.
UTM (Unified Threat Management)	It offers multiple security features (anti-virus, anti-spam, content filtering, and web filtering) in a single device or service on the network to protect users from security threats.
Load Balancers	Load balancing aims to optimize resource use, maximize throughput, minimize response time, and avoid overload of any single resource.
IPS	Intrusion prevention systems (IPS) are network security appliances that monitor network and/or system activities for malicious activity.
Directory services	Directory Services is a network service that discovers and identifies resources on a network and makes them accessible to users and applications.

Table 28: Future State Devices

3.5.2.4 Platforms

Platforms have been used to represent the Application Platform that provides the underlying capabilities needed by the Applications to run and deliver their intended function to the users. These would be the elements used to make up the development, testing and production environment required by the Applications.

Refer Detailed Architecture Requirements - Pillar Documents section Technology Architecture – "*New Requirements Specifications*" for details.

3.5.2.5 Software Development Technology

Following are the new components required for software development

Capabilities	Description
Version control system	Used to store, track, maintain versions for the source code and associated documentation.
Configuration management system	Technology for managing the configuration of software deployed in the enterprise.
Modelling tools	Facilitates the analysis and design of object-oriented systems. The model-centric approach to software development brings modelling artefacts from business requirements to implementation architecture.
Development Environment	Provide an integrated development environment to the developer/ team to write the source code of the application and use the visual frameworks to design the application interface. It also allows the team of developers to collaborate their work and test the application.
Testing tools	Provide a collaborative environment that is intended to make test automation efficient, traceable and clear for stakeholders.
Artificial Intelligence	Facilitate the creation of machines/applications that can act like take decisions like humans.
Virtual Reality	Use of technology to create a simulated environment which resembles real-life situations.

Table 29: To-Be Software Development Technology

3.5.2.6 Computing Stack

Refer Detailed Architecture Requirements - Pillar Documents section Technology Architecture – "*New Requirements Specifications*" for details.

3.5.2.7 Support

Support capabilities would enable the Department's internal and external IT services providers to provide support to end-users and ensure optimal operations of Departments' ICT landscape.

Capabilities	Description
IT Helpdesk	System and helpdesk for registering IT system issues
Unified Contact Centre	Service grievance helpdesk for all service related queries and resolution

Table 30: To- Be Support Capabilities

3.5.2.8 Hosting Location

Considering majority of the infrastructure in state data centre out dated and requires immediate refresh, it is recommended to opt for cloud migration of the existing (systems planned to be retained)

Capabilities	Description
State Data Centre	Phase wise migration to cloud, refer section Cloud Migration Strategy for details
Mini Data Centre	Phase wise migration to cloud, refer section Cloud Migration Strategy for details

Table 31: Hosting Locations List

In addition to the above, Planning department is in the process of purchasing cloud space from MeiTY approved vendor.

3.5.2.9 As -Is System-Technology Matrix

Refer Detailed Architecture Requirements - Pillar Documents section Technology Architecture – "*New System – Technology Matrix*" for details.

3.5.3 Future State Technology Architecture

3.5.3.1 IT Infrastructure

IT Infrastructure plays a major role in success of any Enterprise Architecture project as the initiative is supported by IT applications.

As per the details collected from the departments in scope of Meghalaya Enterprise Architecture, most of the services are being delivered in manual mode. There are challenges related to network connectivity in some of the block and district offices. The IT infrastructure deployed in Data Centres has already crossed end of life. Below are the key requirements as part of the Technology Modernization:

- The State Government needs to revamp and upgrade its IT Infrastructure considering the end of life analysis.
- Primary and secondary network needs to be made available at all District, Block and Circle offices.
- Desktops, Printers, POS machines, Barcode Scanners, Mobile devices need to be procured and distributed to the officers to perform their duties efficiently.

Below is proposed Technology Architecture in future state:

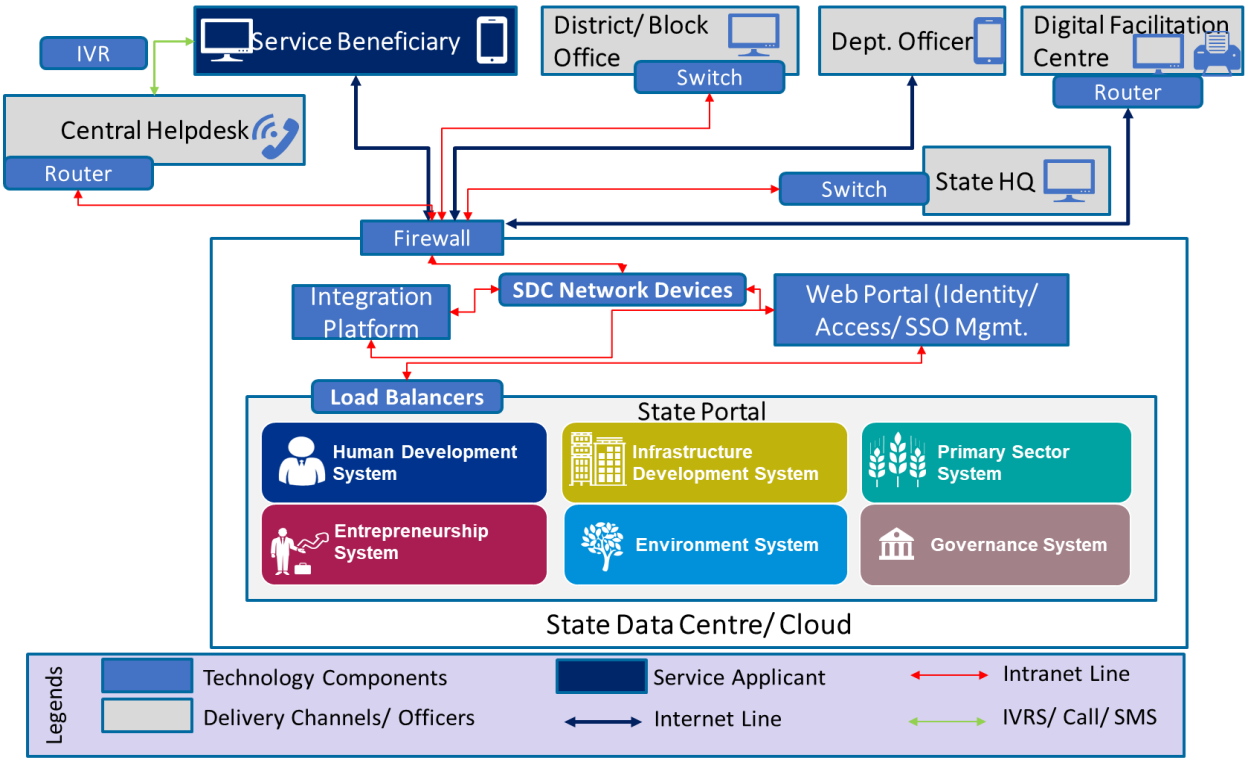


Figure 31: Future State Technology Architecture

3.5.3.2 Core Platform Specifications

Core Platform Specifications are derived based on the requirement for minimum viable architecture, and as per need the core platform requirement. Following matrix provide the core platform specifications;

Technology Component	Description	Specification	Proposed Technology
Integration Platform	The State Service Bus or Integration platform would be based in open-source technology that enables API-centric integration using integration architecture styles such as microservices, cloud-native, or centralized ESB. The platform MUST provide a choice of approaches for either code-driven or graphical, drag-and-drop/configuration-driven integration.	1 GB memory for a Docker container. Minimum 0.5 core (1.0-1.2 GHz Opteron/Xeon processor). 1 GB RAM for JVM. ~512 MB heap size. This is generally enough for processing typical SOAP messages. However, the requirements vary with larger message sizes and the number of messages processed concurrently.	Open Source. The state may opt for WSO2 integration platform.
API Gateway	Integration platform would be based in open-source technology that enables API-centric integration with external systems	Dual core processor, 2 GHz or faster 4 GB memory Dedicated server running one of: Red Hat Enterprise Linux (RHEL) SuSE Linux Enterprise 10 or 11 Solaris 10 (x86 or Sparc) (assuming Java is preferred coding platform) Java SE Development Kit (JDK) 1.8.0 u102 Database license & minimum 500 MB for tablespace (1 - 10 GB recommended)	Open Source.
Chatbot	Chatbot to be deployed and integrated with all systems	Chat Server – High Availability, specification would depend on the solution Digital Messaging Server – This may be required if not packaged with solution Artificial Intelligence tool	Open Source.
Analytics	Tool for business intelligence and analytics processing for data based dashboard	Database Server (this depends on the product) Assuming the product is Microsoft Power BI (this is not a recommendation rather used for illustration) Windows 7 / Windows Server 2008 R2 .NET 4.5 Memory (RAM): At least 1 GB available, 4 GB recommended Processor - 1 gigahertz (GHz) or faster x86- or x64-bit processor recommended.	Recommended Commercial Off-The-Shelf platform
Data Warehouse	To be used for reporting and business intelligence	4 CPU cores @ 2GHz, 4 GB RAM , 32 GB memory, 200 GB GB disk space	Recommended Commercial Off-The-Shelf platform
Consent Management	To store citizen consent for data capture and data sharing	Database Server - Database license & minimum 500 MB for tablespace (2 GB recommended) LBS (Load Balancer Switch) & FOS (Fail Over Switch) at SDC (State Data Centre) between SDC & DR (Disaster Recovery), with licenses	Open Source.
Single Sign On	Refer section Single Sign on Strategy	Dual core processor, 2 GHz or faster 4 GB memory Database Server - Database license & minimum	Open Source.

Technology Component	Description	Specification	Proposed Technology
		2 GB for tablespace (10 GB recommended)	
Data Quality Manager	Refer Data Architecture section	Data Quality tool selection would derive the requirement	Recommended Commercial Off-The-Shelf platform

Table 32: Core Platform Specifications

3.5.3.3 New Requirement Specifications

The new technology component listed below along with High-level specifications based on number of users and volume of expected transactions.

Equipment / component / supply / works	Qty. at Primary Site	Qty. at DR Site	Remarks
Pillar System DB Server	6	6	LBS (Load Balancer Switch) & FOS (Fail Over Switch) at SDC (State Data Centre) between SDC & DR (Disaster Recovery), with licenses
Pillar System App Server	6+6	6	LBS & FOS at SDC between SDC & DR, with licenses
IAM / WAM Software (including SSO and associated software components with 40 Core perpetual license	1	1	
Directory Service per Instance/Node basis	1	1	High Availability Scalability: High Scalability to store minimum 20 Million user records Support for 64-bit Architecture
IAM/WAM Server	1+1	1	LBS & FOS at SDC between SDC & DR, with licenses
IAM/WAM DB Server	1+1	1	LBS & FOS at SDC between SDC & DR, with licenses
Remote Servers at Checkpoints (each)	1		Router and standalone application along with required licenses for syncing data with data centre with daily end of day (EoD) frequency.

Table 33: New Requirement Specifications

In addition to above, there will be infrastructure requirement based on the roles of the officers as defined in each Pillar document.

Key Changes

- Deployment of Enterprise Service Bus and API gateway for effective integration. Re-architecture of systems to SOA/ MSA based architecture.
- Re-architecture of Department portals to modern architecture.
- Implementation of data back-up and disaster recovery mechanism, implementation of DR drills.
- Implementation of analytics software.
- Server virtualization at SDC.
- Implementation of tools for access rights, performance monitoring, and utilization monitoring.
- Implementation of SSO components.

3.5.3.4 Cloud Migration Strategy

The application can be hosted on cloud by provisioning Infrastructure as a Service and Platform as a Service. This would eliminate the need to procure hardware and maintenance of the same thus

leads to huge cost saving towards capital expenses to the Government of Meghalaya. The cloud migration strategy for Meghalaya is as below:

1. *Identify Applications for Migration*

Applications to be assessed for migration needs and prioritization to be done. The application with minimum efforts for migration should be prioritized first and with maximum efforts should be at last in the prioritization list.

2. *Prepare Business Case*

- Cost: The cost for on premise and cloud should be evaluated considering capex (Capital Expenditure) as well as opex (Operational Expenditure) over long term which should include Servers, Components, Licenses, Storage, Network, Power, Space, Maintenance and Manpower etc.
- Benefit: Benefits with respect to Availability, Scalability, Reliability, Performance, Security & Privacy, Urgency, Disaster Recovery etc. should be considered for preparing the business case for cloud migration.
- Risk: All Risks related to on premises and off premise to be recorded and deliberated in the preparing the business case.

3. *Assess Cloud Environment Specification*

The applications would be assessed for computing requirements and based on the same, specifications required for deployment would be decided.

4. *Selection of Cloud Vendor*

The cloud provider should be selected very carefully which provides best value for the required specifications and comply to the government guidelines released from time to time.

5. *Determine Cloud Migration Plan*

- Determine Migration Plan for each Application.
- Rehost the applications where no changes are required to be done in the application.
- Identify the applications where platform need to be changed. Determine new platform on which these need to be migrated and modify the required code based on new platform and migrate the applications.
- Purchase the applications which are required to be deployed as COTS/ SaaS.
- Re-Architect the applications which are not complying to MeghEA architecture and Redesign them from monolithic architecture to service-oriented architecture.
- Decommission the applications which are proposed to be decommissioned and replaced by new applications.
- Develop new required applications in line with MeghEA architecture and host in cloud.
- Retain the applications which are not to be moved to cloud for now and should be revisited later.
- Monitor and validate all applications during migration and transition before deployment into Production.

3.6 MeghEA: Security Architecture

Meghalaya state government has been planned its services online through web and mobile interfaces. This may open a boulevard for multiple threats to access the information, systems, and assets to be viewed and/or altered unauthorized to harm the services, applications or the

departments. This points out the importance of defining and implementing policies, processes, controls for information security.

Security is not confined to a single level but needs to be addressed at business (defining security policies), infrastructure (appropriate configurations at the network, data center, and hardware), application (Application deployment, OS hardening) and data (storage, access) levels. It is least costly and most effective to plan for and implement security-specific elements in the Architecture as early as possible in the MeghEA development cycle.

The goal of Security Architecture is the design artifacts that describe how the security controls are positioned and how they relate to the overall systems architecture. These controls serve the purpose to maintain the system's quality attributes such as confidentiality, integrity and availability. Below points describes the sections of security architecture of MeghEA:

- Current State Security Architecture
- Security Requirements
- Future State Security Architecture

3.6.1.1 Key Concepts

- **Security Model**: A security model outlines the requirements necessary to properly support and implement a certain security policy.
- **Confidentiality**: Confidentiality is the information security property responsible for preventing unauthorized disclosure of information. In other words, it is a mechanism to give access to authorized individuals or systems in the organization only.
- **Integrity**: Integrity is the ability to guarantee the accuracy and consistency of data and information during its entire life cycle.

3.6.1.2 Key Principles

Following are the principles defined for Security Architecture and customized for Meghalaya Enterprise Architecture:

- ✓ **SP1 – Data Integrity**
- ✓ **SP2 – Data Privacy and Confidentiality**
- ✓ **SP3 – Secure by Design**
- ✓ **SP4 – Anonymize Personal Health Records**

Refer annexure on Security Architecture Principles for details around each of the above architecture principles.

3.6.1.3 Standards

Below is the list of standards that needs to be followed for all application design, development and testing:

Code	Standard	Recommendations
TS.1	**Simple Network Management Protocol (SNMP)** For collecting and managing information about managed devices for 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). SNMP is used by network management	Must adhere for implementation of managed devices

Code	Standard	Recommendations
	systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an Application Layer protocol, a database schema, and a set of data objects. SNMP version 3 would be used for national standard.	
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 (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	**SSH and SFTP** Network Protocol for information exchange SSH would be used as default standard for information exchange. Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network. SFTP SFT would be used as default standard for content exchange. SFTP (SSH File Transfer Protocol) is a secure file transfer protocol. 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 (IP) v6** 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 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

Table 34: Technology Architecture Standards

3.6.2 Security Architecture Approach

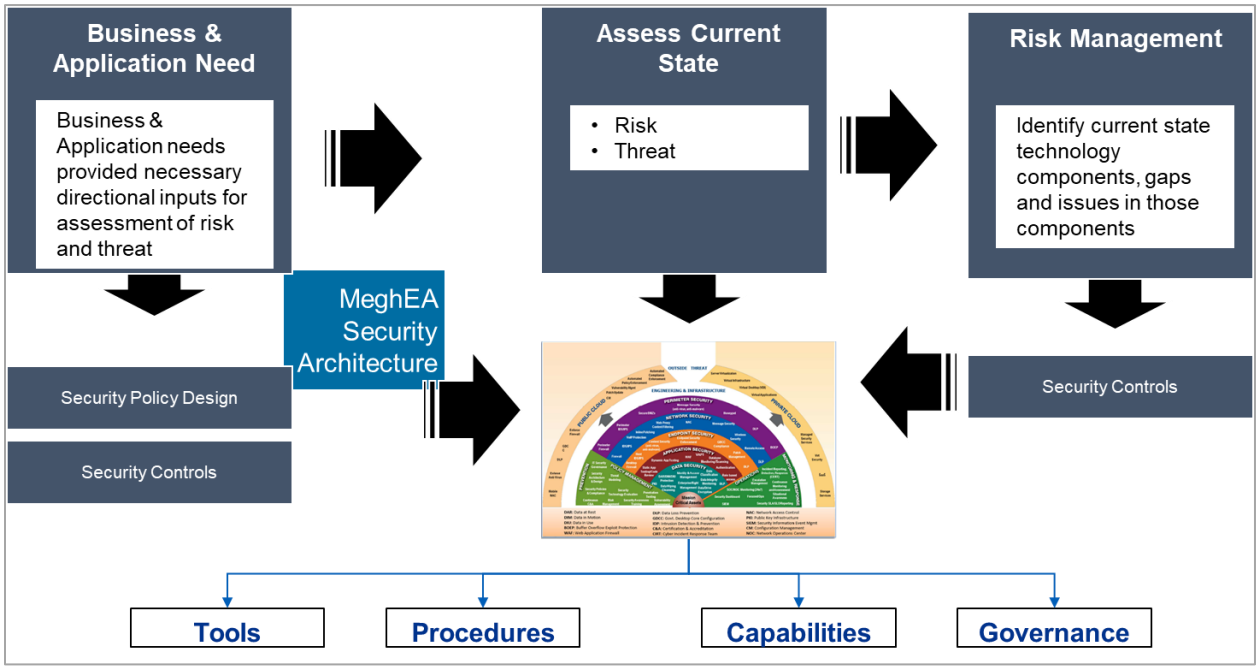


Figure 32: Security Architecture Approach

Important steps as part of Security Architecture:

1. Business and Application Need
    - Refer Single Sign On Strategy – key aspect of business and application need
    - Refer Data Classification – Key aspect of data security
    - Refer Additional Components – Key components to ensure required security
    - Refer Pillar documents security architecture for additional security requirements
2. Assess Current State
    - Refer Threats and Vulnerabilities section
3. Security Policy and Controls.
    - Refer Security Policies and Control section

3.6.3 Access Requirement

The various modules in systems would need varied accesses. The access to various modules should be allowed based on the roles of the stakeholder. Thus, there is a need to identify correct beneficiary, all authorities and their roles. For implementing the same, identify and access management plays a vital role.

3.6.4 Data Classification

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the entity in case the data is disclosed, altered or destroyed without authorization. Sensitivity herein is the control of access to information or knowledge that might result in loss of an advantage or level of security if disclosed to unauthorized one.

Classification Category	Definition	Example of information	Impact of violation
Public	GoM data/information may be made available to the general public and intended for distribution outside of GoM boundaries. It is defined as information with no existing local, national or international legal restrictions on access or usage. This data may be freely disseminated	Scheme data on welfare, education, social initiatives and press releases are under this category.	No impact
Official	Most of the information created or processed by GoM entities. This includes routine GoM operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.	Information pertaining to day to day activity of GoM, service delivery, international relations and diplomatic activities, budget details, public safety, criminal justice and enforcement activities. Many aspects of defense, security and resilience.	High impact
Private	Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors.	GoM bills, Government financial documents or records, crime details, public aid and law and order confidential documents etc.	High impact
Confidential	The GoM's most sensitive information requiring the highest levels of protection from the most serious threats.	Documents of military intelligence, reports of other countries etc., disclosure of which will have serious national and international impact	Very high impact

Table 35: Data Classification Categories

All data entities identified has been classified as per above categorization and accordingly the security and integrity requirements has been defined for each data entity. Please refer Pillar DAR documents for details.

3.6.5 Additional Components

Government of India has proposed several laws to govern data security that would give individuals complete ownership of their data. Individuals would have the absolute right to refuse or allow data to be generated, collected, accessed, transmitted or used. And data collectors would be prohibited from refusing services to those who do not want their data collected or used.

Ministry of Electronics and Information Technology (MeitY) is in process of enacting '**Data Protection Framework on Digital Information Privacy, Security & Confidentiality' Act**, which would be applicable in all domains. This act would provide the framework for Ministry to utilize the individual's data in various programs in a secured manner.

Several key pointers derived based on various digital security acts/ recommendation along with MeghEA security architecture actions or solutions are described in below table:

Key Pointers	Security Architecture Actions/Solutions
The consent manager would be there to ensure that the citizen/ patient as the Data Principal, is in complete control of what data is collected, and how/with whom it is shared and for what purpose, and how it is processed.	Consent Manager
The Health Locker is a standards-based interoperability specification that can be implemented by multiple players to enable the creation of a Personal Health Record ecosystem. When a medical record needs to be issued, only a reference link is shared with the locker ecosystem.	Health Locker
The Anonymizer takes data from the Health Locker and/or other health data sets, removes all personally identifiable information to protect privacy and provides the anonymized data to the seeker. Tools available can anonymize both structured and un-structured data.	Anonymizer

Key Pointers	Security Architecture Actions/Solutions
The data security manager stores information on what data is shared with whom, it also provides the information on the secondary owner of the health record in case of emergency	Data Security Manager
The data flowing out from the secured system to GOI systems would be encrypted and a corresponding key would be shared with authorized entity to decrypt the data	Encryption and Decryption Tool

Table 36: Additional Security Components

Based on the above requirement, the diagram below describes the future state security architecture for Meghalaya Enterprise Architecture.

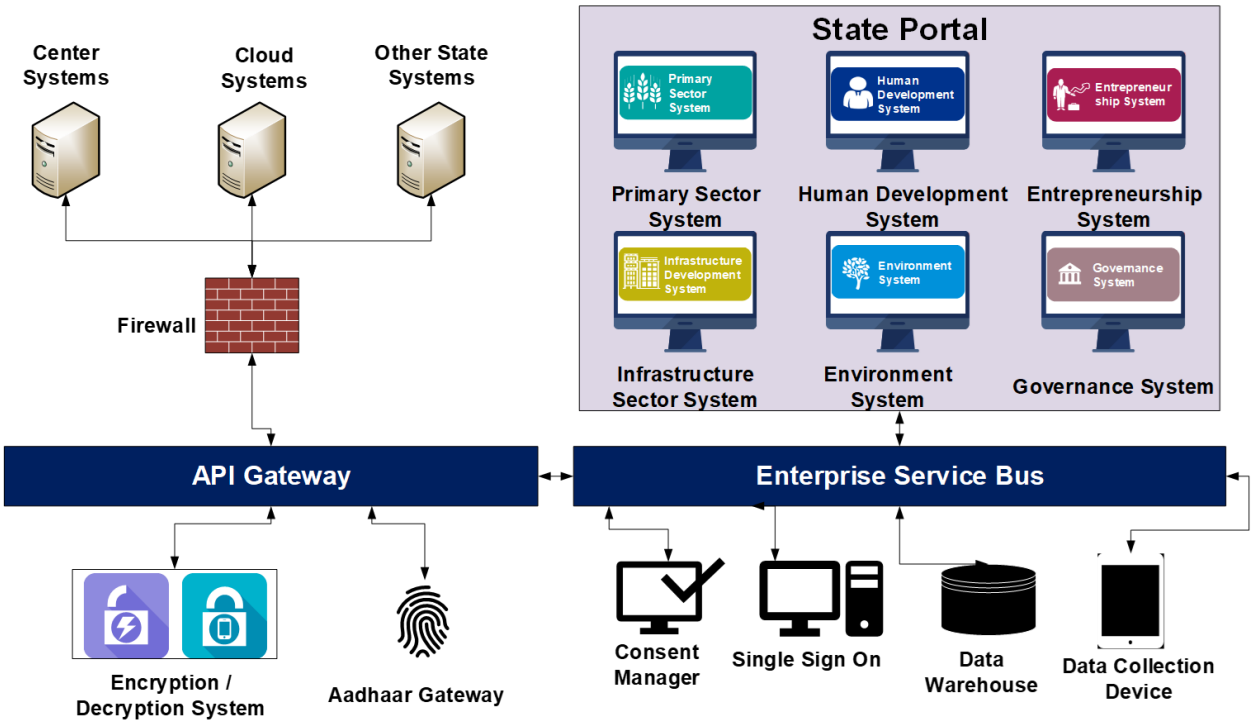


Figure 33: Future State Security Architecture

3.6.6 Single Sign on Strategy

Single Sign-On

Single sign-on (SSO) is a typical IAM solution that enables users to securely authenticate with multiple applications and web portals by logging in only once using a variety of options such as registered mobile number as User ID, OTP, Government Email ID - (username and password) etc. With single sign-on, the application or web portal that the user is trying to access relies on a trusted token to verify the user. The tokens are based on below:

- Credentials integrated with State Digital ID, Official Email ID, Employee ID, Mobile Number
- Caching
- Protocol

Single-Sign-On Flow (SSO): The access control flow is based on the usage of the Single-Sign-On (SSO) enablement and Policy driven authorization. The following sequence illustrates the envisioned access control flow:

- User attempts to access the resources on the Pillar Specific Web Page (from State Portal)
- The Access Proxy component intercepts the user request and determines, whether the User is already authenticated and has an active SSO Session Context.
- In case of no Active SSO Session Context exists, the following process takes place:
    - The Access Proxy component will forward the user request to the Authenticate & Authorize component for verifying the user credentials & querying the authorization details.
    - The user will be prompted to provide the user credentials.
    - The user credentials are collected and validated against the State-wide user directory. Invalid credentials will result in access denial.
    - The Authorization component will query the user attributes for the authenticated users.
    - A secured session context is created and maintained in the authorization component.
- In case of an Active SSO Session Context exists, the following process takes place:
    - The Access Proxy will forward the user request to the PDP via the PEP on the Web Server
    - The PDP determines the applicable access policy for the user by verifying the policy repository
    - If user is authorized, the Access Proxy determines how the authenticated user information need to be communicated to the Protected Resource (e.g. SAML token, HTTP headers, Username token, RACF pass ticket). Security Token Service invokes Access Manager components to validate
    - The Secure Token Services component creates the requested token from the user information. This enables the user information to be mapped to account and attribute information the finance Application recognizes based on configured trust services/policies
    - The user request is then forwarded to the requested resource on the Application container

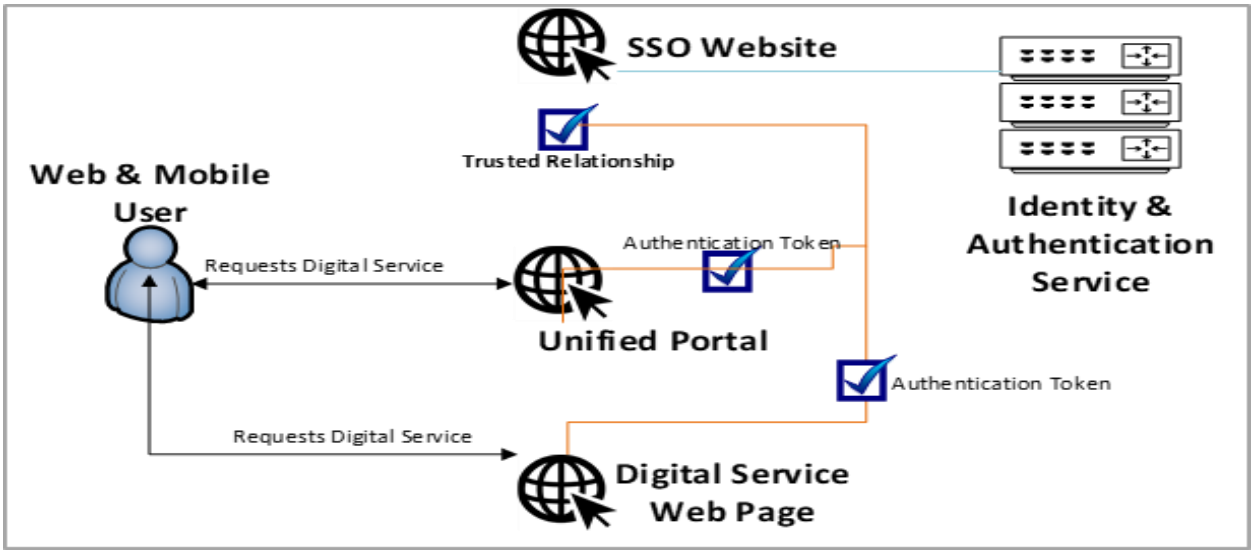


Figure 34: SSO Functional View Diagram

High Level Steps for SSO Implementation

1. List user roles and access privileges for all existing systems.
2. Determine access control requirement for all roles.
3. Define the various login credentials to be used (State Digital ID would be the only user ID).
4. Design solution architecture for SSO.
5. Choose SSO open source product.
6. Determine common systems compatibility to SSO.
7. Implement SSO as proof of concept.
8. Deploy new identity server and authorization server.
9. Migrate all user profile management to new servers.

3.6.7 Threats and Vulnerabilities

Sl. No.	Vulnerability	Threat	Recommendation
1	Terminated/ Suspended/ Retired employees' system identifiers (ID) are not removed from the system	Terminated/ Suspended/ Retired employees can login to the Portals and access data which is not authorized.	System identifiers (ID) for Terminated/ Suspended/ Retired employees should be deactivated as part of the relieving process.
2	Agreements on information transfer	Without an agreement on information transfer, the important information may not be transferred securely and poses risk of unauthorized access.	Agreements shall address the secure transfer of business information between the organization and external parties
3	Virus, spyware, malware or such cyber-attacks through user systems	Data theft, data modification, system intrusion	Implementation of user device configuration patches
4	Malware, phishing attack through emails	Data theft, data modification, system intrusion which may lead to financial and reputation loss or both	Deployment of regular updates and OS patches through automated system. Effective monitoring of the same
5	Confidentiality or non-disclosure agreements	Sensitive Information can be disclosed to the unauthorized person.	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented
6	Policies for Information Security	Without having policy, any and every information can be shared by the employees to any person without any control.	An information security policy document shall be approved by management and published and communicated to all employees and relevant external parties.
7	Review of the policies for Information Security	Decisions related to information security by the management would not be incorporated timely which may lead to information loss.	The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
8	Access Control Policy	Possibility of unauthorized access.	An access control policy shall be established, documented and reviewed based on business and information security requirements
9	Information transfer policies and procedures	Information may not be transferred securely and threat of unauthorized access.	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities
10	Technical review of applications after operating platform changes	Chances of ports exposed to external environment causing threat of information/ data loss.	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

Sl. No.	Vulnerability	Threat	Recommendation
11	Information security policy for supplier relationships	Chances of information sharing outside the organization without any approval can pose risks and legal actions.	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.
12	Documented operating procedures on incident management, business continuity, disaster management, archival procedures and data classification	This can lead to communication gaps, time & cost over runs and loss of data in event of disaster.	Operating procedures shall be documented, maintained and made available to all users who need them.
13	Information security awareness, education and training	Non-Compliance to Information Security policies defined by organization thus results in data/ information loss.	An information security awareness program should be established in line with the organization's information security policies and relevant procedures, taking into consideration the organization's information to be protected and the controls that have been implemented to protect the information. Information security education and training should take place periodically.
14	Classifications of Information	Employees would not understand their responsibility against each type of data like Official Data, Confidential Data, Private Data and Public Data.	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

Table 37: List of Vulnerabilities and Threats

3.6.8 Security Controls

Failure to protect information assets from loss, destruction or unexpected alteration can result in significant impact to productivity, reputation or financial loss to Government of Meghalaya. Security controls derived assess the current state of Information Security and recommends the solution to bridge the gaps.

Basis the output of the risk assessment that contains description of threats, vulnerabilities, measure of the risk, and recommendations on controls for different layers of security reference model of IndEA, below are the necessary security controls along with the risk assessment against each security control and recommendation to bridge the gap

Security Controls	Current Risk Assessment	Impact on non-compliance	Recommendation
Application whitelisting of permitted / trusted programs.	Not Implemented	Possibility of malware, phishing attack and other such security breach	• Consider using application whitelisting technologies already built into the host operating system • Choose best fit product and deploy in user devices in a phased manner
Periodic patching of applications, with the latest versions.	Not Implemented	High threats of application security intrusions and cyber attacks	• Modernize application technology stack • Deploy patches as batch jobs through effective support and impact assessment
Periodic patching of operating system vulnerabilities.	Not Implemented	High threats of security breaches and cyber-attacks	• Modernize OS technology stack • • Deploy patches as batch jobs through effective support and impact assessment

Security Controls	Current Risk Assessment	Impact on non-compliance	Recommendation
Access to sensitive information must only be granted based on principle of least privilege, it translates to giving people the lowest level of user rights that they can have and still do their jobs.	Not Implemented	High risk of information theft and security breach through system or administration accesses	• Define security access requirements • Draft access requirement guidelines and checklist • Document access privilege grant history • Audit access of systems procedures and outcomes • Develop incidence management and response procedures
Automated dynamic analysis of email ,web content and filtering	Not Implemented	Risk of malware/virus attack/ phishing attack	• Implement tool for web and email content security • Develop incidence management and response procedures
Host-based intrusion detection and prevention system to identify anomalous behaviours.	Not Assessed	Risk of data theft through malware and virus attack	• Implement tool for intrusion detection system
Network segmentation and segregation, to isolate portions in case of incidents.	Not Assessed	Cyber attackers gain access to a network and can monitor or steal sensitive information, but without making any change to the data, leaving it intact – example: Endpoint attacks, Malware attacks, Advanced persistent threats, etc.	• Implementation of demilitarised zones and gateways between networks with different security requirements • Implementing server and domain isolation using Internet Protocol Security (IPsec). • Implementing storage-based segmentation and filtering using technologies such as disk and volume encryption and Logical Unit Number masking.
Multi-factor authentication, especially for remote access (e.g. via VPN).	Implemented	User connection being exposed while using public(insecure) WiFi, possibility of detection of web activity	This is already implemented; detailed assessment is required for extension of the technology
Software-based application firewall to block both incoming and outgoing network traffic.	Partially Implemented	Threats in the form of SQL injections, parameter and cookie tampering, and cross-site scripting.	Implementation of web application firewalls (WAFs) to filter, monitor, and block HTTP/S traffic to and from a web application, specifically
Centralised logging of successful and failed computer events.	Not Assessed	Inability to identify security intrusion attempts from different devices	Implementation of centralized event log management systems
Centralised logging of allowed and blocked network activity.	Not Assessed	Inability to identify network security intrusion attempts	Implementation of centralized event log management systems
Web-domain whitelisting for all domains.	Not Assessed	Possibility of malware, phishing attack and other such security breach	• Consider using network whitelisting technologies already built into the host operating system • Choose best fit product and deploy in user devices in a phased manner
Workstation configuration management based on standard operating environment and disabling unneeded / undesired functionalities.	Not Implemented	Data theft through portable storage devices, possibility of spyware or malware attack from different ports (connected devices),	• Implementation of workstation configuration policy • Implementation of software patches to disable functionalities • Implementation of SOPs and system for exception processing
Denial of direct internet access for workstations, with clear process for exceptions.	Not Implemented	Data theft through direct internet access possibility of spyware or	• Implementation of workstation browser configuration policy

Security Controls	Current Risk Assessment	Impact on non-compliance	Recommendation
		malware attack from websites	• Implementation of software patches Implementation of SOPs and system for exception processing
Enforce a strong password policy covering complexity, length and validity aspects.	Not Implemented	High threat of data leakages, unauthorized accesses	• Implementation of password policy • Patches to update/notify/de-activate user basis password policy
User application configuration hardening to disable running of internet based code, untrusted macros etc.	Not Implemented	Data theft through portable storage devices, possibility of spyware or malware attack from different ports (connected devices),	• Implementation of workstation configuration policy • Implementation of software patches to disable functionalities • Implementation of SOPs and system for exception processing
An appropriate set of procedures for data classification has been developed and implemented in accordance with the MeghEA data classification scheme	Not Implemented	Unauthorized access to data, data leakage, possibility of protected or unmasked data being shared, loss of confidential information	• Classification of data entities as MeghEA data classification framework • Implementation of security controls per data category • Implementation of tools and processes • Governance and monitoring
Implementation of data archival policy with data entity specific retention period , process for data revival and process for data disposal/destruction	Not Implemented	Loss of data owing to issues with operational systems.	• Draft data archival process • Implementation of SOPs for data retrieval • Implementation of tools and processes • Governance and monitoring
An effective incident management process is in place for quick response to information security breaches or incidents	Not Implemented	Lack of response to security incidents may prevent immediate controls and measures on security threats or intrusion	Document incidence response procedure and implement tools and process for incidence response management
A business continuity management framework and business continuity plan is in place to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters	Not Implemented	Loss of data owing to natural or man-made calamities.	• Draft BCP management plan • Implementation of SOPs for BCP • Implementation of tools and processes • Governance and monitoring
An effective cryptographic algorithm is in place that limit access to the data to those that hold the proper encryption (and decryption) keys	Not Implemented	Loss of data, data theft through employee (with high privilege) led intentional or unintentional events	Implement and closely monitor data centre and administrative privileged users
Data storage is executed through well-defined procedures that includes type of data file to be stored, medium of storage and back-up device	Not Implemented	Loss of data, unavailability of back-up data	• Outline data types and corresponding storage device • Derive state metadata model adherence and store basis of type of file in corresponding devices

Table 38: Security Controls

Additional security measures:

Apart from the above controls, following measures are necessary that would ensure holistic coverage aligned to IndEA security layers:

ISO: 27001 Compliance for State Data Centre: Though migration to cloud of various systems and data is planned as per MeghEA, State Data Centre needs to go for ISO: 27001 standards compliance. Following are the areas that require intervention:

Management aspect : Security policy, Organization of information security, asset management, compliance, human resource security, business continuity management, communications and operations management.

Technical Aspect : Access control, information security incident management, information system acquisition, development & maintenance, physical and environment security.

4. Architecture Implementation Framework and Action Plan

4.1 Implementation Framework

Strategic Pillar nodal departments and MeghEA architects would work together to understand and deliver around major Government strategies (e.g., Primary Sector). The central EA management team of MeghEA ensures that strategic execution is consistent with other architecture efforts.

There must be clear and distinct roles and responsibilities to implement the architecture. While the common systems, core platform, EA principles and standards would be defined by the MeghEA central team, the implementation responsibility would rely on the Nodal department and Nodal officers.

MeghEA responsibility Triad

The key entities that would drive the architecture implementation are:

- **MeghEA State Team** – The core MeghEA team that would drive the state-wide architecture implementation and would undertake responsibilities to upgrade or refresh the architecture.
- **Strategic Pillar- Nodal Team** – The strategy pillar EA team that would drive the architecture implementation for the respective pillar. There would be SIX such teams.
- **Department Team** – The respective department teams that would implement the services facilitated by above two team .

Below graphical representation explains the responsibilities of each of the teams (in the triad)

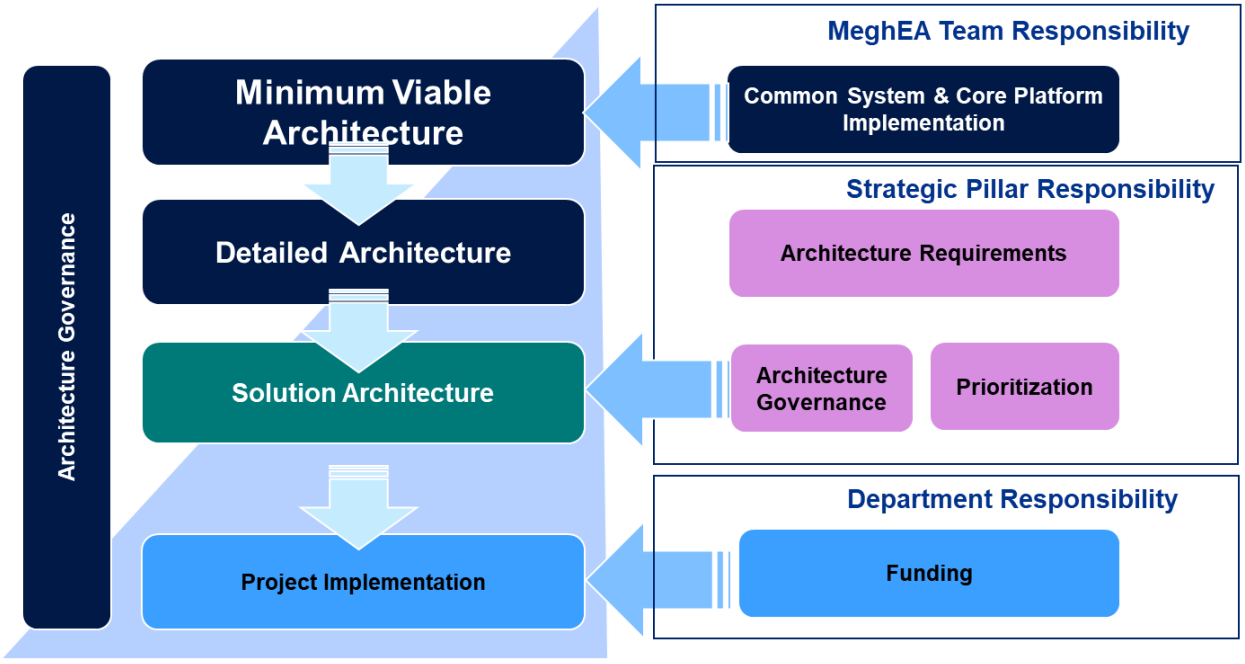


Figure 35: MeghEA Responsibility Triad

Minimum Viable Architecture Implementation (MVA)

As elaborated in the MeghEA: Main Document – Detailed Architecture Requirement, MVA implementation would primarily be executed in 3 phases.

- **Phase-1**: This phase consists of implementation of MANDATORY common systems that are needed for implementation of digital services.
- **Phase-2**: This phase consists of implementation of key common systems that are needed for implementation of digital service considering end-to-end whole-of-service scope.
- **Phase-3**: This phase consists of implementation of common systems that are needed for implementation of specific services.

Please refer "MeghEA Blueprint" for detailed roadmap.

The MVA phases may or may not coincide with the implementation of Strategic Pillar. The common systems and core platform would enable and facilitate implementation of digital services in Strategic pillar. Critical components of MVA needs to be developed before full scale implementation of any strategic pillar.

Primary Responsibility: MeghEA State Team

Detailed Architecture Requirement

Detailed architecture consists of architecture requirements of SIX pillars. Each of the pillars would have a nodal officer leading the team of officers from all other departments. The below table represents the nodal departments for each pillar.

Strategic/Cross-cutting Pillar	Nodal Department
Primary Sector	Agriculture & Farmers' Welfare Department
Infrastructure	Public Health Engineering Department
Human Development	Health & Family Welfare Department
Entrepreneurship	Tourism Department
Governance	Planning Department
Environment	Forest & Environment Department

Table 39: Nodal Department for Strategic & Cross-Cutting Pillars

Primary Responsibility: MeghEA State Team

Solution Architecture

The solution architecture would be derived by the Nodal department for each Strategic/Cross-cutting pillar, facilitated by external consultants or internal recruits with required domain and technical expertise.

Primary Responsibility: Strategic Pillar Nodal Officer Team

Project Implementation

The project implementation would be holistic implementation of roadmap as designed in the solution architecture.

Primary Responsibility: Strategic Pillar Nodal Officer Team

4.2 Detailed Architecture Requirement: Action Plan

The Primary Sector action plan is segregated to four stages:

- **Stage 1:** Governance & Coordination Team – This stage would deal with formation of the MeghEA Governance and Project Coordination Team.
- **Stage 2:** Solution Architecture – This stage would deal with the procurement of expert for solution architecture and finalization of the solution architecture.

- **Stage 3:** Implementation – This stage would deal with IT development, infrastructure procurement and deployment.
- **Stage 4**: Change Management – This stage implements key regulatory changes, legal changes and change management that includes training.

Below is a graphical representation of the same:

Figure 36: Action Plan

Stage 1: Governance & Coordination Team

The stage includes key activities that are necessary for future state architecture realization of the Strategic-Pillar. The activities are listed below:

Activities	Responsibility
Derive MeghEA Governance mechanism that includes Enterprise Architecture Operating Model, EA Governance processes.	MeghEA Consulting Team
Select and notify Nodal Officer for the pillar; notify nodal officers for all included departments.	Planning Department
Formulate necessary Government Orders for implementation of Digital Services, formation of governance team and other legal aspects.	Planning Department
In this stage, finalization of service list for digital implementation is also undertaken	Strategic Pillar Nodal Department
Finalization of service levels (timeline for service delivery).	Department HoDs
Estimation and finalization of implementation budget. Share of funding between departments.	Department HoDs

Table 40: Governance Team Responsibility

Stage 2: Detailed Functional Requirements & Solution Architecture

The stage includes key activities such as Solution Architecture Experts procurement, on-boarding and finalization. The activities are listed below:

Activities	Responsibility
Finalization of process models for all prioritized services	Strategic Pillar Nodal Department
Derive IT system requirements	PMU

Activities	Responsibility
• Modules • Service mapping • Micro services/application services • Application communication requirements	
Derive Data architecture – Physical data models, data integration model and other data requirement basis of MeghEA: Detailed Architecture Requirement	PMU
Derive Technology architecture of the Primary Sector	PMU
Define and finalize implementation roadmap of services, systems and other key changes	PMU

Table 41: FRS & Solution Architecture Responsibility

Stage 3: Implementation

Implementation stage includes IT system development, IT infrastructure procurement and project management. The activities are listed below:

Activities	Responsibility
Finalize functional and technical requirements	Solution Architecture Experts
Procurement of System Integrator OR notification to NIC for implementation	Nodal Officers
Monitoring and project management of the intended systems and process	Nodal Officers/ Project Management Team
Procurement of IT and other Infrastructure	• Department HoDs • Coordination by: Nodal Officers
Final approval of digital services	Departments

Table 42: Implementation Responsibility

Stage 4: Change Management

Change management stage includes legal, regulatory changes and training. The activities are listed below:

Activities	Responsibility
Government Orders, Right to Service Act and other key regulatory changes	Department Nodal Officers
Finalization of training manual and trainings	System Integrator
Implementation of system	System Integrator
Implementation issue resolution	System Integrator

Table 43: Change Management Responsibility

5. MeghEA: Change Impact Analysis

One of the objectives of MeghEA is to make Government of Meghalaya(GoM) function as a high-performing government agency resembling well-run private companies. Comprising of goals; well-designed, rational processes; strict accountability; and effective leadership. But the profound scope and complexities in the purposes, the cultures, and the contexts within which GoM operates leads to different obstacles. The greatest challenge in bringing about successful change and significant, sustained performance improvement in the GoM is not so much identifying solutions, which are mostly straightforward, as working around unique obstacles:

Leadership : Department centric approach and frequent change of department secretaries creates continuity challenge, directional change and delay in decision making.

Processes: Processes and rules, originally adopted to prevent public-sector wrongdoing, have created workplaces that are significantly less flexible and old.

People: Owing to strict hierarchical structure and democratic decision-making approach, a single disapproval creates hindrance in implementation, this leads to delay and loss of interest.

MeghEA would have a holistic approach to ensure a plan is undertaken considering all of the above obstacles.

Figure 37: Change Impact Analysis Approach

1. **Goals & Success Measures** : The SDG has been assigned to each pillar, with indicators relevant to the goals assigned to departments responsible for attaining the goals. Further to this, following are the action points:
    - Government notification on goal assignment to departments along requirement to create attainable targets in 2022, 2024, 2026 and 2028.
    - SDG dashboard implementation that would measure the achievement of indicators.
    - Bi-annual meeting headed by Planning department on progress, issues and actions.
2. **Understand Roles** : In this step, relevant officials from Government needs to be identified:
    - Identification of Nodal Officer of Pillars and backup.
    - Identification of department nodal officers and backup.
    - Formation of MeghEA core team(Please refer “MeghEA Blueprint” for details).

3. **Budget & Planning** : The implementation plan needs to be based on the roadmap (Please refer "MeghEA Blueprint" for details). For budgeting the options are described below:
    - A state pool of funds for MeghEA implementation, segregation of fund to pillars basis Government priority.
    - Shared fund among departments within a pillar, the proportion of investment of department would depend on various factors such as share of services among total service planned for implementation.
4. **Procedure Design** : The MeghEA operating model would detail the procedures for :
    - Architecture reviews
    - Implementation Governance
    - IT Procurement

Please refer "MeghEA Blueprint" for details around key policy interventions for MeghEA.

5. **Awareness & Branding** : Build awareness across the Government and public to gather advocacy. Socialize ideas, objectives, and identify change enablers and champions are some of key objectives of this step. Following are the high-level activities:
    - Socialize MeghEA Vision and Mission through portal, social media and specific posters.
    - Organize sensitization sessions at least once in a quarter, involving department officers.
6. **Training and capacity building**: Organize training sessions on architecture for following sets of stakeholders:
    - All pillar and department nodal officers.
    - Basic architecture training for department leadership.

6. MeghEA Value Realization

MeghEA Detailed Architecture Requirements Documents have derived the key changes that are required at people, process and technology level. However, there is a significant effort required in realization of the desired objective of MeghEA. MeghEA has set a vision " Making Meghalaya The Digital Abode" By Connecting, Collaborating and Empowering Citizens, Businesses & Employees with empathy. In order to realize the vision, there are few steps that needs to be undertaken with careful consideration of the risk of the transformation. This section outlines how architecture requirements would facilitate the implementation through industry standard methodology through an illustrative example of a service

The value realization is described using the following key steps:

1. Use Case description
2. Use Case ArchiMate Model
3. Business Process Model
4. Functional Requirement Specifications
5. Component Diagram UML

6.1 Use Case Description

Illustrative Service: Financial Assistance for Production Activities

SDG the service relates to: Goal 2. End hunger, achieve food security and improved nutrition and promote sustainable agriculture

Key Indicators that the service aims to achieve:

- Growth (percentage) in gross Agriculture expenditure Y-o-Y.
- Percentage of growth of export subsidy to agriculture exports

Use Case Steps: Farmers applies for financial assistance for production activities under different schemes.

Key Activities: As per farming needs and area of cultivation land, farmers apply for the financial assistance through digital platform by providing various details.

Architecture Building Blocks: Workflow.

Use Case Steps: Checking of Eligibility and Funds.

Key Activities: System/ District/ Block officer checks eligibility and funds of that particular production activity under scheme and provide approval. The approval details are notified to the applicant farmers through SMS and app notifications.

Architecture Building Blocks: Workflow, Messaging.

Use Case Steps: Funds transferred to beneficiary account.

Key Activities: As per eligibility, funds will be transferred to bank account of farmer through TreasuryNet system.

Architecture Building Blocks: Messaging, Workflow, Financial Management.

6.2 Use Case ArchiMate Model

The above use cases are illustrated in industry standard notation **ArchiMate** (ArchiMate is an open and independent enterprise architecture modeling language)

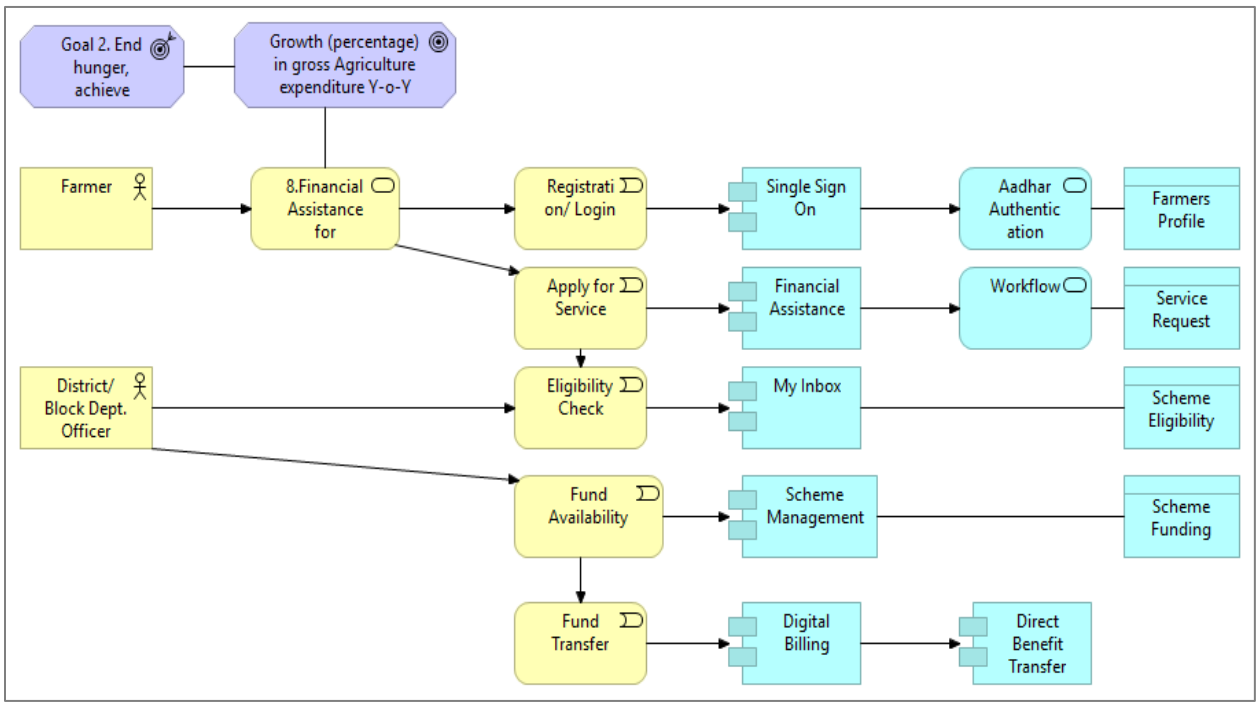


Figure 38: Use Case Model Diagram

It is recommended to derive the future state business process model post deriving the architecture use cases. Use case models enable holistic architecture approach while business process model provides a view of the various steps and activities from application to service completion. Business Process Re-engineering principles from IndEA must be followed to ensure a thorough and holistic BPR. Below diagram illustrates the business process model using industry standard notation–BPMN.

6.3 Business Process Model

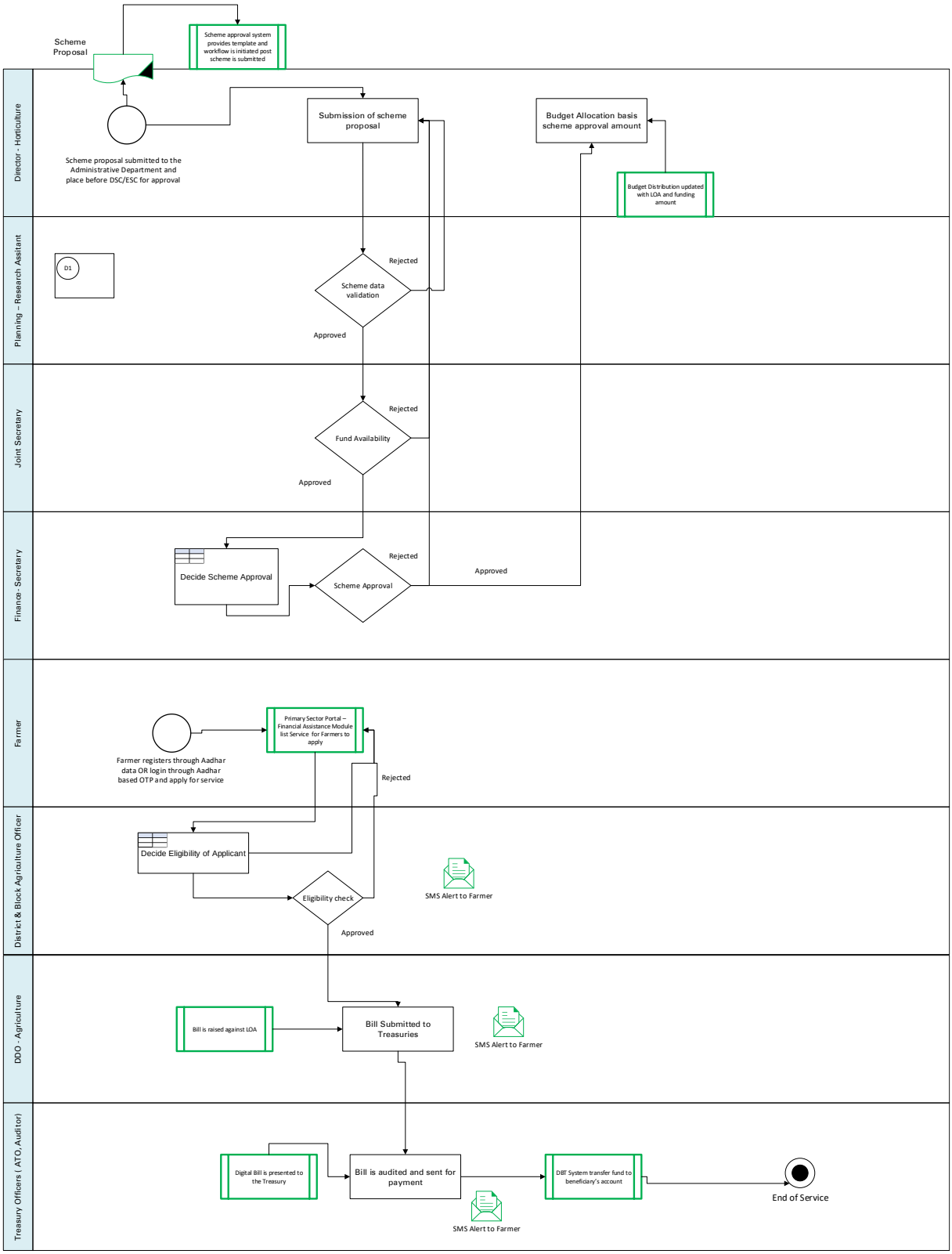


Figure 39: Business Process Model using BPMN

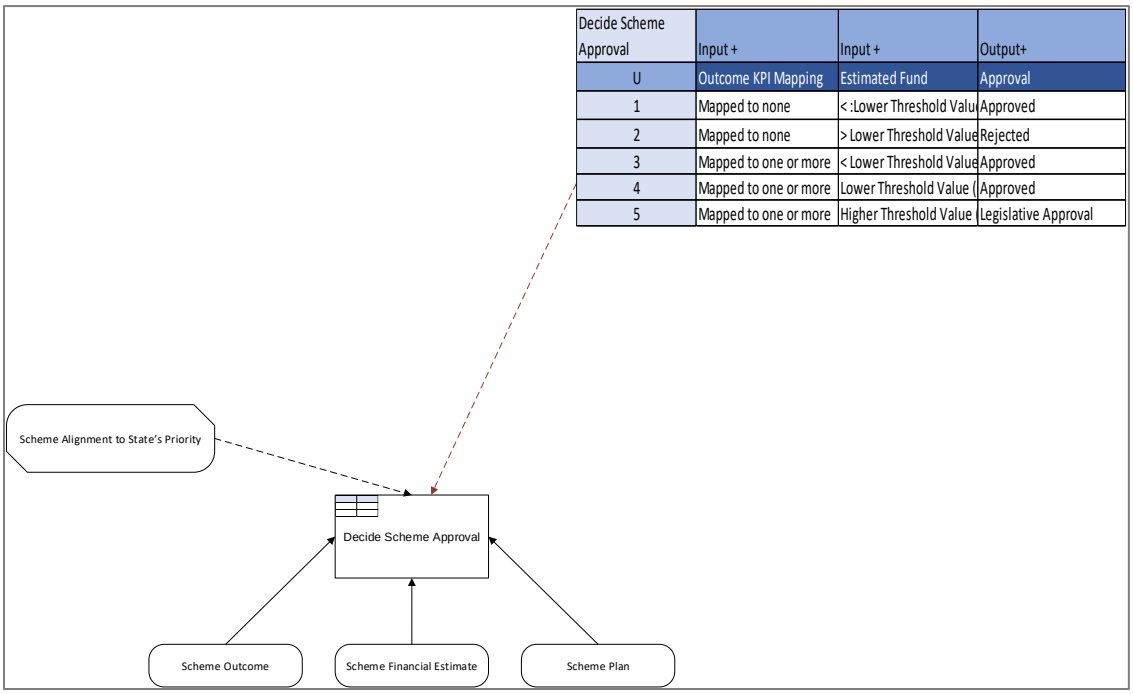
As outlined in the business process model, there are two key decision steps:

- Scheme Approval
- Applicants Eligibility for the service/scheme

There is a need of Decision Model and Notation(DMN) to provide the constructs that are needed to model decisions, so that decision making of Primary Sector (Agriculture & FW) can be readily depicted in diagrams, accurately defined by business analysts, and (optionally) automated. Decision-making is addressed from two different perspectives by existing modeling standards:

Business process models (described in previous section) can describe the coordination of decision-making within business processes by defining specific tasks or activities within which the decision-making takes place. Decision logic can define the specific logic used to make individual decisions, in this case DMN will provide a third perspective – the Decision Requirements Diagram – forming a bridge between business process models and decision logic models.

The two key decision steps are illustrated by the required Decision Requirements Diagrams:



Decide Scheme Approval	Input +	Input +	Output+
U	Outcome KPI Mapping	Estimated Fund	Approval
1	Mapped to none	< :Lower Threshold Valu	Approved
2	Mapped to none	> Lower Threshold Value	Rejected
3	Mapped to one or more	< Lower Threshold Value	Approved
4	Mapped to one or more	Lower Threshold Value (	Approved
5	Mapped to one or more	Higher Threshold Value	Legislative Approval

Figure 40: DRD- Decide Scheme Approval

Scheme Approval decision making would need specific KPIs that would be derived from the strategic goals of the department. These KPIs may have some overlapping with SDG KPIs but would largely be more department program centric. The KPIs would also be derived from existing budget estimates and spending under each head of account.

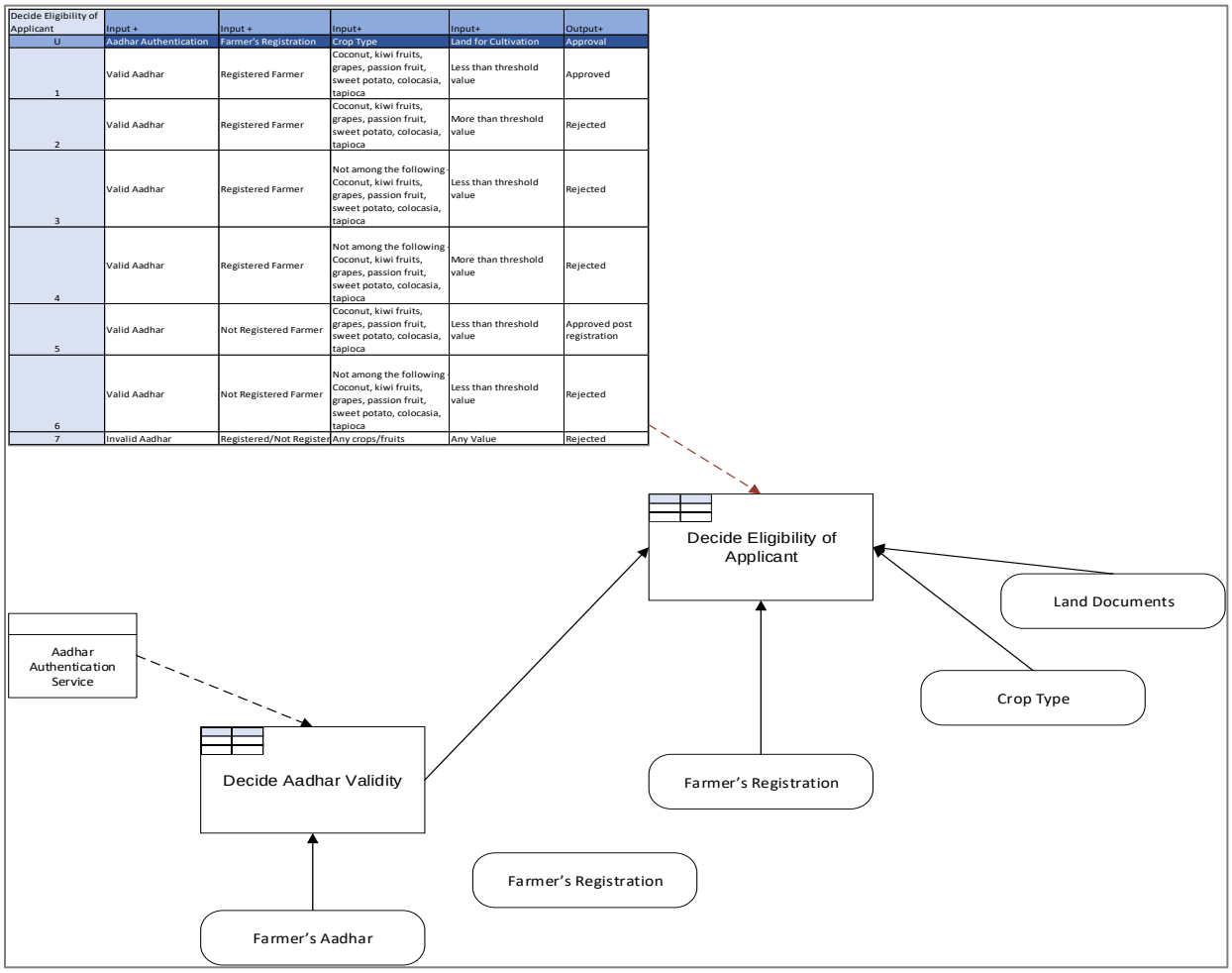


Figure 41: DRD- Decide Eligibility of Applicant

6.4 Functional Requirement Specifications

Post Business Process modelling , it is essential to derive the system functional requirements to enable the development team to implement the system. Below is the Functional Requirement Specifications for the service implementation

S. No	Functional Requirement Specifications
1	System must make "Scheme Management" system available for the Director of Horticulture to enable him/her to create the scheme
2	Scheme management module must provide the option of creating new schemes
3	Scheme management module must provide the template to create new scheme along with necessary data fields
4	Scheme management module must provide the flexibility to "SAVE" draft scheme
5	Scheme management module must provide the ability to submit scheme
6	System must send notification in the form of SMS & Email to the Secretary Agriculture and Farmers Welfare about the scheme approval request
7	System must make "Scheme management module" available for the Secretary Agriculture and Farmers Welfare to enable him/her to verify the submitted scheme
8	System must make "Scheme management module" available for the Secretary Agriculture and Farmers Welfare to enable him/her to submit scheme
9	System must send notification in the form of SMS & Email to the Research Assistant about the scheme approval request
10	System must make "Scheme management module" available for the Research Assistant in Planning department to enable him/her to verify the scheme details for checking completion

S. No	Functional Requirement Specifications
11	System must make "Scheme management module" available for the Research Assistant in Planning department to enable him/her to submit scheme
12	System must send notification in the form of SMS & Email to the Joint Secretary – Planning Department about the scheme approval request
13	System must make "Scheme management module" available for the Joint Secretary in Planning department to enable him/her to verify the scheme details for checking availability of State fund
14	System must make "Scheme management module" available for the Joint Secretary in Planning department to enable him/her to submit scheme
15	System must send notification in the form of SMS & Email to the Secretary – Planning Department about the scheme approval request
16	System must make "Scheme management module" available for the Secretary in Planning department to enable him/her to verify the scheme details
17	System must make "Scheme management module" available for the Secretary in Planning department to enable him/her to submit scheme
18	System should make "Apply Financial Assistance" module available to the Farmers to enable them to apply for the service – "Financial Assistance for Production Activities"
19	System must provide the option to register the farmer
20	System must have the provision to enable Aadhar details verification through One Time Password
21	System must be able to store the Farmers details such as Name, Aadhar (Virtual ID), Address and provide farmers ID in SMS
22	System must be able to enable farmer to login through Aadhar based verification (for previously registered farmer)
23	System must be able fetch details of farmers from existing record against Aadhar
24	System must pre-populate service application form basis pre-filled data
25	Service application form may only require few fields basis service, all common data should be pre-filled
26	System must provide farmer ability to submit service request
27	System must generate unique service request number for the applied service
28	System must provide SMS and email alert along with the service request number to the farmer
29	System must notify District/Block Agriculture department officer about the service request
30	System must make the service request available in the "Inbox" module of the District/Block Agriculture department officer
31	System must facilitate District/Block Agriculture department officer to verify service eligibility and application details. Please note service eligibility MAY be verified by system through pre-filled data, this is a preference not a mandate
32	System must allow the District/Block Agriculture department officer to approve or reject the service
33	System must allow District/Block Agriculture department officer to provide the text-based response to the service with regards to its approval or rejection
34	System must provide SMS alert to farmer about the status of the service post action from District/Block Agriculture department officer
35	System must allow DDO to create the bill from Governance Portal -> Finance-> Digital Billing against the allocated fund for the scheme. System must create the bill automatically, DDO would need to verify and submit the bill
36	System must send API request to Governance Portal -> Finance-> Digital Billing to create automated bill for approval
37	System must make "Digital Billing" module available for the Treasury officer to enable him/her to audit and approve the bill
38	System must send fund transfer request to enable transfer of fund to beneficiaries
39	System must send SMS notification to farmer on the amount transferred to his/her bank account

Table 44: Functional Requirement Specifications

6.5 Component Diagram

The envisioned architecture pattern is Micro-Service based architecture for the system planned for development. Aligning to the Business Capability Model derived in Pillar documents (please refer pillar documents – "Business Capability" section), the micro services identified are listed below

Micro-Service	Description
Beneficiary Identification	Micro-service to identify citizen that applies for the service and associate the citizen with Farmers ID from existing database of farmers
Beneficiary Authorization	Micro-service to authorize login of citizen and provide necessary access to apply service
Beneficiary Aadhar Verification	Micro-service to verify Aadhar data entered by beneficiary and pull relevant details from UIDAI database for further processing of service application
Beneficiary Registration	Micro-service to help citizen register themselves in state portal for application for any service.
Notification	Micro-service to send SMS/email-based notification to citizens, employees and relevant stakeholders
Service Status	Micro-service to identify status of the service that has been applied for processing
Service List	Micro-service that stores currently operational list of services along with unique service id
Service Eligibility	Micro-service that returns the eligibility status of the applicant for the selected service. Please note this does not processes the eligibility
Scheme Funding	Micro-service that returns the amount of funding that is approved but not availed for a particular service associated with a scheme
Scheme Creation	Scheme creation service facilitate creation of scheme based on predefined template and requirement
Scheme Update	Micro-service to update details of a scheme

Table 45: Micro Service List (Tentative)

The above list of Micro-services works in a synchronized manner termed as Choreography to perform one or more application service. It is necessary to describe the function of the above Micro-Services through a component diagram to illustrate how these Micro-services would work together to deliver the business services. A component diagram facilitates visual representation of the system and would facilitate construction of executables by using forward and reverse engineering. Refer ArchiMate to understand the different notations followed in the diagram below:

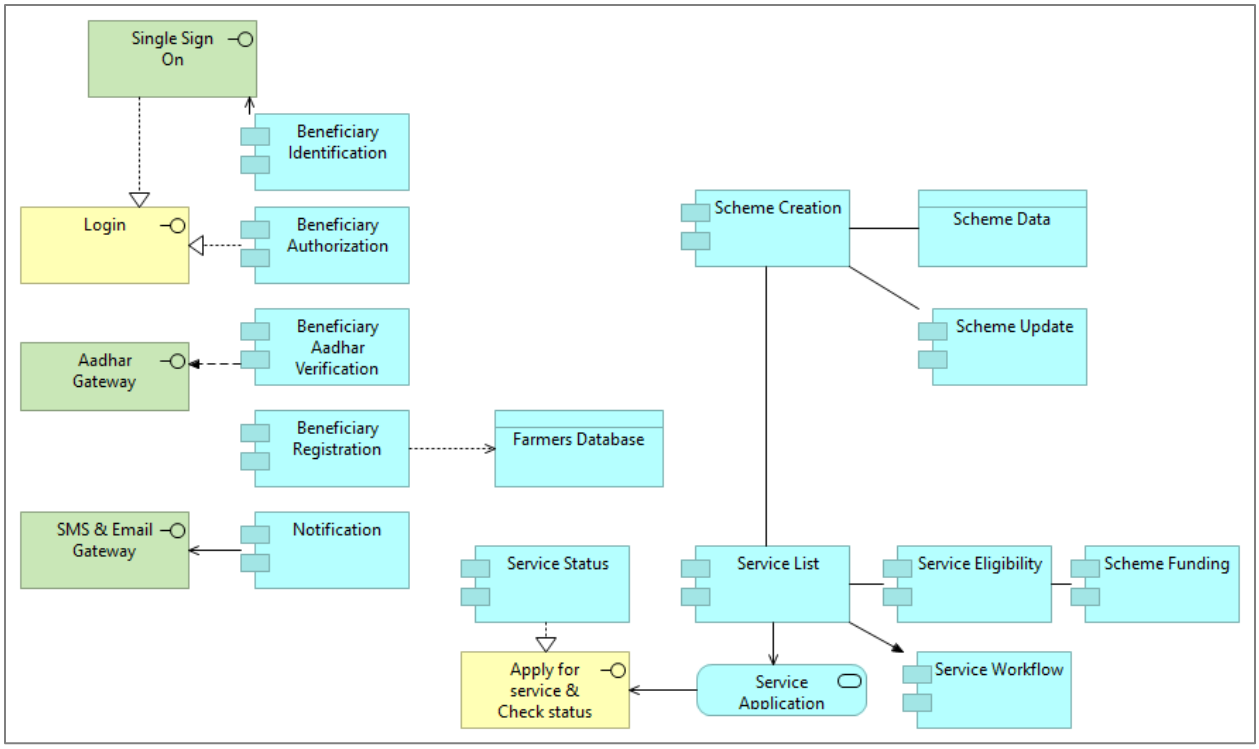


Figure 42: Component Diagram

7. Annexure

7.1 Performance Architecture Principles

Name	Performance measurement must be linked to Goals and Indicators aligned to State's Growth Agenda
Statement	Performance measurement must be linked to Goals and Indicators aligned to State's Growth Agenda – the strategic and cross-cutting pillars
Rationale	Performance measurement when linked to Goals and indicators , provides a measurable parameter to understand the progress, the achievement and the benefit. The Goals and indicators must be outcome oriented to measure service delivery outcome, however, certain indicators might be there to measure internal process improvement.
Implications	• Provide a ONE Government experience – Unified and Uniform Interfaces. • The one government foundational capability aims to provide seamless delivery of services to various stakeholders by integrating various departments through enterprise service integration. The initiative would cut across departments, making them collaborate to deliver services, appearing as a "One Government" to the service beneficiary.

7.2 Business Architecture Principles

Name	Integrated Services
Statement	Integrated Services that cut across department-silos are identified, designed and delivered through multiple delivery channels, to realize the vision of ONE Government.
Rationale	Government of Meghalaya envisages to provide seamless services to the citizens through possible Integration Services. Various departments delivering similar services have been brought together to form pillars and brought on one platform through enterprise service integration to deliver services end to end and provide ONE Government experience to the citizens.
Implications	• Provide a ONE Government experience – Unified and Uniform Interfaces. • The one government foundational capability aims to provide seamless delivery of services to various stakeholders by integrating various departments through enterprise service integration. The initiative would cut across departments, making them collaborate to deliver services, appearing as a "One Government" to the service beneficiary.

Name	Maximization of Benefit
Statement	All Information Management decisions are made to maximize the benefit to Government as a whole.
Rationale	Any decisions made from enterprise (Whole-of-Government) perspective will have greater long-term benefits than the decisions made from that of an individual department. In this process, some departments may have to concede their own preferences to the greater benefit of the enterprise (Government).
Implications	• Achieving maximum state-wide benefit will require changes in the way services are designed and information is managed. Technology alone will not bring about this change. • Application development priorities must be established by the entire enterprise for the entire enterprise. • Applications components should be shared across organizational boundaries.

	• As needs arise, priorities must be adjusted. A forum with comprehensive enterprise representation should make these decisions.

Name	Business Process Re-Engineering
Statement	Existing processes are re-engineered to eliminate non-value-adds and to make the services citizen-centric /business-centric.
Rationale	Business Process Re-Engineering will help Government of Meghalaya to provide better citizen service, by redesigning the workflows which will enable higher levels of efficiency.
Implications	• BPR will help to assess the challenges and implement new level of performance with better efficiencies and effectiveness to achieve the future objectives and goals. • Automation of existing processes through use of IT and making services of departments available online.

Name	Inclusive Services
Statement	State systems shall be designed to be inclusive.
Rationale	Systems will be designed to reach out to the “unconnected”, digitally illiterate, remote, hilly and tribal areas. All employees and workers would facilitate “unconnected” citizens to avail services from designed systems.
Implications	• Employees and workers would be trained to facilitate citizens to avail services from connected devices. The employees and workers would be facilitated through portable connected devices to deliver services.

Name	Unique State Digital ID
Statement	Unique and Single Digital ID for State Government Service
Rationale	State to focus on linking all IDs to a single unique state Digital ID, to promote integrated services to its beneficiaries.
Implications	• Unification of IDs and mapping with unique Digital ID would necessitate changes in the services from GoI-ministries.

Name	Digitally Deliver Payments related services
Statement	All financial benefits would follow Direct Bank Transfer (DBT) mode of transfer.
Rationale	DBT would eliminate the need for cash transactions reducing any service delivery gap.
Implications	• All financial assistance schemes under the pillars would be brought under the scope of State DBT.

Name	Enable Digital Certificates for all Services
Statement	Enable digital certificate acceptance and issuance through Digital Citizen Locker
Rationale	Accepting digital certificates from citizen locker would promote certificate less governance, reducing several bottlenecks and manual interventions.

Implications	• All universities, boards, other certificates or license issuing organizations under the purview of Government of Meghalaya needs to deliver digital certificates in citizen locker proactively.

7.3 Application Architecture Principles

Name	**One User Interface**
Statement	All user groups shall be provided with One user interface for various business requirements.
Rationale	From an end-user perspective, provide a common software interface even though these may in turn access data from multiple systems and the business rules may be performed through various applications and functions. A common interface will also drive a common branding and consistent look and feel
Implications	User interface for all Departments may need to be developed which provides access to multiple applications. This may need to support Single Sign-On technologies so that users do not need to perform login multiple times. Suitable technology architecture (e.g. Service Oriented Architecture and Integration Platform) may need to be developed which can integrate multiple software applications and data stores. User interface will lead to better productivity and cut back on training time.

Name	**Sharing & Reusability**
Statement	All commonly used Applications built part of MeghEA common application to be used and deployed for all departments. One single application for logical set of cross cutting and supporting business services.
Rationale	Common systems built for MeghEA would deliver common functionality for all departments, eliminating duplicate systems and saving Government cost and time
Implications	• Lower cost to the Government – shared system would mean reduced duplicity and hence impact cost of ownership • Standardization of support services

Name	**Technology Independence**
Statement	Application Design for department systems to be based on open standards and these would be technology-independent
Rationale	To promote interoperability for applications and prevent any technology vendor locks; all applications needs to be designed to factor technology independence. The application would share data through APIs and process rules through configurable interfaces
Implications	Applications would be loosely coupled from each other; leading to an architecture that is easily replaceable in the future

Name	**Loosely Coupled Application Architecture**
Statement	All IT Systems in Finance department to be developed MUST have features and functionality that are made available as loosely coupled, self-contained, standards based and configurable services
Rationale	• Loose coupling promotes interoperability between systems in a seamless manner. This is critical for the planned integration and collaboration principle • Reusable application components are key to increased productivity and rapid application deployment. The application communication middleware supports a loosely coupled design to be interoperable with other components
Implications	• Systems needs to API friendly and designed in standards-based, interoperable specifications or protocols that provide a contract-based interaction between Service consumers and providers

Name	Adherence to Non-Functional Requirement
Statement	Adhere to all the Non-Functional criteria for Service Window of availability, Disaster Recovery, Scalability, Maintainability, Configuration Management Software Development Life Cycle, Build and Deployment process.
Rationale	IT systems must meet the set of non-functional requirements for availability, performance and reliability to each set of stakeholders. Non-functional requirements should get adequate emphasis during design/selection and roll out of software systems.
Implications	IT systems need to be designed to cater to well-defined non-functional requirements relevant for Finance Department. This will help ensure that IT performance is commensurate with business needs and expectations. It would be required to maintain a set of non-functional requirements for availability, performance and reliability and the overall IT architecture needs to be supportive of the same.

Name	Applications to interoperate using integration platform
Statement	All applications to interoperate using integration platform only
Rationale	Integration platform would manage the traffic, perform transformation and other allied activities to facilitate smooth and efficient integration
Implications	• Elimination of API based Enterprise Application Integration • Elimination of data level integration • All system needs to be designed to enable data sharing via APIs/services registered in integration platform

7.4 Data Architecture Principles

Name	Data-sharing
Statement	All Department users have access to the data, necessary to perform their duties; therefore, data is shared across departments, branches and other government agencies to deliver services.
Rationale	Timely access to accurate data is essential to improving the quality and efficiency of service delivery and decision-making. It is less costly to maintain timely, accurate data in a single application, and then share it, than it is to maintain duplicative data in multiple applications. The speed of data collection, creation, transfer, and assimilation is driven by the ability of the department to efficiently share these islands of data across the pillar(s).
Implications	• For both the short term and the long term we must adopt common methods and tools for creating, maintaining, and accessing the data shared across the enterprise. • Data sharing will require a significant cultural change. • Under no circumstances will the data sharing principle cause confidential data to be compromised. • Data made available for sharing will have to be relied upon by all users to execute their respective tasks. This will ensure that only the most accurate and timely data is relied upon for decision-making. Shared data will become the state-wide "virtual single source" of data.

Name	Data-asset
Statement	Data is an asset that has a specific and measurable value to the Government and is managed accordingly.
Rationale	Data is a valuable state resource; it has real, measurable value. Data is the foundation of decision-making, so data must be managed carefully to ensure that department can rely upon its accuracy and can obtain it when and where we need it.

Implications	• Stewards must have the authority and means to manage the data for which they are accountable. • We must make the cultural transition from "data ownership" thinking to "data stewardship" thinking. • The role of data steward is critical because obsolete, incorrect, or inconsistent data could be passed to enterprise personnel and adversely affect decisions across the enterprise.

Name	**Data-Trustee**
Statement	Each data element has a trustee accountable for data quality, retention and security
Rationale	As the degree of data sharing grows and departments and divisions rely upon common information, it becomes essential that only the data trustee makes decisions about the content of data. Since data can lose its integrity when it is entered multiple times, the data trustee will have sole responsibility for data entry which eliminates redundant human effort and data storage resources and data security.
Implications	• The data trustee will be responsible for meeting quality requirements levied upon the data for which the trustee is accountable. • It is essential that the trustee can provide user confidence in the data based upon attributes such as "data source". • Information should be captured digitally once and immediately validated as close to the source as possible. Quality control measures must be implemented to ensure the integrity of the data. • As a result of sharing data across the enterprise, the trustee is accountable and responsible for the accuracy and currency of their designated data element(s) and, subsequently, must then recognize the importance of this trusteeship responsibility.

Name	**Data Privacy and Security**
Statement	Data is protected from loss, unauthorized use and corruption, through adoption of international standards and best practices, duly protecting the privacy of personal data and confidentiality of sensitive data.
Rationale	Existing Data Privacy and security laws/regulations require the safeguarding of national security and the privacy of data, while permitting free and open access. Pre-decisional, decisional, classified, sensitive, or proprietary information must be protected to avoid unwarranted speculation, misinterpretation, and inappropriate use.
Implications	• Data security safeguards can be put in place to restrict access to "view only", or "never see". Sensitivity restrictions for access to pre-decisional, decisional, classified, sensitive, or proprietary information must be determined. • Security must be designed into data elements from the beginning; it cannot be added later. Systems, data, and technologies must be protected from unauthorized access and manipulation.

Name	**Common Vocabulary and Data Definitions**
Statement	Data is defined consistently throughout all levels of Government, and the definitions are understandable and available to all users.
Rationale	The data used in applications must have a common definition throughout the Departments and divisions to enable sharing of data. A common vocabulary will facilitate communications and enable dialogue to be effective. In addition, it is required to interface systems and exchange data.

Implications	• The Departments must establish the initial common vocabulary, the definitions will be used uniformly throughout the Pillars. • Ambiguities resulting from multiple parochial definitions of data must give way to accepted state-wide definitions and understanding. • Multiple data standardization initiatives need to be co-ordinated. • Functional data administration responsibilities must be assigned.

7.5 Technology Architecture Principles

Name	Technology Independent Architecture
Statement	Architecture to be developed in a technology-neutral manner to avoid captivity to a specific product or implementation method.
Rationale	This principle will control the design of architecture, making it technology agnostic and implementation process agnostic. The adoption solutions must adhere to the architecture requirement not vice-versa, hence, this will prevent vendor lock-ins, product captivity, etc.
Implications	• Policies, standards, and procedures that govern acquisition of technology must be tied directly to this principle. • Technology choices will be constrained by the choices available within the technology blueprint. Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be developed and emplaced.

Name	Open Standards
Statement	Open Standards are adopted in the design and implementation of all greenfield systems. Legacy systems are incentivized to migrate to open standards, where required.
Rationale	Software and hardware should conform to open standards that promote interoperability for data, applications, and technology. Standard adherence would lead to ease of interoperability.
Implications	• All new technology component adoption must go through open standard adherence procedure and architecture compliance assessment. • Legacy systems must be migrated to open standards in the near or long term.

Name	Shared Infrastructure
Statement	IT Infrastructure is shared to ensure optimal utilization and effective maintenance.
Rationale	IT infrastructure needs to be used in shared manner, accommodating systems from other Government of Meghalaya departments and strategic pillars. The deployment needs to be further virtualized to enable effective sharing of infrastructure, ensuring optimal usage.
Implications	• Planned resource utilization for all systems needs to be in place to ensure effective sharing. • Virtualization of data centre is required.

Name	Resilient Architecture
Statement	Infrastructure will be selected and implemented with appropriate emphasis on fault-tolerance, stability, and recoverability to ensure the ongoing capability to support ministry applications.
Rationale	• Infrastructure need to be categorized/ prioritized according to business recovery needs following Continuum of Government guidelines.

	• Product/ solution maturity should be taken into consideration for implementation of system. • Disaster recovery policies and standards need to be developed.
Implications	• Minimize infrastructure and application downtime • Facilitates organized disaster recovery capability. • Protects investment in operational data. • Application data will be secured.

Name	**Optimized Infrastructure**
Statement	All IT system must follow the principle of re-use first then buy, meaning the infrastructure must be shared and re-used by newly developed systems before planning for any procurement.
Rationale	• All infrastructure listing and mapping with applications. • Infrastructure utilization reporting. • New deployment scalability requirement submission. • Re-use use case and approval.
Implications	• Reduce end user operation costs. • Reduce service desk problems. • Reduce security breach and impacts. • Reduce data loss and recovery cost. • Improves in deployment of new application. • Reduce unplanned downtime.

Name	**Network and Connected device at all service delivery centres**
Statement	Network and Connected device at all service delivery centres
Rationale	All healthcare workers and educational institutes would have access to connected digital devices.
Implications	Manual processes such as registry entry, ad-hoc system management would be eliminated.

Name	**Control Technical Diversity**
Statement	Technological diversity is controlled to minimize the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments.
Rationale	There is a real, non-trivial cost of infrastructure required to support alternative technologies for processing environments. There are further infrastructure costs incurred to keep multiple processor constructs interconnected and maintained. Limiting the number of supported components will simplify maintainability and reduce costs. The business advantages of minimum technical diversity include standard packaging of components; predictable implementation impact; predictable valuations and returns; redefined testing; utility status; and increased flexibility to accommodate technological advancements. Common technology across the enterprise brings the benefits of economies of scale to the enterprise. Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology.
Implications	• Policies, standards, and procedures that govern acquisition of technology must be tied directly to this principle. • Technology choices will be constrained by the choices available within the technology blueprint.

	• Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be developed and put in place. • The technology baseline is not being frozen

Name	Interoperability
Statement	Software and hardware should conform to defined standards that promote interoperability for data, applications, and technology.
Rationale	Standards help ensure consistency, thus improving the ability to manage systems and improve user satisfaction, and protect existing IT infrastructure, thus maximizing return on investment and reducing costs. Standards for interoperability additionally help ensure support from multiple vendors for their products and facilitate integration.
Implications	• Interoperability standards and industry standards will be followed unless there is a compelling business reason to implement a non-standard solution. • A process for setting standards, reviewing and revising them periodically, and granting exceptions must be established. • The existing IT platforms must be identified and documented.

7.6 Security Architecture Principles

Name	Data Integrity
Statement	Data is correct, consistent and un-tampered
Rationale	Data residing in various systems needs to be referred in real-time or near real-time to facilitate decision making. Data quality management of the data is the responsibility of the data trustee and data custodian, measures would be taken to correct any data quality issues. Also, data modification to all the in-scope data would be bound by access management rules.
Implications	The data that would be used for reporting and decision making, is devoid of quality issues enabling departments to take key decisions on the data.

Name	Data privacy and confidentiality
Statement	Information is shared on a Need-To-Know basis and is collected/accessed/ modified only by authorized personnel.
Rationale	All data should be classified properly to ensure only authorized access to data. Further, the principle ensure restriction on the availability of classified, proprietary, and sensitive information. Existing laws and regulations require the safeguarding of security and the privacy of data, while permitting free and open access.
Implications	Standards and procedures to be defined to classify or declassify data as public, open, private, official and restricted. Access to information based on a need-to-know policy will force regular reviews of the committee. Security needs must be identified and developed at the data level, not the application level. Data security safeguards can be put in place to restrict access to “view only”. Procedures for designing security into data elements from the beginning to be prepared. Systems, data, and technologies must be protected from unauthorized access and manipulation.

Name	Secure by Design
Statement	Security has to be built into all stages and all aspects of architecture development. Security concerns extend to all the IT activities of the enterprise.
Rationale	Security must cover all architecture domains to ensure a holistic coverage of secured design is

	executed.
Implications	Security by design implies coverage of security aspects in application design to ensure information processing is secured and managed. This may lead to use of IAM solutions to ensure security. Data and technology architecture design also needs to cover the security aspects as well.

Name	Anonymize Personal Health Records
Statement	Anonymize personal records before storing in Personal Health Locker.
Rationale	Aligned to National Digital Health Blueprint; all personal health record would be only stored in personal health locker (at National level).
Implications	Data related to personal health must be stored on personal health locker; these would lead to changes in design of existing systems.

7.7 User Experience Transformation

Meghalaya Enterprise Architecture would look to transform the user experience in several ways. Basis architecture requirements the user experience transformation would be achieved in following areas:

Service Awareness

Service awareness is a key aspect of Government of Meghalaya, MeghEA would look to construct a mechanism of service awareness through systems, service catalogue and social media.

Delivery Channel

MeghEA would look to add several service delivery channels that includes web, mobile, social media, chatbot and unified contact center.

User Experience

Digital Service Standard would be followed to design service user experience. Services would be organized as per life-cycle stages to facilitate service delivery to all stages of citizen's life cycle.

Forms

MeghEA would extensively use digital registries to enable pre-population of service-related forms; eliminating the need for any data entry or minimum data entry.

Alerts and Notifications

Service delivery stages may require interventions from both sides, regular alerts and notifications would enable easier and faster service resolution. It would also eliminate surprises to the beneficiary.

Service Process

Extensive BPR would be carried out to ensure services processes are lean and would be almost always executed through digital channels.

Service Output

Significant re-engineering would be executed at service output level to ensure the beneficiaries get what they want in the simplest format. Certificate less Governance, DigiLocker, and many such measures and tools would be used.

Following sections details out envisioned user transformation for 5 marque service types.

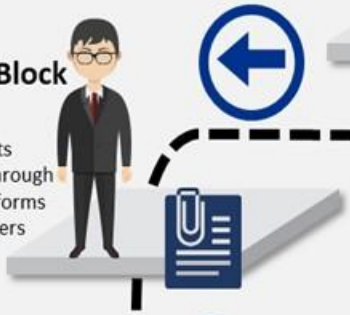
Financial Assistance Service under various schemes to Farmers

Current State User Experience

Farmers Apply
Farmers enquires from community and applies for service

Village Headman
Endorses the farmer's application by classifying him a farmer

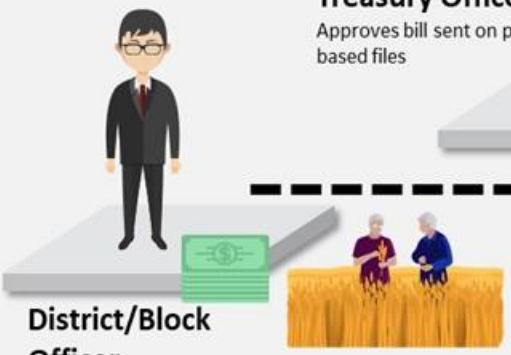
District/Block Officer
Officer accepts application through paper based forms filled by farmers



Department Officer
Reviews application and approves through paper based files

Treasury Officer
Approves bill sent on paper based files

District/Block Officer
Hands over cash to farmers



MeghEA Transformation

Future State User Experience

State Digital ID – Forms data pre-populated

SMS – Notification at every step

Farmers Apply
Farmers are aware and apply for services using contact center / mobile app or web

District/Block Officer
Gets alerts on application submission and approves from web/mobile

Direct Bank Transfer
Amount is transferred to farmers bank account

Real-time Reporting
Reporting of scheme details at real-time using business intelligence

Below are some of the schemes where the above transformation would be applicable:

- Financial Assistance for Establishment of Agriculture Infrastructure
- Providing Financial Assistance for purchase of Agricultural Machineries & Equipments
- Financial Assistance for Production Activities
- Financial Assistance for Establishment of Fisheries Infrastructure
- Assistance for Establishment of new garden for fruit, plantation crops etc under MIDH
- Providing infrastructure for seed production by farmers' producer groups
- Crop Insurance under PMFBY
- Assistance for Establishment of small nurseries for fruit plants under MIDH
- Income support to farmers through Pradhan Mantri Kisan Samman Nidhi
- Financial Assistance under National Bamboo Mission
- Assistance for purchase of Plant Protection equipment under Plant protection scheme
- Assistance for purchase of post-harvest management tools and implements under Agricultural Marketing Scheme
- Financial Assistance for Paddy cum fish Culture
- Financial Assistance for Renovation of Individual and Community Ponds
- Assistants for construction of mounting hall to Sericulture Farmers
- Financial Support for fencing of mulberry plantation to Sericulture Farmers
- Financial Assistant for construction of silkworm rearing houses

Food and Nutrition Services to Pregnant Women

Current State User Experience

Pregnant Women Apply
Women registers her name for services

ASHA Worker
Registers name and sends to health department

Institutional Treatment
Applies for institutional delivery by visiting hospital

Mother
Applies for services for new born and lactating mother

Health Dept. Officer
Reviews application and process

Health Officer
Approves and delivers Take home ration services to women

Take Home Ration
Mother receives food from far distant offices

MeghEA Transformation

Future State User Experience

State Digital ID – Forms data pre-populated

SMS – Notification at every step

Pregnant Women
Register name with ASHA worker

Data Flow to Department

Health Dept. Officer
Provides periodic awareness and facilitates delivery

Data Flow for Food Services

Health Dept. Officer
Approves Take Home Ration service

Data Flow To FPS

Mother
Food and Nutrition delivered through nearest FPS

Immunization
Immunization related alerts are sent to the mother

Data Flow To Immunization Program

New Business Setup in Meghalaya

Current State User Experience

New Investment
Investor apply for new Business Setup

Commerce & Industries
Reviews manual proposal and approves

Labour
Reviews manual proposal and approves

Pollution Control
Reviews manual proposal and approves

Electricity (Power)
Reviews manual proposal and approves

Tourism
Approves and delivers
Take home ration services to women

Approved for setting up new business
Certified approval

MeghEA Transformation

Future State User Experience

Commerce & Industries
Reviews digital application and approves

Labour
Reviews digital application and approves

Tourism
Reviews digital application and approves

Pollution Control
Reviews digital application and approves

Power
Reviews digital application and approves

Integrated EoDB System

Registrar of Companies
- Registration
- Data Sharing

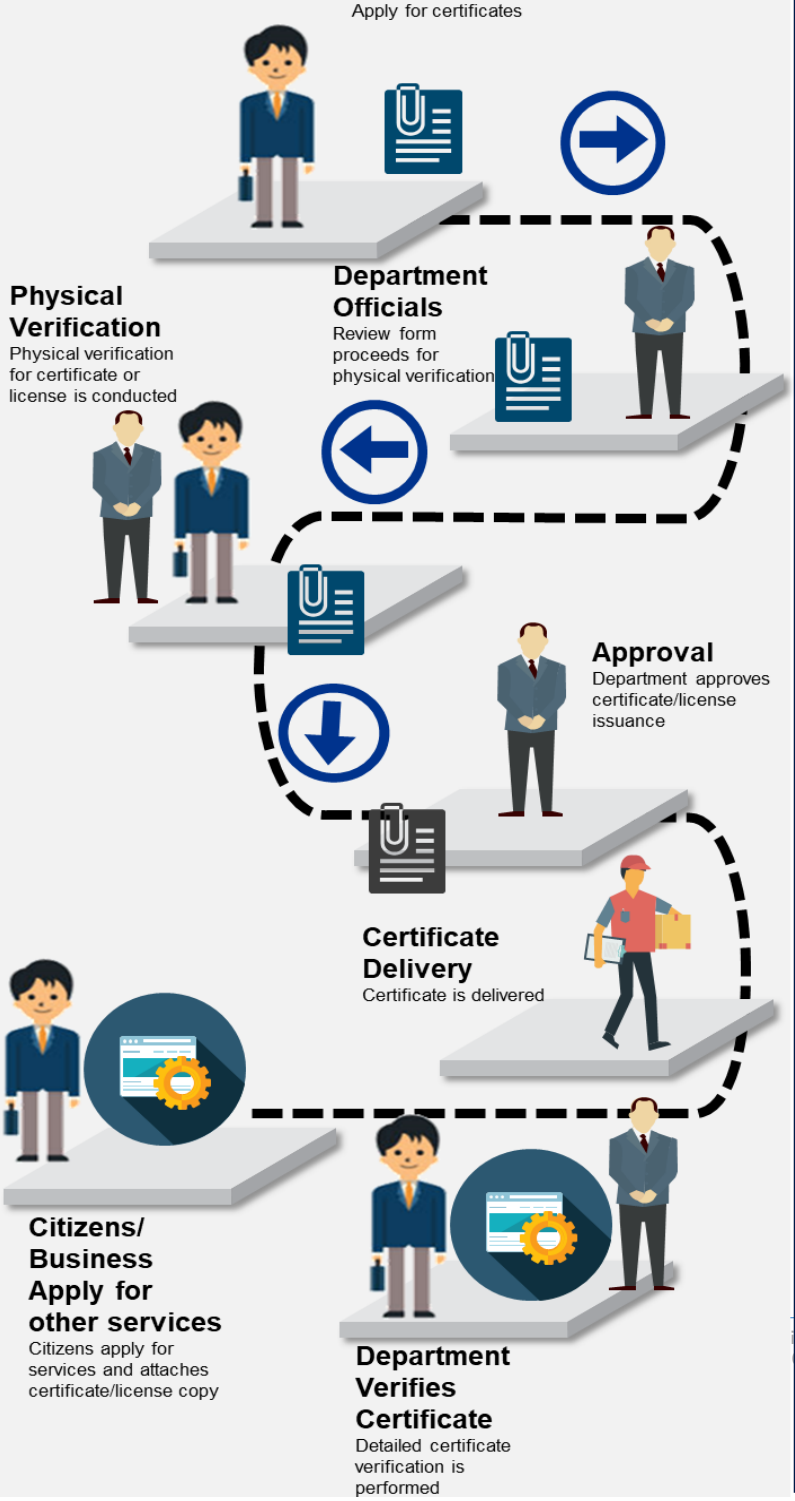
New Investment
Investor apply for new Business Setup

State Digital ID GSTN – Forms data pre-populated

SMS – Notification at every step

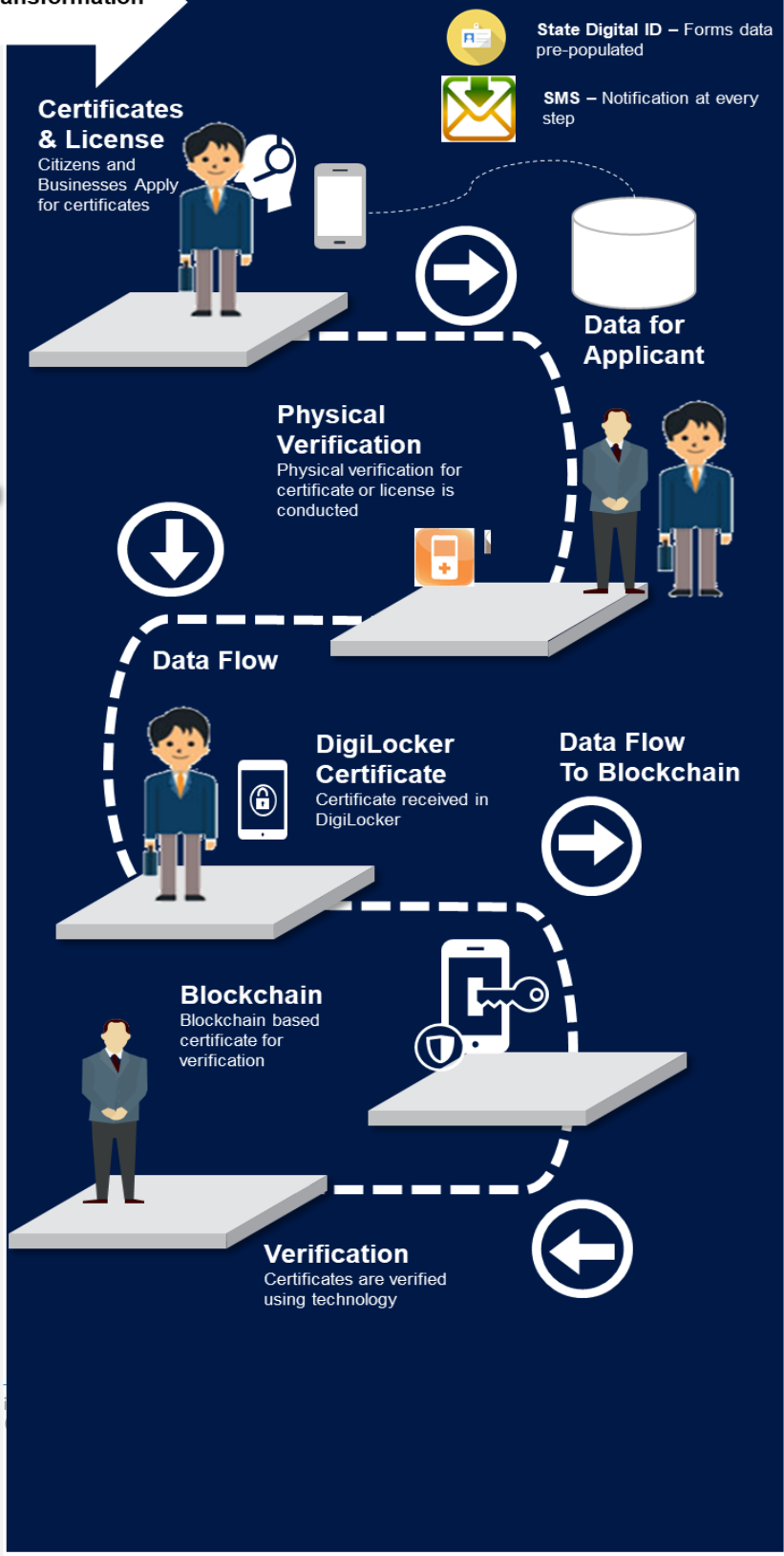
Trade Licenses, Permits and Certificates

Current State User Experience

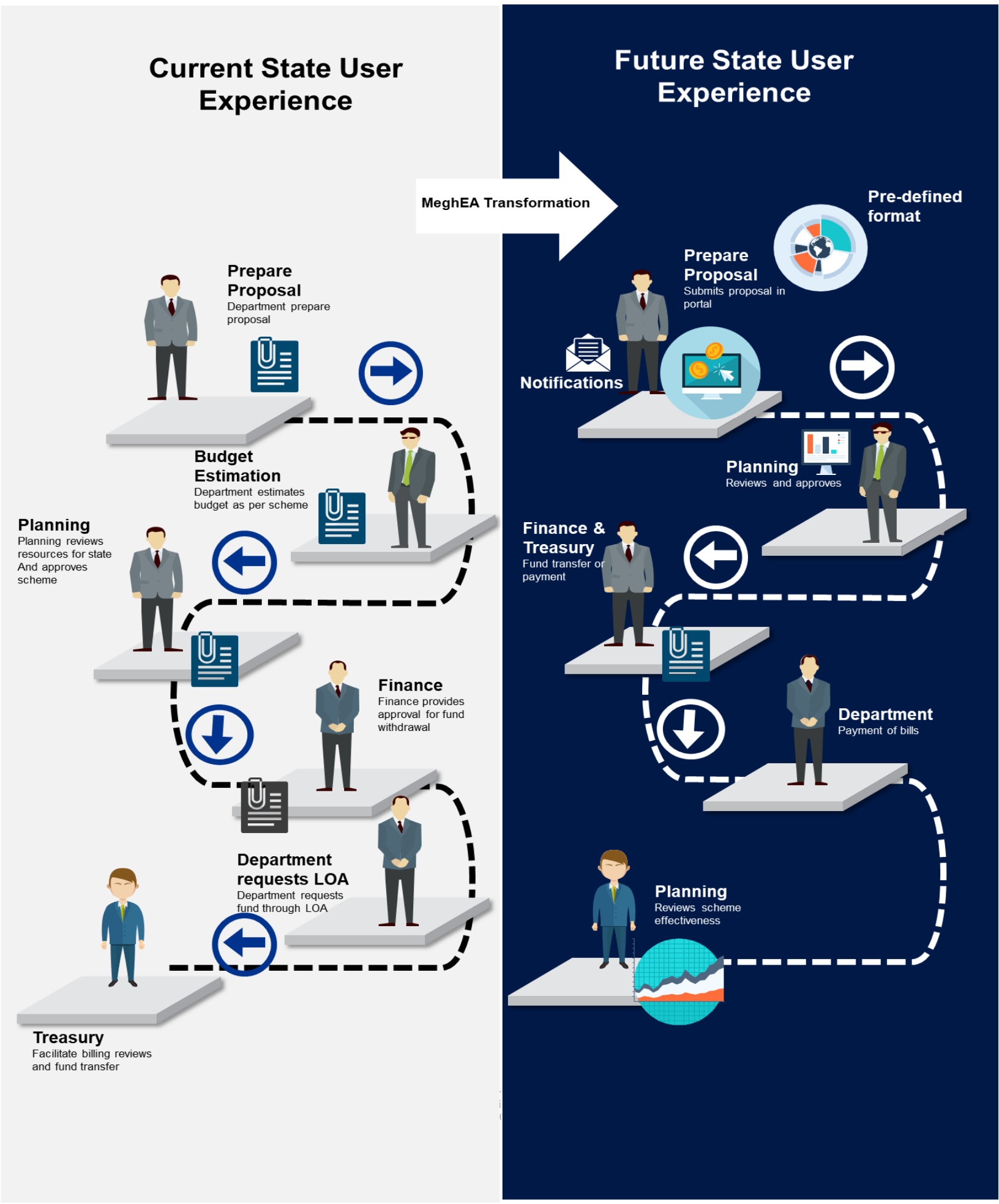


MeghEA Transformation

Future State User Experience



Scheme proposal, approval and reporting



Integrated Child Development Services

Current State User Experience

MeghEA Transformation

Future State User Experience

Manual identification of Pregnant Women

Asha Worker visits Pregnant Women for Maternal Care and Counselling

Care, Nutrition, Health and Hygiene Education

Manual Counselling by Health Workers

No predefined appointment / intimation

Health Check-up

Infant and Young Child Feeding (IYCF) Promotion and Counselling

No predefined appointment / intimation & no schedule

Supplementary Nutrition Immunization and Micronutrient supplementation

State Digital ID – Forms data pre-populated

SMS – Notification at every step

Helpline/ Mobile/ Asha Worker based online registration

Digital Care, Nutrition & Health Record

Pre Recorded Videos, Pre Schedule for Visits and online appointments

Pre-Scheduled Health Check-ups & App based tips

Pre-Recorded Videos / Online Counselling Scheduled Visits

Scheduled Pre-Scheduled Immunization based on data and Supply of Supplementary Nutrition

Unemployment Allowance for Person with Disabilities

Current State User Experience

MeghEA Transformation

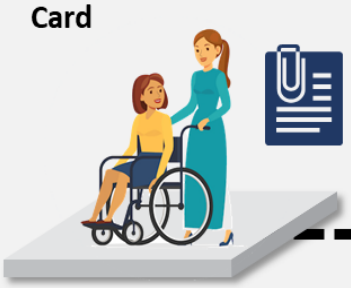
Future State User Experience

State Digital ID – Forms data pre-populated

SMS – Notification at every step

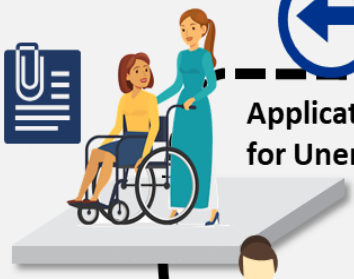
Current State

Application for Disability Card



Health Check-up & Verification by CMO office and Issuance of Disability Card

Application to Social Welfare for Unemployment Allowance



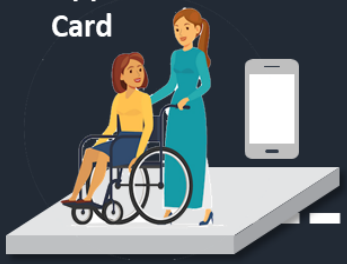
Verification by Health Department

Preparation of Proposal and approval of Scheme for providing Benefits

Cash provided to Beneficiary on receipt from Treasury based on Scheme Approval and Sanction

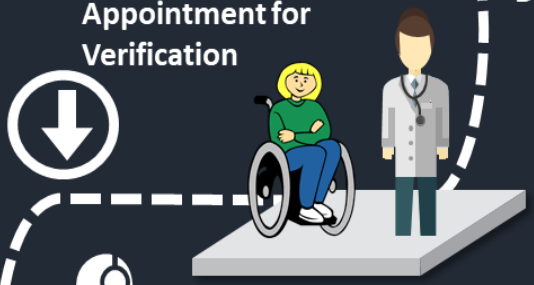
Future State

Application for Disability Card

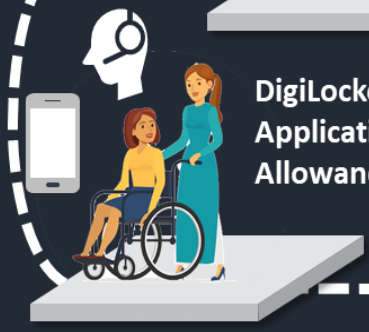


Issuance of Card in DigiLocker

Pre-Scheduled Appointment for Verification



DigiLocker Authenticated online Application for Unemployment Allowance



Online Proposal Sanction using Scheme Management System

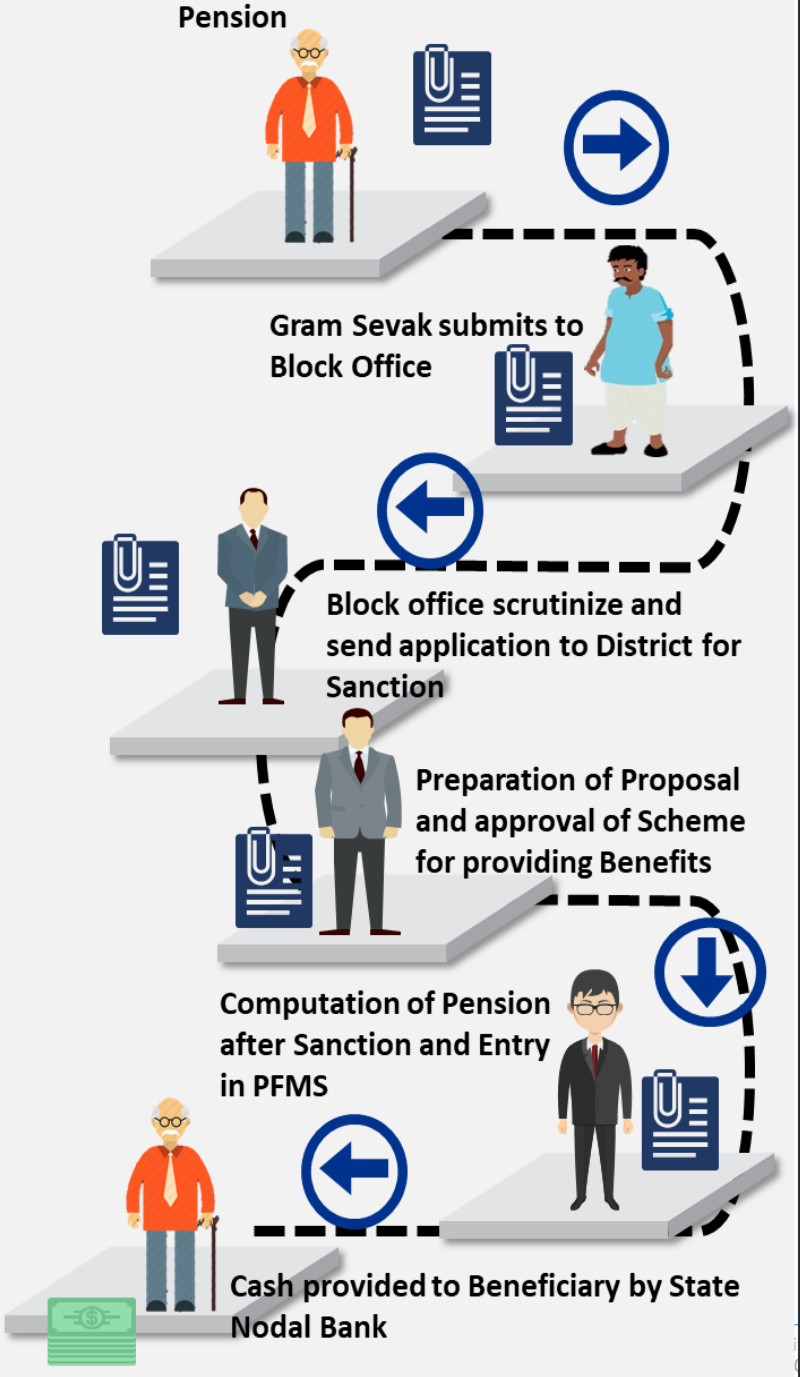
DBT in beneficiary account (Cashless Benefit Transfer)

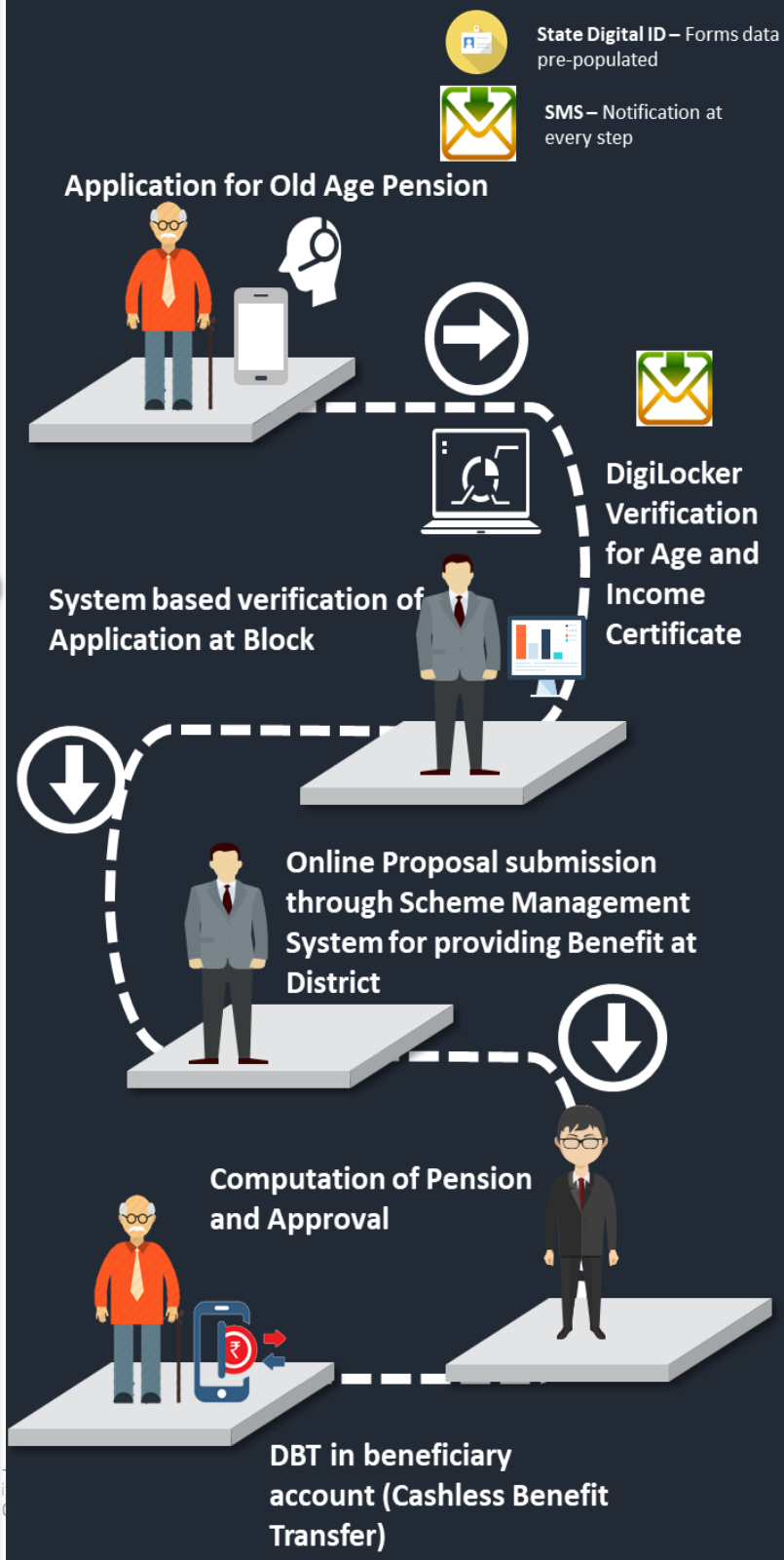
Old Age Persons Financial Assistance

Current State User Experience

MeghEA Transformation

Future State User Experience





7.8 Current State Digital Service Assessment Framework -

Assumptions and key considerations

1. This framework is for assessment of existing digital services; as per the framework any service that is currently being delivered through manual mode scores "0" and is considered to be low maturity
2. The assessment is comparative, that implies total score obtained is normalized to arrive at the low, medium or high maturity category. There is no specific cut-off for maturity category
3. The assessment does include review of design process of the services
4. All subjective assessment criteria mentioned in DSS has been purposefully excluded to avoid any biases
5. High maturity category does not mean that the service adheres to ALL DSS principles, rather it is a comparative assessment compared to other services in the pillar
6. The framework has been significantly modified for Finance department services, please refer the Finance Solution Architecture for details

Sr. No	Parameter	Rating (0 to 5)	Weightage	Score	Scoring Guide	Remarks for Exclusion
A	B	C	D	E (C X D)		
Assessing the DEFINE PHASE						
1	Are the objectives of DS defined?	2	**1**	2	Services mapped to department's goals & objectives - 2 marks Services mapped basis analysis of department's goals & objectives - 1 mark Not mapped to department's goals & objectives – 0	
2	Are the Objectives of DS SMART (Specific, Measurable, Achievable, Relevant, Time- specific)?	2	**1**	2	Service catalogue lists objectives in state portal - 2 marks For all other cases - 0 marks	
3	Do the Objectives derive from SDG's or the Priority Programs of the Government?	2	**2**	4	Service catalogue lists KPI - 2 Right to service act outlines service TAT - 2 Other cases - 0	
4	Are the user charges/ fees published/ Publicized?	3	**1**	3	Service fee listed in portal/citizen charter/other modes - 3 All other cases - 0	

Sr. No	Parameter	Rating (0 to 5)	Weightage	Score	Scoring Guide	Remarks for Exclusion
5	Has the DS been classified appropriately? And / Or Are the services organized along life-events?	2	**1**	2	Service organized as life events - 2 All other cases - 0	
6	Are the services organized along life-events?	0	**1**	0		Excluded as it repeated, follow Sr. No 5
7	Does the DS have personalization features?	1	**1**	1	Service availability in all digital channels - 1 Other cases - 0	
8	Has the DS been conceptualized and scoped consultatively?	0	**1**	0	Service development phase activity	Service design process not reviewed
9	Does the DS provide end-to-end functionality?	1	**2**	2	SSO - 1 marks Whole of Service - 1 marks All other cases - 0	
10	Is the DS integrated or linked to the related DS's?	0	**2**	0		Integration platform unavailable BPR for back-office processes - Not conducted
11	Have Service Levels been defined and publicized for DS?	0	**2**	0		Service TAT included in Sr. No 3, quality levels are subjective hence excluded
12	Has the QoS been defined for the DS?	0	**3**	0		QoS not defined for any service
13	In case of a Portal, does the directory of DS's follow a standard taxonomy?	1	**2**	2	Service Areas defined - 1 marks Service Metadata - 1 marks All other cases - 0	
14	Has the metadata of the DS been published?	0	**1**	0		None of the services follow DSS service metadata
15	How well is the DS visible?	1	**1**	1	Portal Search - 1 marks All other cases - 0	
SUB-TOTAL (DFINE PHASE)			**46%**	19		
Assessing the REALIZE Phase (DESIGN)						
1	Has User Needs Analysis been made?	0	**2**	0		Service design process not reviewed
2	Has BPR been undertaken?	1	**2**	2	Evidence of BPR - 1 marks All other cases - 0 marks	

Sr. No	Parameter	Rating (0 to 5)	Weightage	Score	Scoring Guide	Remarks for Exclusion
3	Is the DS Secure	0	**2**	0		ISO 27001 security assessment needs to covered in separate audit
4	Has survey of best practices been done?		**2**	0		Service design process not reviewed
5	Is the DS Cashless? Is e-Payment is integrated with the service? (net-banking, payment bank, debit/ credit card, APB)	1	**2**	2	Digital Payment mode >1 - 2 marks Digital Payment mode - 1 - 1 marks All other - 0 marks	
6	Is the DS Contactless?	1	**2**	2	Service application channel digital -2 marks All other - 0	
7	Is the DS Paperless?	0	**3**	0		All services requires paper documents in some stages or the other, hence, this is not considered
8	Is the DS being delivered is through multiple channels? (Web/Mobile/Kiosk etc.)	0	**1**	0		Repeated, follow Sr. No 7
9	Are the forms simple? (less than 2-page long)	1	**2**	2	Less than 2 page < 2 All other cases - 0	
10	Have the attachments been eliminated or reduced? (0 or 1 attachment)	1	**2**	2	Number of attachments required: for 1 attachment - 2 marks for more than 1 - 0 marks	
SUB-TOTAL (DESIGN)			**24%**	10		
Assessing the REALIZE Phase (UX and UI)						
1	Is the DS easily 'discoverable', through the use of simple keywords in a web search?	1	**2**	2	Discoverable in standard search engines - 2 marks All other cases - 0 marks	
2	Does the system notify the user the regarding the current status of the application/ request w.r.t. current internal process?	2	**1**	2	Notification & Status - 2 marks Only status - 1 marks All other - 0 marks	
3	Are the on-screen messages to the user in simple, natural language?	0	**1**	0		Subjective assessment, hence, excluded

Sr. No	Parameter	Rating (0 to 5)	Weightage	Score	Scoring Guide	Remarks for Exclusion
4	Does the DS provide 'undo', 'redo' buttons?	1	**1**	1	Clear button , Undo button - 1 marks All other - 0	
5	Does the DS provide online validation of the inputs provided by the user?	1	**2**	2	Server based validation - 2 marks Script validation - 1 marks All other - 0 marks	
6	Does the site have online help feature?	1	**2**	2	Online Help - 1 marks All other - 0 marks	
7	Has UNICODE been used for all labels, messages and form fields?	0	**1**	0		Not found in any service hence this is marked as not relevant
8	Does the DS meet the special accessibility requirements of the differently abled?	1	**2**	2	Aligned to GIGW standards - 2 marks All other - 0 marks	
9	Are the forms in the DS downloadable and in an open format and fillable offline?	1	**2**	2	Downloadable forms - 2 All other - 0	
10	Does the DS provide an acknowledgement to user on completion of the request?	0	**1**	0		Notification already covered
11	Does the site/portal provide SSO feature for accessing multiple services in the same session?	0	**1**	0		No SSO in state
12	Is the DS responsive?	0	**3**	0		Subjective assessment, hence, excluded
13	Does the DS ensure and assure the privacy of the personal information?	0	**2**	0		Architecture assessment detailed in pillar documents, hence, excluded
14	Are all the user interfaces clear to an average user?	0	**2**	0		Subjective assessment, hence, excluded
15	Are the screens and messages precise?	0	**2**	0		Subjective assessment, hence, excluded
SUB-TOTAL (UX and UI)			**30%**	13		
Assessing the REALIZE Phase (Architecture & Standards)						

Sr. No	Parameter	Rating (0 to 5)	Weightage	Score	Scoring Guide	Remarks for Exclusion
1	Has the Digital project adopted any Architecture framework or standard?	0	**5**	0		No architecture framework adopted in the state, hence, excluded
2	Are MDDS Standards of GoI followed?	0	**3**	0		MDDS standards compliance requires detailed DB level assessment, hence, excluded
3	Are the Regulations of UIDAI followed in the in the matters relating to security and privacy of Aadhaar data?	0	**3**	0		UIDAI audit report is not available
4	Is the ISO 27001 complied with by the DS Project?	0	**3**	0		ISO 27001 compliance check requires TPA report review. No TPA report available
5	Is an annual audit of the application/ DS Project conducted?	0	**2**	0		Annual audit not conducted at SDC level for all services
6	Has an open API-based architecture been adopted to create an eco-system?	0	**3**	0		Not adopted for any service
7	Is the use of local language in compliant with UNICODE?	0	**2**	0		Not adopted for any service
8	Have the relevant documentation standards been followed in the development?	0	**2**	0		No documents are available
10	Is there a version control system in place?	0	**2**	0		Not followed for any service
SUB-TOTAL (Architecture & Standards)			**0%**	0		
Assessing the REALIZE Phase (Delivery)						
1	Does the DS provide for the inclusion requirements of disadvantaged groups?	0	**2**	0		GIGW standards cover this aspect, hence, excluded
2	Is the feedback and grievance redressal mechanism for the DS functional?	0	**2**	0		Grievance system covers any and all service grievances, hence, excluded
3	Does the organization have a Unified Contact Centre?	0	**2**	0		No UCC, hence, excluded
4	Is the DS delivered also in an assisted mode?	0	**1**	0		No such systems, hence, excluded
5	Has the organization adopted appropriate capacity building exercises for operationalization of DS?	0	**1**	0		Planning and design not reviewed
SUB-TOTAL (Delivery)			**0%**	0		
GRAND TOTAL			**100%**	42		

Table 46: DSS Assessment Framework