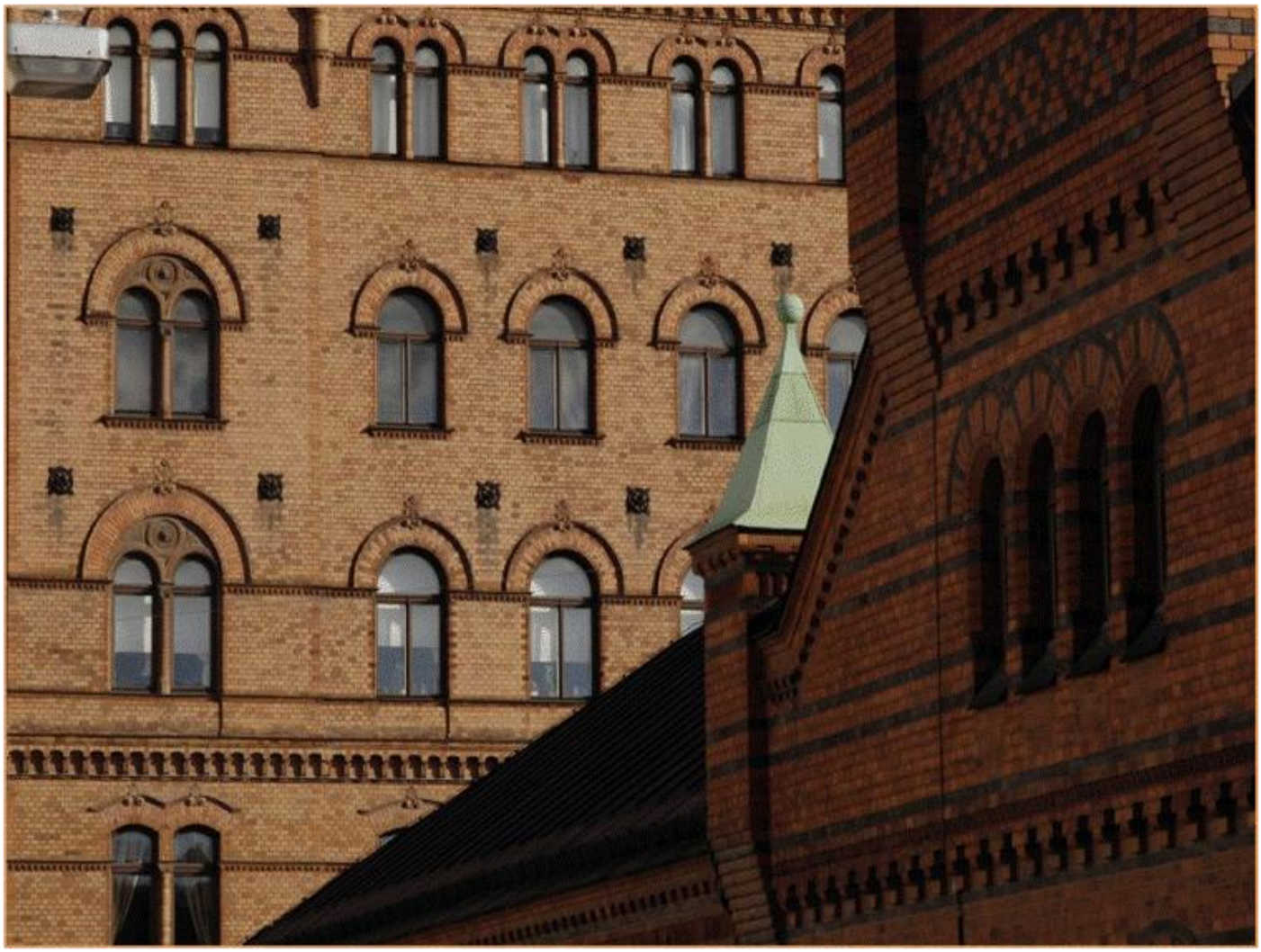
Nepal Government Enterprise Architecture - Main Report



GEA will provide the foundation to enable the Government of Nepal to effectively deliver services across all service delivery channels to citizens, business and other government units

pwc

Jan 2011

Document History

Date	Version	Author	Description
November , 2010	Draft	PwC India	Nepal Government Enterprise Architecture – Main Report – Draft version
January , 2011	Final	PwC India	Nepal Government Enterprise Architecture – Main Report – Final version

Distribution

Title	No. of Copies
HLCIT: **Primary**: Mr. Juddha B. Gurung **Secondary**: HLCIT to decide	1

Table of Contents

1. Executive Summary

1. Executive Summary

1.1 E-Government Vision & Mission

With the rapid development and expansion of ICT, and in particular, with the fast penetration of the Internet, government administrative services is also transforming from its traditional, manual, passive services to active, enhanced, consolidated and automated services. In line with such trend in ICT, globally governments are aiming to establish the e-government which can improve productivity in administrative services, realize a networked government, satisfy its people's demand in administrative services, and enhance the national competitiveness through proactive services.

To achieve good governance and social and economic development by establishing effective, systematic, and productive e-Government, the Government of Nepal have established the e-Government Master Plan (eGMP) with the objective of leveraging the full potential of Information and Communication Technology (ICT) to improve the efficiency and capability of government processes and services.

To realize the e-Government in prompt, effective & efficient manner, the e-Government vision and mission and the strategies to achieve such vision and mission was established for the Govt. of Nepal.

The Nepal e-Government Vision is the "The Value Networking Nepal" through –

- Citizen-centered service
- Transparent service
- Networked government
- Knowledge based society

The Nepal e-Government **Mission** statement is to –

*Improve the quality of people's life without any discrimination, transcending regional and racial differences, and realize **socio-economic development** by building a **transparent government** and providing value added quality **services through ICT***

1.2 Project Background

To realize Nepal's e-Government vision and mission of providing a "**Value Networking Nepal**" by building efficient, transparent and citizen centric government services, termed as "**e-Services**" through ICT, defining the "**Government Enterprise Architecture**" for Nepal has been one of the key priority projects identified.

The Government Enterprise Architecture (GEA) project has been envisioned to deliver a common integrated interoperability platform or service delivery gateway for information exchange and host the national portal of Nepal that will act as the single window (one-stop-shop) for all government e-Services and electronic information of Nepal to be delivered to citizens (G2C), business (G2B) and government employees (G2E). Delivery of **e-Services** will enable increased citizen participation and attempt to create an open, transparent environment through integration of different government information systems and services.

In this context, PwC has been engaged to assist the Government of Nepal in design and commissioning of the GEA based on SOA principles which encompasses -

- Review of business strategy & drivers, identification of critical services across the various departments of Govt of Nepal, current state assessment of the short-listed services, business process re-engineering with recommendation of re-engineered process design principles,
- Defining the GEA principles, standards, polices, specifications, guidelines across various architectural segments i.e. business, data, application, technology, security & integration based on SOA
- Defining the Nepal e-Government interoperability framework
- Conceptualize and implement the national portal of Nepal

1.3 Purpose

The purpose of this document is to outline the recommended Government Enterprise Architecture under Government of Nepal's GEA programme. It aims to provide a linkage between the Government of Nepal's eGovernance vision and its realization through the conceptualization of the Nepal GEA and national portal which will serve as the service delivery architecture for the government G2C, G2B, G2E & G2G services.

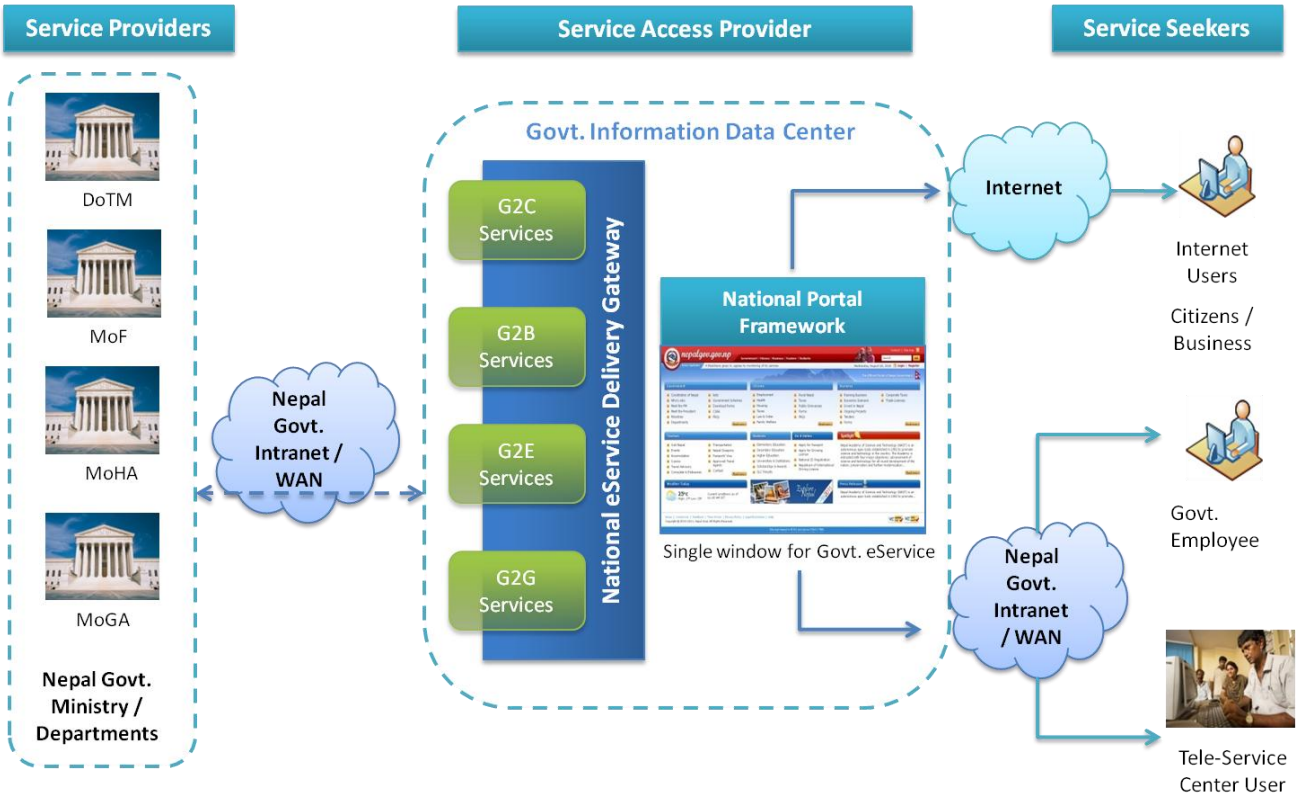
The report captures the recommended enterprise architecture and outlines the proposed high level conceptual architecture proposed for each architectural segments i.e. business, data, application, technology, security and integration.

Along with the enterprise architecture, the guideline also briefly outlines the proposed Nepal eGovernment Interoperability framework (NeGIF). **NeGIF** provides a framework to share, collaborate and integrate information and organisation processes by defining the minimum set of collection of ICT standards and technical specifications governing the communication of systems, flow of information, as well as the exchange of data and business processes that relates to Government Ministries, agencies and departments.

It is advisable for all upcoming Govt. of Nepal ICT projects to adhere and comply with the recommended Nepal GEA & eGIF guidelines, standards, principles & specification.

1.4 Nepal GEA Service Delivery Landscape

The overall landscape for the subsequent delivery of eServices has been depicted below –



As one of the major components of NGEA initiative of Nepal, it is envisioned that practically all the eServices and electronic information in Nepal will be delivered via a comprehensive integration service delivery platform "**National eService Delivery Gateway**" which services as the gateway for electronic information exchange and interactions in Nepal. Government **eService Provider** typically back-end ministry / departments / government agencies will put up its service be it G2C, G2B, G2E or G2G for electronic delivery through the National eService Delivery Gateway. All the government and public e-Services (electronic Services) will be compliant with the GEA specifications.

The National eService Delivery Gateway & National Portal of Nepal will serve as the **Service Access Provider** that will provides the infrastructure to facilitate government service access by the Service Seekers. Linked to the Service Access Providers will be the delivery channels, which would be the access mechanism for the citizens and businesses to avail the e-governance services.

The Nepal **National Portal** will act as the single window one-stop store for the delivery of Govt. G2C, G2B & G2E eServices. **eService Seekers** typically citizens, business, government employee & tele-center users can avail these service by logging into the national portal and filling & submitting the service request forms online.

1.5 Nepal Govt. Enterprise Architecture Framework

Government Enterprise Architecture is a guided by the architectural framework which provides guidelines, architecture principles, architecture development methodology, content metamodel and the reference model from business and technology services perspective defining the principles of interoperability between departments for better and efficient service delivery to the citizens and businesses in a country.

PwC had followed the industry standard TOGAF for developing the government enterprise architecture for Govt. of Nepal.

Using TOGAF as the architecture framework will allow architectures to be developed that are consistent, reflect the needs of stakeholders, employ best practice, and give due consideration both to current requirements and to the likely future needs of the government. TOGAF provides a platform for adding value, and enables users to build genuinely open systems-based solutions to address their business issues and needs. Besides it underpins a practical standardized methodology of implementing successful EA to organizations and is widely accepted and the most adopted architectural framework.

The Open Group Architecture Framework (TOGAF 9.0) was adopted for the development of the Nepal GEA framework. TOGAF was tailored as appropriate to meet the needs of the Govt. of Nepal's EA requirements.

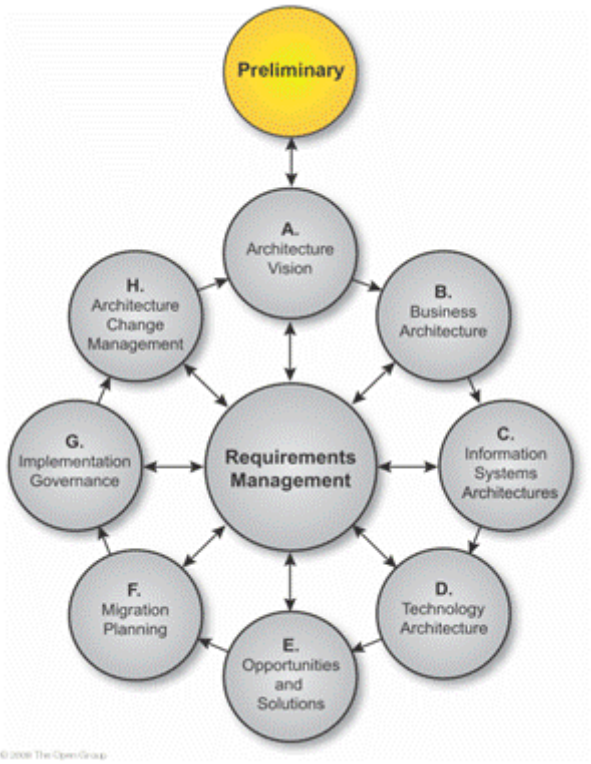
1.6 Definition, acronym and abbreviation

Abbreviation	Expansion
ACMM	Architecture capability maturity model
ADM	Architecture Development Method
BPM	Business Process Management
BPR	Business Process Reengineering
CBA	Component-based Architecture
CDMA	Code Division Multiple Access
CIO	Chief Information Officer
COBIT	Control Objectives for Information Technology
COSO	Committee of Sponsoring Organizations
COTS	Commercial Off-The-Shelf
DoLRM	Department of Land Reforms Management
DoR	Department of Roads
DRM	Data Reference Model
EA	Enterprise Architecture
eGMP	e-Government Master Plan
ESB	Enterprise Service Bus
FCGO	Financial Comptroller General Office
G2B	Government to Business Services
G2C	Government to Citizen Services
G2E	Government to Employee Services
G2G	Government to Government Services
GEA	Government Enterprise Architecture
GUI	Graphical User Interface

Abbreviation	Expansion
ICT	Information and Communication Technology
III-RM	Integrated Information Infrastructure - Reference model
ISO	International Standards Organization
IT	Information Technology
ITIL	The Information Technology Infrastructure Library
KMC	Kathmandu Metropolitan City
KPI	Key Performance Indicator
LAN	Local Area Network
MCU	Master Control Units
MoGA	Ministry of General Administration
MVC	Model View Controller
NeGIF	Nepal e-Government Interoperability Framework
NGSDG	Nepal GEA Service Delivery Gateway
NTA	Nepal Telecom Authority
OASIS	Organization for the Advancement of Structured Information Standards
PCI DSS	Payment Card Industry Data Security Standard
PMBOK	Project Management Body of Knowledge
PRINCE2	Projects in Controlled Environments version 2
RAS	Remote Access Server
RBAC	Role-Based Access Control
SC	Supreme Court
SDG	Service Delivery Gateway
SIB	Standard Information base
SOA	Service-Oriented Architecture
SSL	Secure Sockets Layer
TCO	Total Cost of Ownership
TOGAF	The Open Group Architecture Framework
TRM	Technical Reference Model
TSL	Transport Layer Security
URL	Uniform Resource Locator
VC	Video Conferencing
WAN	Wide Area Network
XML	Extensible Markup Language

2. TOGAF ADM Preliminary Phase

2. Preliminary Phase



Phase Overview

The objectives of the Preliminary phase is to –

Review the organizational context for conducting enterprise architecture, identify the sponsor stakeholder(s) and other major stakeholders impacted by the business directive to create enterprise architecture and determine their requirements

To identify and scope the key drivers and elements of the enterprise organizations affected by the business directive and define the constraints and assumptions

To define the "architecture footprint" for the organization - the people responsible for performing architecture work, where they are located, and their responsibilities

To define the enterprise architecture framework and detailed methodologies that are to be used to develop enterprise architectures in the organization concerned (typically, an adaptation of the generic ADM)

2.1 Scope of the enterprise organizations impacted

The Government Enterprise Architecture would be architected keeping in mind all the ministries and it's departments that would need to adhere to the standards, policies and architectural principles as proposed by the GEA. However, since the Government of Nepal has 8 constitutional bodies 22 ministries with its departments and 10 Banking and Financial institutions with varying level of maturity in eGovernance & digitization, GEA PwC team in partnership with HLCIT in the requirement phase has identified the following set of ministries and departments that will be considered in the scope of GEA.

Govt. Organization Type	Shortlisted Govt. Organization / Unit / Department / Agencies in Scope of GEA
Constitutional Bodies	1. Supreme Court 2. Election Commission 3. Public Service Commission

Govt. Organization Type	Shortlisted Govt. Organization / Unit / Department / Agencies in Scope of GEA
Government Ministries & Departments	1. Prime Minister & Cabinet Office 2. Ministry of Environment, Science And Technology 3. Ministry of Finance • Inland Revenue Department (IRD) • Financial Comptroller General Office (FCGO) 4. Ministry of Foreign Affairs 5. Ministry of General Administration • Department of Civil Personnel Records 6. Ministry of Home Affairs • Nepal Police • National ID Management Committee (NIDMC) 7. Ministry of Information And Communication • Nepal Telecom Authority (NTA) • Department of Postal Services – Tele-Centre Network 8. Ministry of Labour And Transportation • Department of Transport Management (DoTM) 9. Ministry of Land Reform And Management • Department of Land Reform & Management (DoLRM) 10. Ministry of Local Development • Municipalities (KMC) 11. Ministry of Physical Planning & Works (MoPPW) • Department of Roads (DoR)
Banking institutions	1. Nepal Rastra Bank (NRB)

Services were short-listed from these Ministries / Departments / Agencies thereafter fully assessed in their "As-Is" State utilizing a combination of Personal Meetings (with various Officers and Technology Partners in concerned Departments), Questionnaires (that captured the details pertaining to a particular Government Service along with the Ministry / Department / Agency delivering the same) and Secondary Research (from the Official Websites, Rule Books, Manuals, Documentation of Applications currently being used, etc.). It was further ensured that PwC's previous experiences from across the world are referred to during Current State Assessment and Learning's from such assignments are also factored in while understanding the core Governance Principles on which the short-listed services are based upon.

Following are the parameters utilized to prioritize the scope of Government services for assessment

Parameter	Weightage allocated
Would have high-visibility when implemented	10%
All Stakeholders would be ready to accept the changed Service	5%
Would have suitable IT Systems to support reengineered flows	15%
Owner Department would be ready to adopt and adapt to the changed processes	10%
BPR would reduce overall cost and time for Owner Depts. to deliver the Service	10%

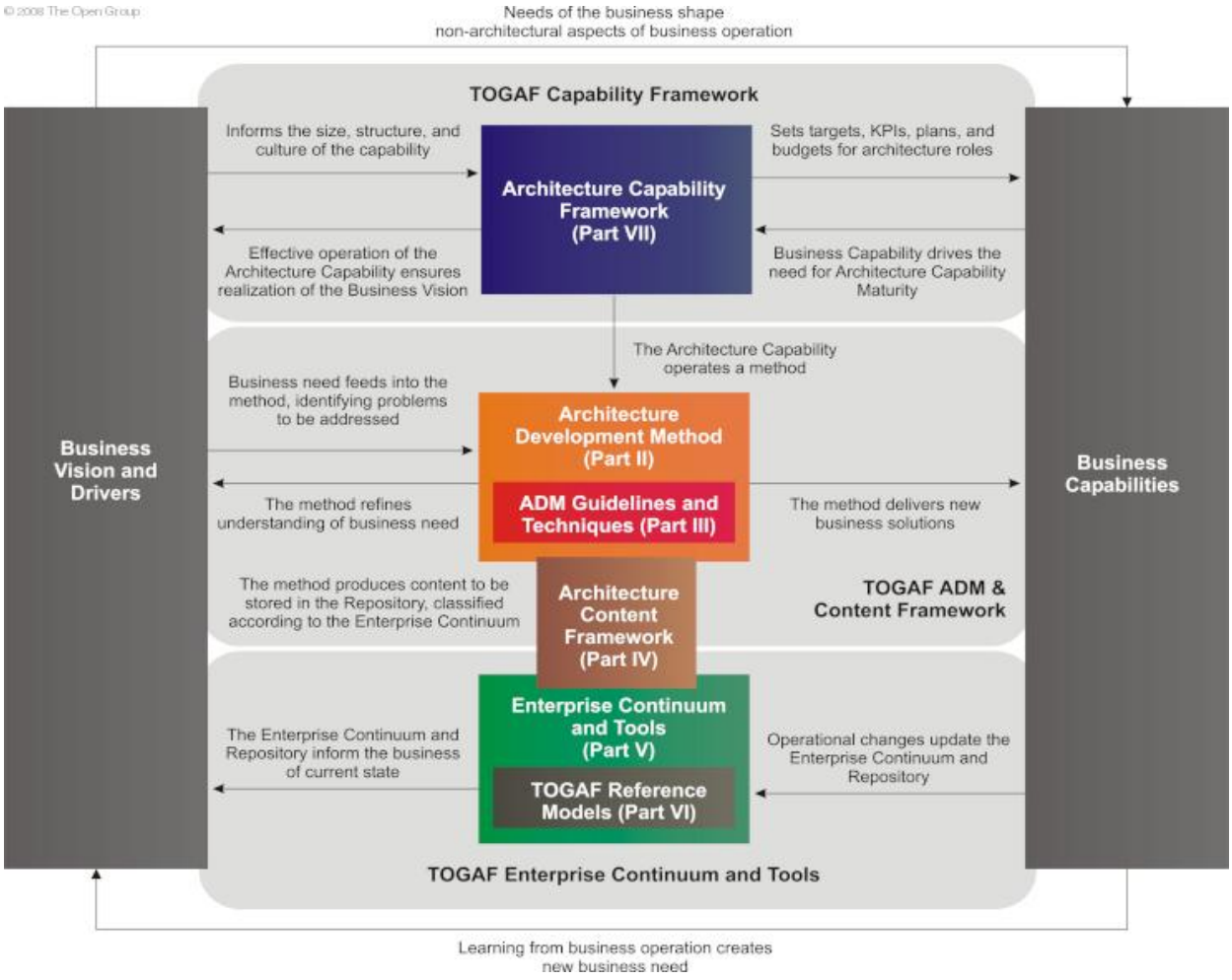
Parameter	Weightage allocated
Would enhance the efficiency (by providing more Lead-time, by easing the flows, etc.) of Process Participants	5%
Would reduce Overall Cost for recipients to avail the service	10%
Impacts a large number of stakeholders	15%
Would be a Long-term solution and can be persisted with for a feasible period of time	10%
Would give rise to suitable Web Service(s)	10%

The short listed business services in scope of the GEA are listed below -

Ministry / Departments	Shortlisted Business Service
IRD / MoF	• Issue of PAN to a person • Issue of PAN to an Entity • Facilitating the filing of Income Tax by a Taxpayer • Registration for VAT and facilitation for filing VAT Returns • Facilitating the filing of returns by a TDS Withholder
DoTM	• Registration of new vehicles • Change of ownership of a vehicle • Renewal of a Vehicle's Registration • Issue of Route Permits to Commercial Vehicles • Issue of a new Driving License • Addition of a new Category to an existing License • Renewal of an existing License • Conversion (Nepalikaran) of a Foreign Driving License • Duplication of an Driving License
Supreme Court	• Creation and communication of the Cause List
Municipality (KMC)	• Birth Registration
MoHA	• Issue of Character Certificate to a Citizen • Issue of Citizenship Certificate
FCGO / MoF	• Control & Management of Public Finances
DoR	• Tender Management
MoFA	• Issue of an ordinary Passport
EC	• Registration of Voters

Ministry / Departments	Shortlisted Business Service
MoGA	• Creation and management of Employee Records • Employee Performance Management • Employee Grievance Redressal • Pension Management of Retired Govt. Employees • Management Audit for Govt. Depts. / Agencies • O&M Surveys for Govt. Depts. / Agencies
DoLRM	• New Land Registration & Issue of Land Certificate • Land Mutation (Change of Ownership) • Management of Land Disputes
NTA	• License Award Process • Type Approval Process • Consumer Grievance Redressal / Complaints Management
PSC	• Collecting Manpower Requirements from different ministries • Submission of Application Form by Applicants • Publishing Results of Examination
Department of Postal Services	• Tele-center Network
Nepal Rastra Bank	• Submission of Periodic Data from Banks & Financial Institutions

2.2 Approach: TOGAF Capability Framework

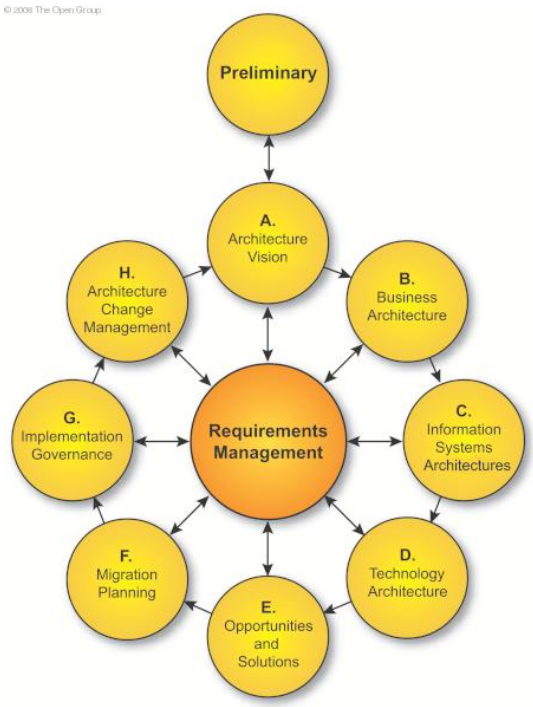


2.2.1 *Part II: Architecture Development Method*

This is the core of TOGAF. It provides a step-by-step approach to develop and use enterprise architecture

The ADM comprises a series of linked phases which enable

- the full life-cycle management of an Enterprise Architecture
- from planning to operational deployment and change



Preliminary Phase

Objective: Prepare the enterprise for successful Preliminary Enterprise Architecture

- Establish organizational context
- Identify sponsor (and other) stakeholders
- Gain commitment to the approach
- Define enterprise scope
- Define "architecture footprint"
- Define framework and detailed methods
- Confirm governance framework
- Select supporting tools and infrastructure
- Define architecture principles

Phase A: Architecture Vision

Objective: Initiate a cycle of the ADM

- Ensure this evolution has recognition and support
- Define and organize an architecture development cycle
- Validate business principles, goals, drivers
- Establish Enterprise Architecture KPIs
- Define scope and components
- Define relevant stakeholders, their concerns and objectives
- Define key business requirements to be addressed
- Articulate an Architecture Vision
- Create a comprehensive plan
- Secure formal approval to proceed
- Understand the impact on and of other parallel architecture development cycles

Phase B: Business Architecture

Objectives:

- Describe the Baseline Business Architecture
- Develop a Target Business Architecture
- Product/service strategy
- Organizational, functional, process, information, geographic aspects
- Analyze the gaps
- Select and develop relevant Architecture Viewpoints
- Select relevant tools and techniques to be used

Phase C: Information Systems Architectures

Objectives:

- Develop Target Architectures covering either or both (depending on project scope) of the data and application systems domains
- Focuses on identifying and defining the applications and data considerations that support an enterprise's Business Architecture

Data Architecture:

- Define the major types and sources of data
- Understandable by stakeholders
- Complete and consistent
- Stable

Application Architecture:

- Define the major kinds of application system necessary
- To process the data
- To support the business

Phase D: Technology Architecture

Objectives:

- Map application components into a set of technology components
- Software
- Hardware
- Defines the physical realization of an architectural solution.

Phase E: Opportunities and Solutions

Objectives:

- Review target business objectives and capabilities
- Consolidate gaps from Phases B to D
- Organize groups of building blocks to address these capabilities
- Review and confirm the enterprise's current parameters for, and ability to, absorb change
- Derive a series of Transition Architectures that deliver continuous business value

- Generate and gain consensus on an outline Implementation and Migration Strategy

Phase F: Migration Planning

Objectives:

- Co-ordinate the Implementation and Migration Plan with management frameworks
- Prioritize all work packages, projects, and building blocks
- Assign business value
- Conduct cost/business analysis
- Finalize the Architecture Vision and Architecture Definition Documents, in line with the agreed implementation approach
- Confirm the Transition Architectures with stakeholders
- Create, evolve, and monitor the detailed Implementation and Migration

Phase G: Implementation Governance

Objectives:

- Formulate recommendations for each implementation project
- Govern and manage an Architecture Contract covering the overall implementation and deployment process
- Perform appropriate governance functions while the solution is being implemented and deployed
- Ensure conformance with the defined architecture
- Ensure that the program of solutions is deployed successfully, as a planned program of work
- Ensure conformance of the deployed solution with the Target Architecture
- Mobilize supporting operations that will underpin the future working lifetime of the deployed solution

Phase H: Architecture Change Management

Objectives:

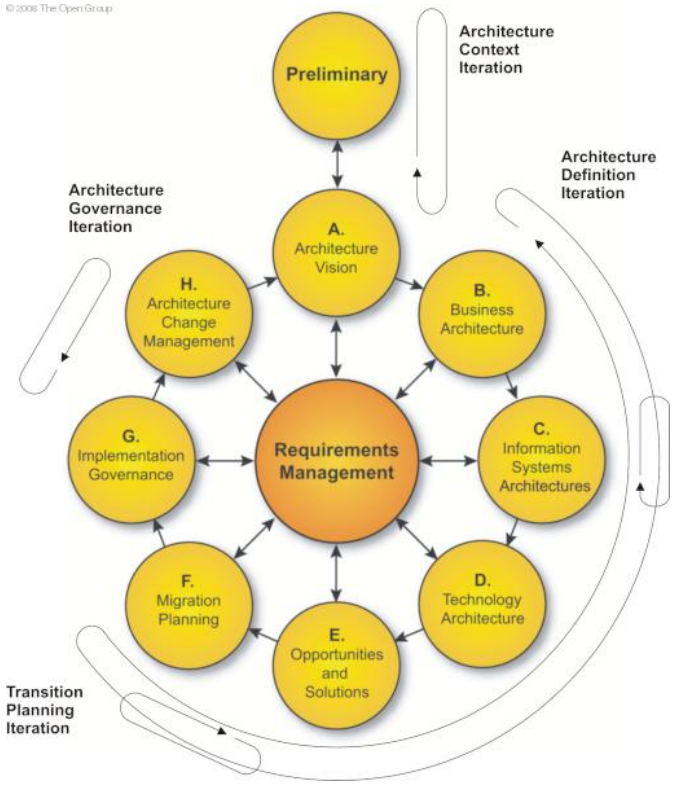
- Ensure that baseline architectures continue to be fit-for-purpose
- Assess the performance of the architecture and make recommendations for change
- Assess changes to the framework and principles set up in previous phases
- Establish an architecture change management process for the new enterprise architecture baseline that is achieved with completion of Phase G
- Maximize the business value from the architecture and ongoing operations
- Operate the Governance Framework

Requirements Management

Objectives:

- Define a process to manage requirements
- Identify
- Store
- Feed into and out of relevant ADM phases

During each phase, work is validated against the current business requirements that motivate the development



2.2.2 *Part III: ADM Guidelines and Techniques*

Following are the ADM guidelines that would be of interest to GEA Nepal

- Interoperability and the ADM - Refer to next section 2.1.2.1
- Government Transformation Readiness & Capability Based Planning
- Risk Management

2.2.2.1 Interoperability and the ADM

Interoperability is defined as the -

- The ability to share information and services.
- The ability of two or more systems or components to exchange and use information.
- The ability of systems to provide and receive services from other systems and to use the services so interchanged to enable them to operate effectively together.
- The ability for two or more things to work with each other. When things can interact with each other without encountering Errors
- More than an information or technology problem

There are many ways to define interoperability and the aim is to define one that is consistently applied within the enterprise and extended enterprise. Broadly interoperability could be categorized as follows -

- Business Interoperability
- Information Interoperability
- Technical Interoperability

Following table represents how interoperability is defined and implemented across the ADM lifecycle of EA.

ADM Phase	Interoperability activity
Preliminary Phase	Defining interoperability in a clear unambiguous manner is a key objective of Enterprise Architecture
Phase A Architecture Vision	The nature and security Preliminary considerations of the information and service exchanges are first revealed within the business scenarios
Phase B Business Architecture	Business Interoperability is defined by the set of services offered by each government departments and the format information exchange that happens between the departments in a structured format.
Phase C Information System Architectures	The Information system architecture defines the data formats that are exchanged between different department aligned with G2C, G2B and G2G services. The data formats that are interoperable are also defined in the phase.
Phase D Technology Architecture	The Technology architecture phase defines the technology stack around integrations, security and infrastructure in the form of Nepal Government Interoperability framework (NeGIF) document that would provide the standards and guidelines to provide an environment to support interoperability.
Phase E Opportunities & Solutions	The actual solutions (e.g., Commercial Off-The-Shelf, COTS, packages)
Phase F Migration Planning	The interoperability is logically are selected implemented

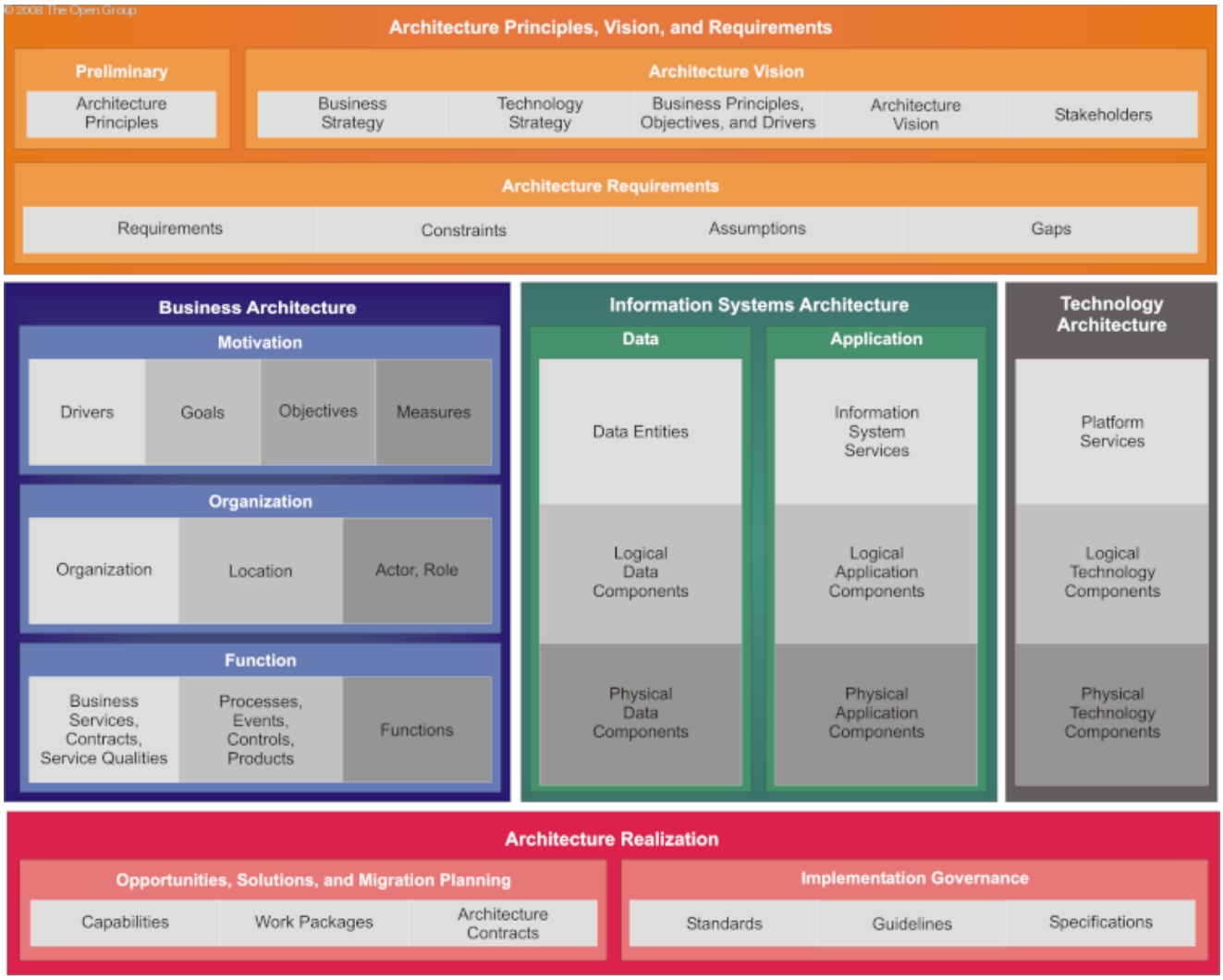
2.2.3 Part IV: Architecture Content Framework

The content framework is intended to

- Provide a detailed model of architectural work products
- Drive greater consistency in the outputs that are created when following ADM
- Provide a comprehensive completeness, and traceability checklist of architecture outputs that could be created
- Reduce the risk of gaps within the final architecture deliverable set
- Help an enterprise mandate standard architectural concepts, terms, and deliverables

The content metamodel allows architectural concepts to be

- Captured,
- Stored,
- Filtered,
- Queried, and
- Represented
- In a way that supports consistency, completeness, and traceability



2.2.4 Part V: Enterprise Continuum and Tools

Please refer to the section 3.7 for GEA Enterprise Continuum & section 3.8 for the GEA Architecture repository.

2.2.5 Part VI: TOGAF Reference Models

Please refer to section 3.7 for the Foundation Architecture (Enterprise reference models).

2.2.6 Part VII: Architecture Capability Framework

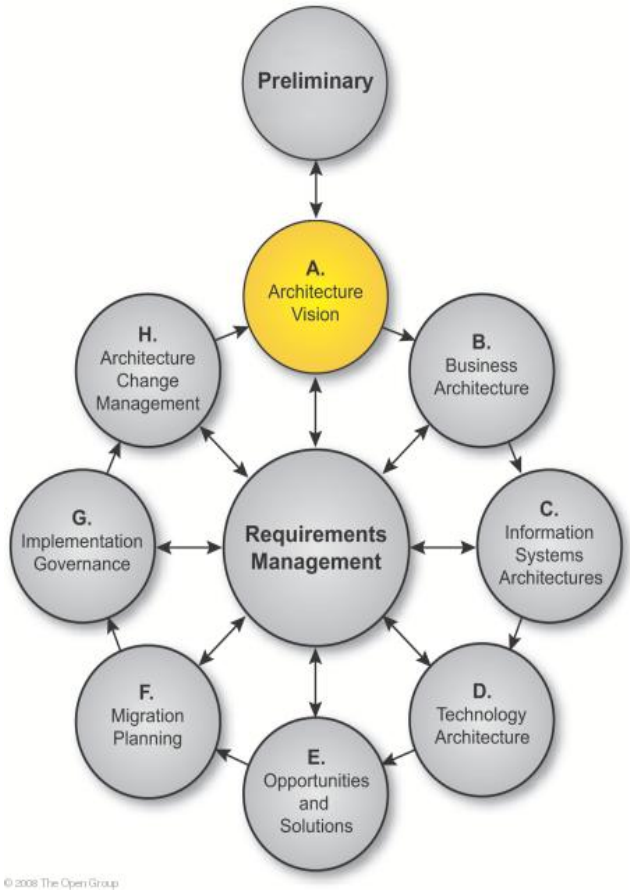
Please refer to the TOGAF 9 documentation for further details at http://www.opengroup.org

2.3 Tailored Architecture Framework

- Terminology Tailoring: TOGAF terms would be used in GEA Nepal project.
- Process Tailoring: The TOGAF ADM provides a generic process for carrying out architecture. Process tailoring provides the opportunity to remove tasks that are already carried out elsewhere in the organization, add organization-specific tasks (such as specific checkpoints) and to align the ADM processes to external process frameworks and touch-points. Key touch-points that need to be addressed include:
    - Portfolio management processes (project and service)
    - Project lifecycle
    - Operations handover processes
    - Operational management processes (including configuration management, change management, and service management)
    - Procurement processes
- Content Tailoring: Using the TOGAF Architecture Content Framework and Enterprise Continuum as a basis, tailoring of content structure and classification approach allows adoption of third-party content frameworks and also allows for customization of the framework to support organization-specific requirements. – Refer to section 3.7 for the GEA Architecture Continuum.

3. TOGAF ADM Phase A - Architecture Vision

3. Phase A: Architecture Vision



Phase Overview

The objectives of this phase are:

To define and organize an architecture development cycle within the overall context of the architecture framework, as established in the Preliminary phase

To define and validate the enterprise architecture principles including the business principles, business goals, and strategic business drivers of the organization and the enterprise architecture Key Performance Indicators (KPIs)

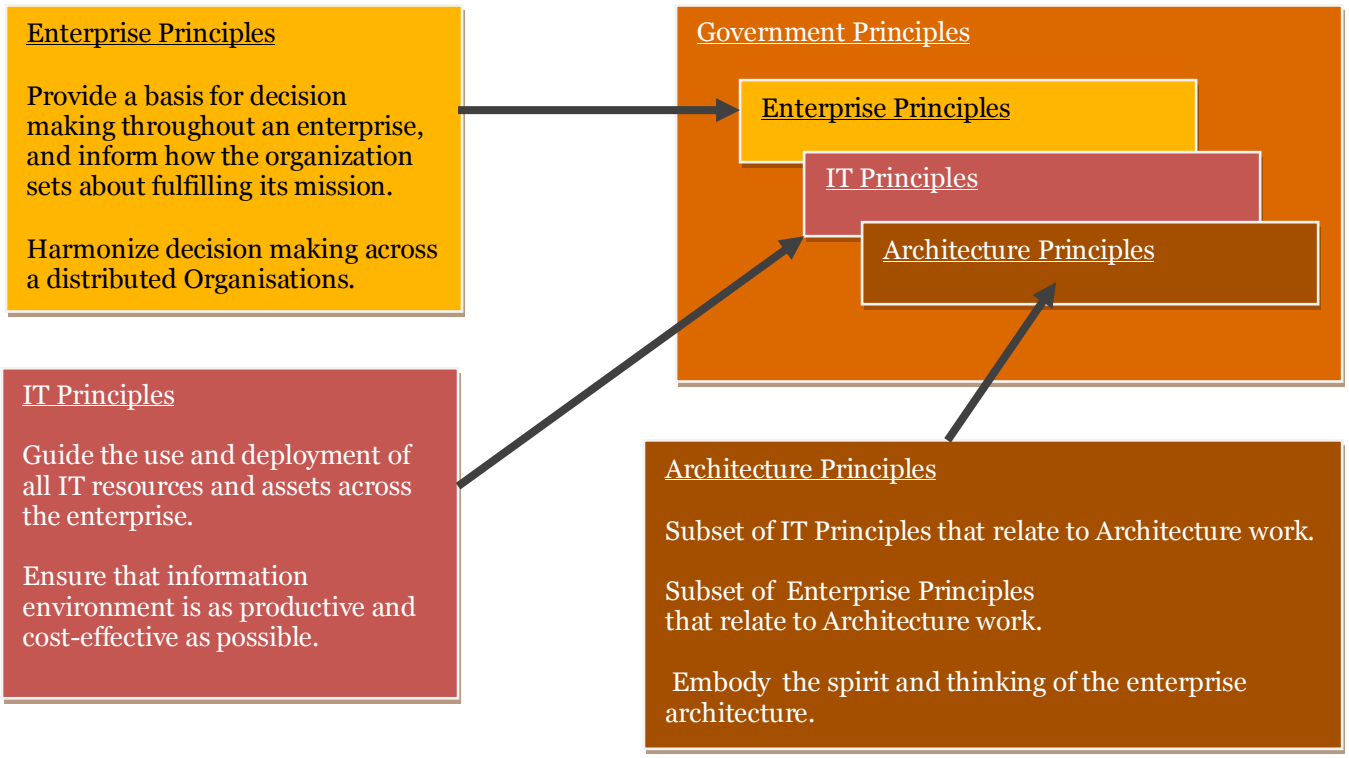
To define the relevant stakeholders, and their concerns and objectives, define the key business requirements to be addressed in this architecture effort, and the constraints that must be dealt with

To articulate an Architecture Vision and formalize the value proposition that demonstrates a response to those requirements and constraints

To create a comprehensive plan that addresses scheduling, resourcing, financing, communication, risks, constraints, assumptions, and dependencies, in line with the project management frameworks adopted by the enterprise (such as PRINCE2 or PMBOK)

3.1 Enterprise Architecture Principles

Principles must be established at multiple levels



3.1.1 Government Principles

Government Architecture principles are general rules and guidelines that support the way in which a Government organization sets about fulfilling its mission.

Architecture principles also provide the anchor for effective Architecture Governance, through a set of principles related to the government, corporation, regulations, IT etc.

The challenges facing the government in the 21st Century cut across agency missions. In fact, fiscal viability, security, environmental quality, health care, disaster response, global interdependence cut across governments and sectors, as well.

Government coordination depends upon consistent decision making across multiple departments and projects. But a natural tension exists whenever more than 25 ministries and its departments must work together as one. An enterprise-wide architecture tries to create a framework for effective decision making across multiple departments. Otherwise, independent groups decide alone resulting in inconsistency, information islands, isolated business processes, and inefficient technologies. This mixture is a recipe for poor performance.

To get consistent behaviour, the Nepal government must create a framework of guiding principles to define what is most important to the enterprise. Guiding principles define the government's strategy for certain business and technical functions. They balance department and agency mandates on the one hand and government-wide interests on the other. They filter decision making, eliminating solutions that don't meet the federal government's objectives. This clarity of executive intent takes the guesswork out of lower-level decisions. Clear, well-understood and sanctioned principles, combined with an executive commitment to enforce them, help drive change across disparate departments and programs.

Each of the architecture principles for the government has four parts: a statement of principle, brief description, the rationale for the principle, and implications or consequences of adopting or ignoring the principle. Other managerial and technical principles may exist. Ministries and its department's technical officials are expected to adopt these principles, and identify department-specific ones that express the same shared focus.

Preamble

The Government Enterprise Architecture is a mission-focused framework for ministries, its department, and its constitutional bodies to improve government performance. By aligning Governments, business processes, information flows, and technology consistently across and throughout the Government, the GEA builds a blueprint for improving programs.

Principle #1: The government focuses on citizens

Citizens' needs determine how government functions are defined and delivered. Functions include direct services and regulating society to serve the public.

Rationale

The government exists to serve the Nepal public who want simpler, faster, better and cheaper access to government services and information.

Implications

- Departments will design and apply their business processes and services to benefit citizens, even when the services cross lines of business.
- The federal government offers citizens a single, "unified" face, reducing duplicate, needlessly complex, inconsistent ways of using government services.
- Citizens can access government services through various means.

Principle #2: The government is a single, unified enterprise

The government operates as a single enterprise with decision-making flexibility at the agency level.

Rationale

A single enterprise with shared strategic objectives, common governance, integrated management processes and consistent policies improves the implementation of government-wide strategies and the coordination of the delivery of department citizen services.

Implications

- Government optimizes resource allocations across the enterprise to achieve common goals.
- Government optimizes information across the enterprise to support services and processes.
- Architectural designs integrate services for efficiency and keep autonomy of operations for effectiveness.
- Architectural designs identify and accommodate distinctive (non-homogenous) approaches to maintain important policy objectives.

Principle #3: The Government architecture is mission-driven

Government core mission needs and priorities are the primary drivers for architecture.

Rationale

A business-led architecture is more successful in meeting strategic goals, responding to changing mission needs and serving citizens' expectations.

Implications

- Business-approved architecture is a prerequisite for investment, so CIOs and architects must ask program leaders to say how it should look and work. Architecture is driven by program mission needs and enabling technology.
- Departments/Agencies will first seek to optimize business processes, and then use performance standards to define automation requirements.
- Systems and processes will use an architecture that responds quickly to events, including a "push" model for delivering information.
- The government and agencies will use their enterprise architectures to guide their capital planning, budget and investment decisions.
- Agencies will manage change in government operations with enough security to keep services flowing.
- Government solutions must be agile and flexible to meet business needs.

Principle #4: Security, privacy and protecting information are core government needs

Security, privacy and protecting information are integral to government operations, and are part of the architecture. Government must protect information against unauthorized access, denial of service, and both intentional and accidental modification.

Rationale

Government must protect confidential information to increase public trust and improve the security of its resources.

Implications

- The business context defines security and privacy requirements, which integrate into the entire architecture throughout the business lifecycle.
- Architectures must reflect policies to minimize improper use of data and security violations.
- Government must apply security and privacy consistently and monitor compliance.
- Information security controls need to be clearly defined so cost and risk are balanced and managed.

Principle #5: Information is a national asset

Information is an asset needed by citizens and leveraged across the government to improve performance.

Rationale

A well informed citizenry is necessary to our democracy. Further, accurate information is critical to effective decision making, improved performance, and accurate reporting.

Implications

- The government will improve its information sharing environment to better disseminate information to the public.
- This requires Government to identify authoritative sources of high quality information, and agencies to provide access to specified data and information.
- Authoritative data sources may need to be restructured and catalogued for easy dissemination, access and management.
- To realize this principle requires a government strategy to promote cost effective data sharing with other levels of government.

Principle #6: The architecture simplifies government operations

Architecture is designed to reduce complexity and enable integration to the maximum extent possible.

Rationale

Complex processes and systems with tightly coupled modules are difficult to manage, risk failure, are inflexible to changing agency mission needs, and are expensive to maintain. Highly modular, loosely coupled systems and processes take advantage of shared services and reusable components within government and available commercially.

Implications

- This requires loosely coupled software components shared as services and compatible application development.
- Agencies must share their best practices and reusable business and technical components.
- Building and integrating reusable components must become a common development method.

3.1.2 Architecture Principles

Architectural principles provide a set of general rules and overarching guidelines intended to support the long-term development and governance of the enterprise architecture. The goal of these principles is to apply constraints such that decisions reflect a balance of these elements, while providing maximum benefit to the organization. Principles may be just one element in a structured set of ideas that collectively define and guide the organization, from values through to actions and results providing a number of key benefits like -

- Provide a framework within which the government can make conscious decisions around IT
- Act as drivers for defining functional requirements for the architecture; and
- Provide input for assessing the existing IT systems and developing future strategic portfolio

Architecture Principles reflect a level of consensus across the government organization, and embody the spirit and thinking of "end-to-end" value for the government organization across the individual architecture domains of Business, Information (Data & Application) and Technology.

The following section lists some of the high level architectural principles that are to be applied to the Nepal Govt. enterprise architecture and the projects that implement it. The architectural principles has been categorized under the following architectural segments –

Business Architecture Principles

- Primacy of Principles
- Service Orientation: Identify & Deliver Government Services that are Critical, Flexible & Reusable
- Compliance with Legislation, Government Regulations and Standards

Data Architecture Principles

- Data is an Asset
- Data is shared
- Data is created, accessible and shareable
- Data has an owner/trustee
- Data security and permission
- Standard, Common vocabulary and data / metadata definitions.

Application Architecture principles

- Modular and component based
- Ease of use and re-use

Technical Architecture Principles *(Include integrations, infrastructure and security)*

- Interoperability
- Confidentiality
- Open standards based
- ESB based national service delivery gateway
- Web services for information exchange and granular service.
- Scalability, Availability, Backup & Archival
- Security Control Compliance, Selection & Standardization
- Levels of Security
- Security Measurement
- Use of common User Authentication Framework

Architecture Governance principles

- Formalize Governance Model to Govern GEA

3.1.2.1 Business Architecture Principles

Principle # 1	
Name	Primacy of Principles
Statement	The architectural principles defined apply to all government organisations, units / department and agencies within the Government of Nepal's GEA ICT initiative.
Rationale	• The effectiveness of an enterprise-wide GEA in terms of providing a consistent and measurable level of quality information to decision makers depends on all groups within an organisation abiding by the principles upon which that architecture is based. • Without this principle, inconsistency would rapidly undermine the achievement of the government's long-term objectives • These principles will guide the selection, creation and implementation of technology solutions and provide a workable transition path to targeted technologies, maintain flexibility and enhance interoperability and sharing.

Principle # 2	
Name	Service Orientation: Identify & Deliver Government Services that are Critical, Flexible & Reusable
Statement	The Government of Nepal's ICT information systems must identify and deliver services that are critical, flexible and sensitive to citizen needs. Identify common services that could be re-used by the other departments and ministries.
Rationale	• It is a key aim of any ICT vision to provide services in a flexible manner. This supports the target of improving service to citizens • Reusing services across departments & ministries eliminate duplicity. Duplicative capability is expensive and contributes to the proliferation of conflicting data
Implications	• A current state assessment of the possible set of government service to be conducted to review the business strategy / drivers and benchmark the existing processes & services against leading international best practices to arrive at the re-engineered services that are critical, flexible and reusable. • Data and information used to support enterprise decision making requires enterprise-wide standardization. • New systems and modifications will need to validate against a common Reference Architecture to enable systemic thinking as transactions cross traditional domain boundaries.

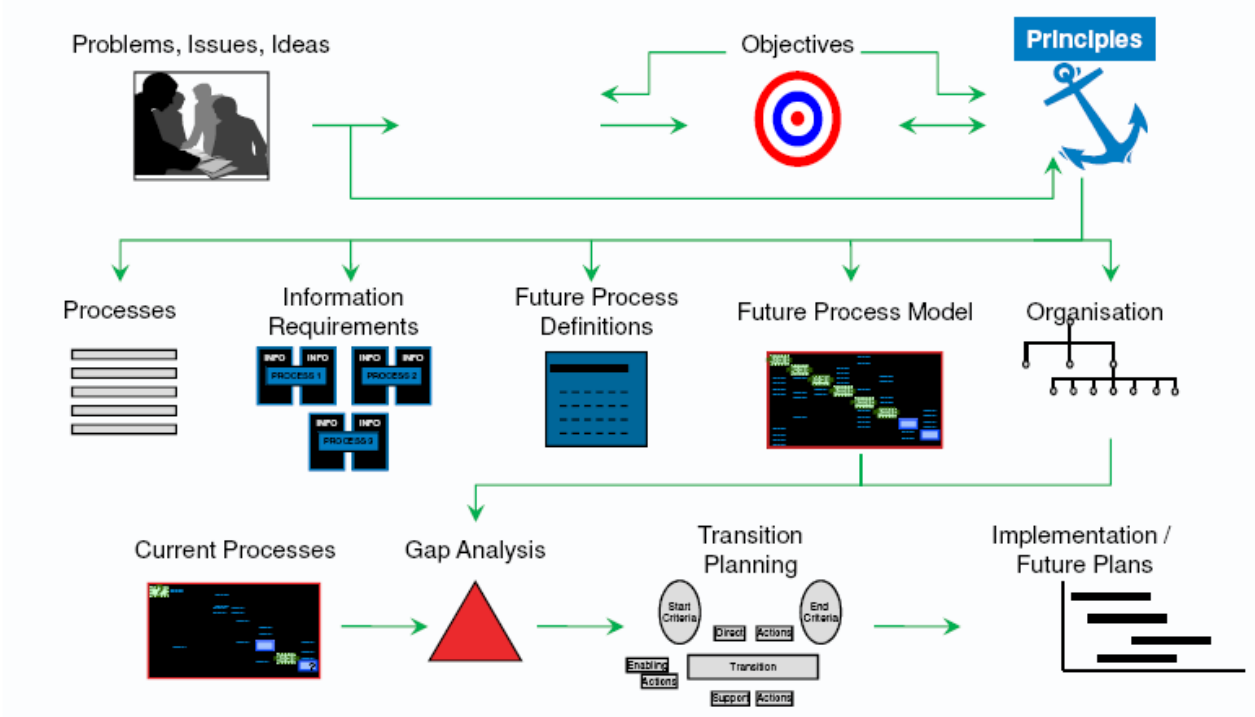
Principle # 3	
Name	Compliance with Legislation, Government Regulations and Standards
Statement	Government of Nepal's ICT information system access, processes and data management must comply with relevant legislation, government regulations and standard
Rationale	• Government GEA policies should necessarily be compliant with all applicable legislation, government regulation and standards • Compliance is key to maintaining stakeholder trust in the services that the GEA

	provides – e.g. ISO 27001 Privacy Directives, Data Protection Act, Right to Information Act, etc
Implications	• A current state assessment of the possible set of government service to be conducted to review the business strategy / drivers and benchmark the existing processes & services against leading international best practices to arrive at the re-engineered services that are critical, flexible and reusable. • Data and information used to support enterprise decision making requires enterprise-wide standardization. • New systems and modifications will need to validate against a common Reference Architecture to enable systemic thinking as transactions cross traditional domain boundaries.

3.1.3 Applying Architecture Principles

Principles are interrelated, and need to be applied as a set:

- For example the principles of "accessibility" and "security" tend towards conflicting decisions
- Each principle must be considered in the context of "all other things being equal"
- The rationale for decisions should always be documented
- A principle may be self-evident however it may not be conformed with – even when there are verbal acknowledgments of the principle



3.2 Capability Assessment

The Government and its departments have been implementing IT systems. The capability assessment helps to identify the current capability and with the establishment of Enterprise architecture, how it would improve the capability in the area of development and application of enterprise architecture and communicate its level of capability to its business partners. The architecture maturity models are used in enabling an enterprise to determine the state of enterprise architecture and to evaluate risks and options during the development of the enterprise architecture.

Capability Maturity Model Objectives

- To enable an organization to determine how capable they are in a particular area : In this case the development and application of enterprise architecture
- To enable an organization to set targets for the development of capabilities in a particular area.
- To enable an organization to communicate its level of capability to a business partner.

Architecture capability maturity model (ACMM)

(This model would aid in conducting Government internal assessments only)

Elements of ACMM are -

The Architecture Capability assessment maturity matrix consists of six maturity levels and nine enterprise architecture elements.

The six levels are

1 None
2 Initial
3 Under Development
4 Defined
5 Managed
6 Measure

The nine architecture elements are :

1 Architecture process
2 Architecture development
3 Business Linkage
4 Senior Management Involvement
5 Operating unit participation
6 Architecture communication
7 IT Security
8 Architecture Governance
9 IT Investment and Acquisition strategy

Two complementary methods will be used in the ACMM to calculate a maturity rating

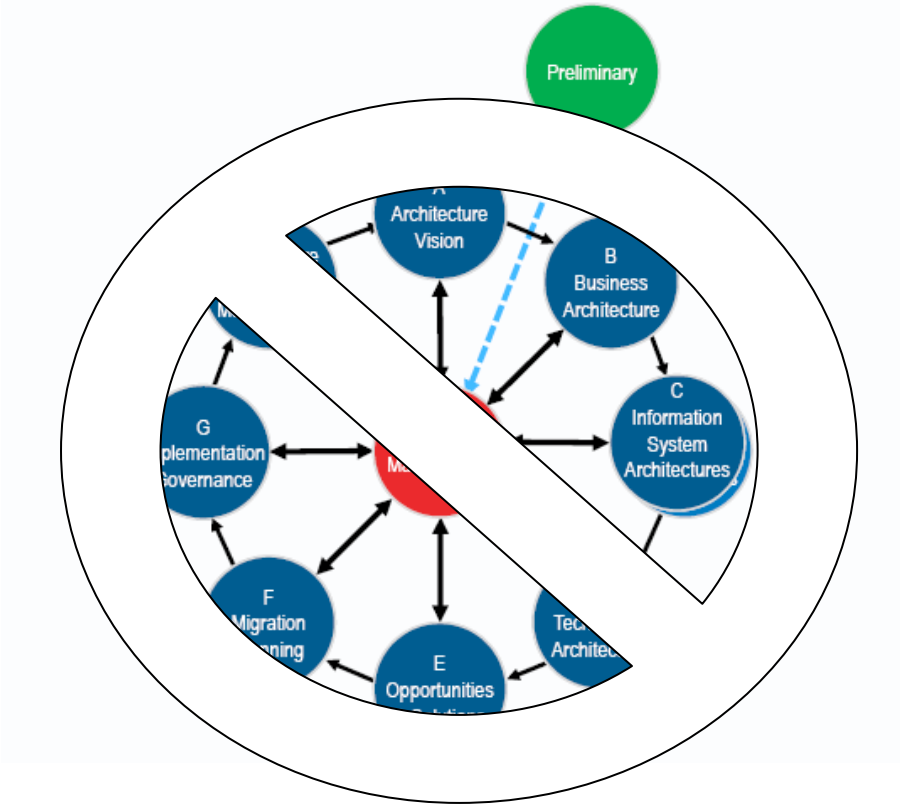
- The first method obtains a weighted mean Enterprise Architecture Maturity Level
- The second method shows the percentage achieved at each maturity levels for the nine architecture elements.

Method 1: Weighted mean Enterprise Architecture Maturity level using six levels

Maturity Level 1: None

Description of Maturity Level 1

- No Enterprise Architecture program. No Enterprise Architecture to speak of.



Assessment: The Government of Nepal EA capability was at level 1 before the beginning of the GEA Nepal project.

Maturity Level 2: Initial – Informal Enterprise Architecture Process underway

Description of Maturity Level 2

- Processes are ad hoc and localized. Some Enterprise Architecture processes are defined. There is no unified architecture process across technologies or business processes. Success depends on individual efforts.
- Enterprise Architecture processes, documentation and standards are established by a variety of ad hoc means and are localized or informal.
- Minimal, or implicit linkage to business strategies or business drivers.
- Limited management team awareness or involvement in the architecture process.
- Limited Operating Unit acceptance of the Enterprise Architecture process.
- IT Security considerations are ad hoc and localized.
- No explicit governance of architectural standards.
- Little or no involvement of strategic planning and acquisition personnel in the enterprise architecture process. Little or no adherence to existing Standards.

Assessment: The Government of Nepal EA capability was at level 2 before the beginning of the GEA Nepal project.

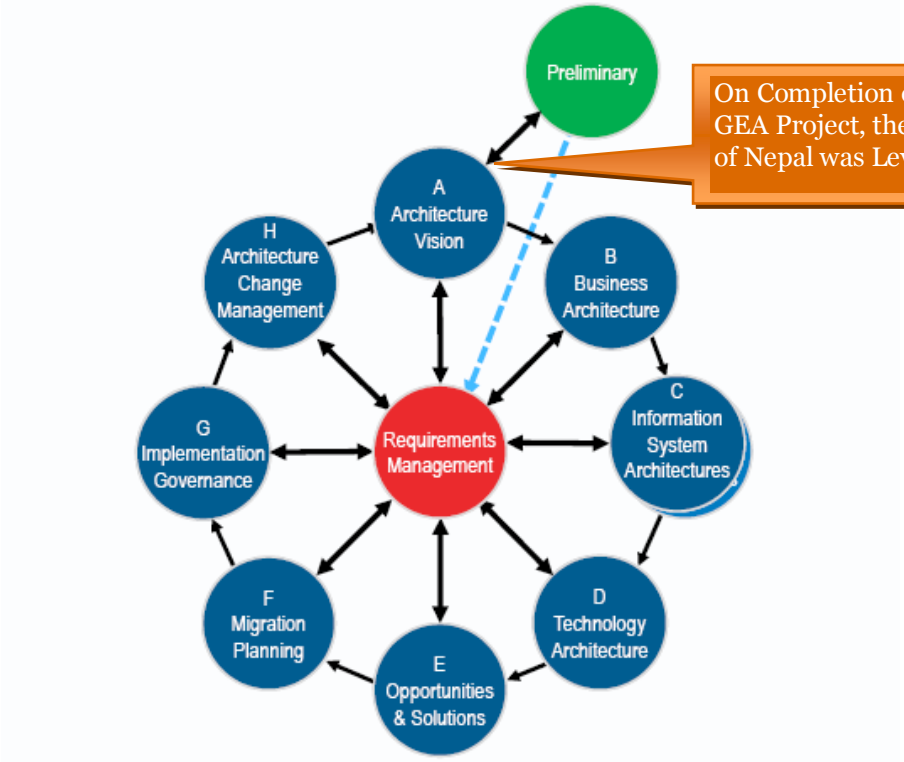
Before the start of Preliminary phase of GEA Project, the Architecture Capability of Nepal is Level 2

Assessment: The Government of Nepal EA capability was at level 2 before the start of Preliminary Phase.

Maturity Level 3: Under Development – Enterprise Architecture Process is under development

Description of Maturity Level 3

- Basic Enterprise Architecture Process program is documented. The architecture process has developed clear roles and responsibilities.
- IT Vision, Principles, Business Linkages, Baseline, and Target Architecture are identified. Architecture standards exist, but not necessarily linked to Target Architecture. Technical Reference Model (TRM) and Standards Profile framework established.
- Explicit linkage to Department processes.
- Management awareness of Architecture effort.
- Responsibilities are assigned and work is underway.
- The Governing body of Enterprise Architecture updates the Web Pages periodically and are used to document architecture deliverables.
- IT Security Architecture has defined clear roles and responsibilities.
- Governance of a few architectural standards and some adherence to existing Standards Profile.
- Little or no formal governance of IT Investment. Operating Unit demonstrates some adherence to existing Standards Profile.



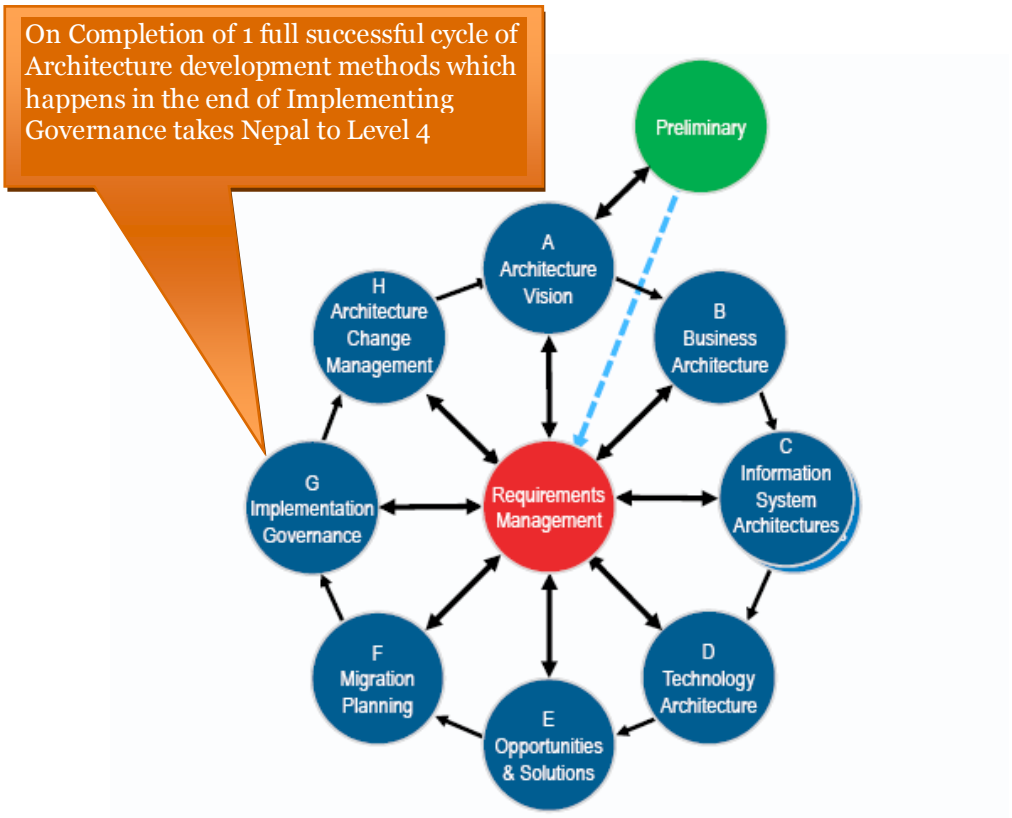
On Completion of Preliminary phase of GEA Project, the Architecture Capability of Nepal was Level 3

Assessment: The Government of Nepal EA capability was at level 3 after the completion of the Preliminary Phase of the GEA Nepal project.

Maturity Level 4: Defined – Defined Enterprise Architecture Including Detailed Written Procedures and Technical Reference Model

Description of Maturity Level 4

- The architecture is well defined and communicated to IT staff and business management with Operating Unit IT responsibilities.
- Gap Analysis and Migration Plan are completed. Fully developed Technical Reference Model and Standards Profile. IT goals and methods are identified.
- Enterprise Architecture is integrated with capital planning and investment control.
- Senior-management team aware of and supportive of the enterprise-wide architecture process. Management actively supports architectural standards.
- Most elements of Operating Unit show acceptance of or are actively participating in the Enterprise Architecture process.
- Architecture documents updated regularly on Departments Enterprise Architecture Web Page.
- IT Security Architecture Standards Profile is fully developed and is integrated with Enterprise Architecture.
- Explicit documented governance of majority of IT investments.



Assessment: The Government of Nepal EA capability is at Maturity level 4 as one full cycle of ADM has been successfully completed. Moving beyond maturity level 4 requires changes to people, processes and culture. This would be current level of Nepal with respect architecture maturity (as of Dec 2010).

Maturity Level 5: Managed – Managed and Measured Enterprise Architecture Process

Description of Maturity Level 5

- Enterprise Architecture process is part of the culture. Quality metrics associated with the architecture process are captured.
- Enterprise Architecture documentation is updated on a regular cycle to reflect the updated Enterprise Architecture. Business, Data, Application and Technology Architectures defined by appropriate de-jure and de-facto standards.
- Capital planning and investment control are adjusted based on the feedback received and lessons learned from updated Enterprise Architecture. Periodic re-examination of business drivers.
- Senior-management team directly involved in the architecture review process.
- The entire Operating Unit accepts and actively participates in the IT Architecture process.
- Architecture documents are updated regularly, and frequently reviewed for latest architecture developments/standards.

- Performance metrics associated with IT Security Architecture are captured.
- Explicit governance of all IT investments. Formal processes for managing variances feed back into Enterprise Architecture.
- All planned IT acquisitions and purchases are guided and governed by the Enterprise Architecture.

Assessment: The Government of Nepal EA capability will achieve these levels after the complete roll out of and adoption GEA Nepal. This will be the next Maturity level for the Nepal Government to target.

Maturity Level 6: Measured - Continuous Improvement of Enterprise Architecture Process

Description of Maturity Level 6

- Concerted efforts to optimize and continuously improve architecture process.
- A standards and waivers process is used to improve the architecture development process.
- Architecture process metrics are used to optimize and drive business linkages. Business involved in the continuous process improvements of Enterprise Architecture.
- Senior management involvement in optimizing process improvements in Architecture development and governance.
- Feedback on architecture process from all Operating Unit elements is used to drive architecture process improvements.
- Architecture documents are used by every decision maker in the organization for every IT-related business decision.
- Feedback from IT Security Architecture metrics are used to drive architecture process improvements.
- Explicit governance of all IT investments. A standards and waivers process is used to improve governance-process improvements.
- No unplanned IT investment or acquisition activity.

Assessment: The Government of Nepal EA capability will achieve these levels when the improvement cycles are planned, measured and implemented over the existing architecture process. The Nepal Government these levels after achieving Level 5.

3.3 Risk Management

Risk Management is a technique used to mitigate risk when implementing an architecture project

Two levels of risk

- Initial Level of Risk
  - Risk categorization prior to determining and implementing mitigating actions
- Residual Level of Risk
  - Risk categorization after implementation of mitigating actions

Risk Management Processes

- Risk classification
- Risk identification
- Initial risk assessment
- Risk mitigation and residual risk assessment
- Risk monitoring

Risk Classification Scheme

Corporate Risk Impact Assessment					
Effect	Frequency				
	Frequent	Likely	Occasional	Seldom	Unlikely
Catastrophic	E	E	H	H	M
Critical	E	H	H	M	L
Marginal	H	M	M	L	L
Negligible	M	L	L	L	L

E: Extremely high risk

H: High Risk

M: Moderate Risk

L: Low Risk

Risk Identification for GEA Nepal and its Mitigation Assessment

Risk Category	Risk factors	Preliminary Risk			Mitigation	Residual Risk
		Effect	Frequency	Impact		
Organization Fit	Slower adoption of business process re-design	Critical	H		Focused BPR exercise	NA (Currently in iteration 1)
Organization Fit	Lack of Mandate to follow enterprise wide Design that supports Data integration	Critical	H		GEA Governance body to drive this.	NA
Skill Mix	Insufficient training and re-skilling	Marginal	M		Focused efforts on training	NA
	Insufficient internal expertise	Critical	H		Coach internal experts	NA

Risk Category	Risk factors	Preliminary Risk			Mitigation	Residual Risk
	Lack of business analysts with business and technology Knowledge	Marginal	M		Augment the expert staffing/Consultants	NA
	Failure to mix internal and external expertise effectively	Marginal	M		Adopt an effective outsourcing model to hold IP	NA
Management structure and strategy	Ineffective communications	Critical	H		Adopt a communication plan	NA
	Lack of proper management control structure	Catastrophic	E		Governance Structure with empowered status.	NA
	Lack of a champion	Catastrophic	E		Clearly identified Champion.	NA
Software systems design	Failure to adhere to standardized specifications which the software supports	Critical	H		Review process to stringent to dis-allow non compliant systems to move to production.	NA
	Lack of integration	Marginal	M		Follow GEA guidelines	NA
User involvement and training	Insufficient training of end-users	Critical	H		Focused staff training	NA
	Ineffective communications	Marginal	M		Better collaboration and messaging platform	NA
Technology planning/integration	Attempting to build bridges to legacy applications	Marginal	M		Phased approach to enabling / revamping legacy.	NA

3.4 Statement of Architecture Work

A Request for Architecture Work describes the business imperatives behind the architecture work, thus driving the requirements and performance metrics for the architecture work. This should be sufficiently clear so that initial work may be undertaken to scope the business outcomes and resource requirements, and define the outline information requirements and associated strategies of the architecture work to be done.

The Request for Architecture Work is a document that is sent from the sponsoring organization to the architecture organization to trigger the start of an architecture development cycle. Requests for Architecture Work can be created as an output of the Preliminary Phase, a result of approved architecture Change Requests, or terms of reference for architecture work originating from migration planning.

In general, all the information in this document should be at a high level.

Request for Architecture Work

Summary of Request

In 2005, the Government of Nepal (GoN), adapted e-Government Master Plan (eGMP), with the objective of using Information and Communication Technology (ICT) to enhance government process, service to citizens and foster social integration, economic growth and poverty reduction. The Asian Development Bank (ADB) provided Technical assistance for developing the e-Government projects under the guidelines of eGMP and Enterprise Architecture is one of the major projects. The Implementing agency for this project is Ministry of Home Affairs.

Under the eGMP, all the citizen centric services that are provided by the GoN were prioritized in order to identify the services which have the most impact to the citizen. The objective was to identify government services which are critical to the citizen and those which cause the most inconvenience to the citizen at present, when obtaining such services. Through Business Process Reengineering, these services would be reengineered to make them more efficient and citizen friendly. ICT would be used as an energizing tool to further enhance the efficiency of the reengineered business processes. These services are referred to as 'eServices'.

The Government of Nepal intends to leverage ICT in meeting its development goals and has designed the E-Governance Master Plan with a specific focus in the areas of e-Services, e-Community and e-Economy.

As an important component of the e-Governance initiatives in Nepal, it is envisioned that practically all the eServices and electronic information in Nepal will be delivered via a comprehensive integration platform and collections of portals and applications. This wide collection of software infrastructure and systems which is envisioned to be the gateway for electronic information and electronic interactions in Nepal is generally referred to as Government Enterprise Architecture (GEA) initiative.

All the government and public e-Services (electronic Services) will be compliant with the GEA. This project envisions the planning, design, development or customization to the requirements of the Government of Nepal, facilitation and implementation of all required infrastructure, protocols, frameworks and national standards for Government Enterprise Architecture.

This ICT development project has been taken up to support concrete initiatives to implement the Government's ICT-led development strategy. The project aims at (i) improving the enabling environment for the use and adoption of ICTs for economic development, (ii) generating increased employment in the IT and IT-Enabled Services sector and (iii) enhancing efficiency, transparency and accountability to facilitate good governance and improve access to information and services for citizens and businesses.

The Government considers that for good governance, easy access to quality/ timely information is a must. Cognizant of this, the Government is keen to provide access to information and knowledge to citizens and businesses to empower them to fully participate in the processes of governance.

Organization Sponsors

This architecture work is requested and sponsored by:

Mr. Juddha B. Gurung

Member Secretary

High Level Commission for IT

juddha_hits@wlink.com.np

Business Imperative

Most countries have evolved or are in the process of evolving strategies for standards and e-government frameworks for government business and effective public service delivery. The aim is to assist IT managers and software developers to access a single point of reference, to locate appropriate standards and architecture specifications that should be followed for the specific project. This can be achieved by bringing together the relevant specifications under the overall framework. In complying with the pre-determined standards and specifications, system designers can ensure interoperability between systems while retaining the flexibility to select different hardware platforms, and application software to implement specific solutions.

With the rise of multi-tier applications, the variations with which applications can be delivered have dramatically increased. Organizations have started to recognize the need for a standardized baseline model that can act as a template for all others. This baseline has been abstract in nature but specifically aims to define the technology, boundaries, rules, limitations, and design characteristics that apply to all applications in the pursuit of efficiency, economy and interoperability. This gives rise to application architecture.

Current e-government practices are fraught with many inherent deficiencies and shortcomings. Systems are generally not designed for cross-platform interoperability and information sharing.

The rationale and method for Enterprise Architecture (EA) forms an inherent part of the e-government investment program.

Business Goals (and Changes)

The rationale for establishing e-government needs to relate directly to the common needs and goals of the community if it is to form a vision for an e-government program in Nepal. The vision needs to be shared by the stakeholders including communities, businesses, special interest groups and others.

Such goals commonly include

- Rural poverty alleviation
- Improved service delivery to the community;
- Enhanced productivity (and efficiency) of government agencies;
- Gender and youth agendas
- More effective rule-of-law with a stronger legal system and law enforcement;
- Economic and business development
- Strengthening participation and other aspects of good governance.

Strategic Plans of the Business

The underlying concept for the planned approach is that the Government of Nepal is to be perceived as a single entity with a seamless flow of information across individual ministries and departments. *A standards and architecture framework should be provided to ensure uninterrupted and seamless flow of information and to improve the coherence of information systems maintained by agencies supporting easy integration of government applications and supporting existing and any new technology and tools without under the same framework.* The framework should define the set of specifications to facilitate government systems to communicate and efficiently and effectively interoperate with other systems, both within the government and external to it.

The EA for this Nepal e-government program should be developed to ensure that the following attributes, but not limited to, are addressed in every aspect of design and application:

- ***Interoperability***: Interoperability allows seamless exchange of information, reuse of data models and inter-changeability of data across systems.
- ***Open Standards:*** Open standards are expected to provide interoperability, data preservation and greater freedom from technology and vendor lock-in. Adoption of open standards will facilitate storing of electronic national records and data using open data file formats.
- ***Flexibility*:** The framework facilitates adoption of new technologies and allows managing any change in governance processes.
- ***Collaboration:*** The architecture provides a platform that will allow various stakeholders to make use of the repositories such as reusable models, script, data and metadata etc.
- ***Technology*:** The technologies adopted are open so that they can be easily interfaced with other systems and other systems with them.

Enterprise architecture must integrate the existing information systems on a continuous basis and cannot be considered as a one-off effort.

There are various frameworks for EA design frameworks to choose from such as Zachman Framework (ZF), the Open Group Architecture Framework (TOGAF)[1] first developed in 1995, Department of Defence Architecture Framework (DODAF), and the Federal Enterprise Framework (FEA).

Success Criteria

The following compliance requirements at minimum are set out for the Government Enterprise Architecture version 1.0.

GEA Standards & Guidelines
Network Domain
Platform Domain
Data Management Domain
Distributed Environment Management (DEM) Domain
Application Domain
Collaboration and Workflow Domain
Middleware Domain
Security Domain
Web Domain

Adherence to 'Government Enterprise Architecture' (GEA) in case of Government e-Services Portal

GEA will address a consistent set of principles, standards and guidelines that guide the government agencies in the design, acquisition, implementation and management of ICT systems. It enables interoperability for cross-agencies' systems leading to better information sharing amongst agencies, provide awareness and framework for coherent system design and technology selection, reduce integration complexity for cross-agencies' systems,

[1] The Open Group Architecture Framework: http://www.opengroup.org

maximize the ability to leverage existing technology assets which are widely accepted by the IT industry, and facilitate disciplined and alignment in development and deployment of systems and infrastructure

Adherence to Nepal e-Government Interoperability Framework (NeGIF)

'NeGIF' establishes the recommendations for common data architecture and standards for data exchange between various institutes of Government of Nepal. 'NeGIF' is formulated to provide guidelines to different government organizations to standardize the data architecture and data exchange. XML is identified as the standard format for data exchange between these organizations

Adherence to 'Government Internet Connectivity Framework'

The information backbone infrastructure for the e-Government System will be enabled by the 'Internet Service by an Internet Service Provider' (to be considered under separate Contract), which connects most of the project sites with minimum 128kbps bandwidth connectivity. E-Government Internet Connectivity will be a widely available, secure and reliable underlying information infrastructure backbone. The connectivity between the NITC Government Data Centre (GIDC) and project sites will be provided through a Backbone of fibre optic cables/wireless Internet Connectivity or satellite to procuring entities with independent dedicated leased lines provided by the Internet Service Providers, including CDMA, WiMAX based Internet Connectivity in some of the distant entities in different districts. GIDC will have uninterruptible dedicated Internet Connectivity with 99.95 uptime and local loop connectivity of uptime 99.99.

Timescale

Please refer the Project Plan

3.5 Stakeholder Management

An important discipline that successful architecture practitioners can use to win support from others

Benefits:

- The most powerful stakeholders can be identified early and their input can then be used to shape the architecture
- Support from the more powerful stakeholders will help the engagement win more resource
- By communicating with stakeholders early and frequently, the architecture team can ensure that they fully understand the architecture process
- The architecture engagement team can more effectively anticipate likely reactions to the architecture models and reports, and can capitalize on positive reaction whilst avoiding or addressing any negative reactions

The following **RACI** chart shows the key stakeholders and their activities, and the role played by each stakeholder in terms of (**R**)esponsible, (**A**)ccountable, (**C**)onsulted, (**I**)nformed for the engagement

Key Stakeholders	Designation / Depts	Activity	R	A	C	I
Mr. Manohar Kumar Bhattarai	Vice Chairman	Key Stakeholder	√	√		
Mr. Juddha B. Gurung	Member Secretary	Key Stakeholder	√	√		

Key Stakeholders	Designation / Depts	Activity	R	A	C	I
Mr. Ombindu L. Rajbhandary	Team Leader. Project Management Consultant	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Debesh Prasad Lohani	System Integration Specialist, Project Management Consultant	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Anup Babu Shreshtha	Project Management Consultant	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Ishwar M Shreshtha	Network Integration Specialist. Project Management Consultant	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Birendra Kumar Mishra	Director, IT, Inland Revenue Department	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Amber Sthapit	Deputy Director, Engineering Section, Nepal Telecom Authority	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Purushottam Khanal	Deputy Director, Administration, Nepal Telecom Authority	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Deepesh Acharya	Deputy Manager, License & R T D Section, Nepal Telecom Authority	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Bikal Paudel	Deputy Director, PIU Member, Nepal Information Technology Centre	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Kapil Dev Shrestha	Director, IT, Department of Land Reforms and Management	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Chudamani Guragain	Computer Officer, Department of Land Reforms and Management	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Anil Kumar Gurung	Director, Department of Transport Management	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Harish Bhatt	Computer Officer, Department of Transport Management	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Prahlad Pokhrel	Under Secretary, PIU Member – NID, National	Sharing As-is dept landscape			√	√

Key Stakeholders	Designation / Depts	Activity	R	A	C	I
	Identity Card Management Centre	and GEA requirements				
Mr. Jagat B Bhandary	Computer Officer, Ministry of Home Affairs	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Dilli Raj Pokharel	Section Officer, Ministry of Home Affairs	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Manish Luatel	Computer Engineer, Ministry of Home Affairs	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Rajendra Sigdel	Section Officer, Ministry of Home Affairs	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Sushil Kumar Ojha	Joint Secretary, Public Service Commission	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Lok Raj Sharma	Computer Officer, Public Service Commission	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Sashidhar Karki	Public Service Commission	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Ramesh Sharma Paudyal	Computer Officer, Ministry of General Administration	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Ridesh Tamrakar	Computer Operator, Dept. of Civil Personnel Record, Ministry of General Administration	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Shyam Sundar Sharma	Joint Secretary, Election Commission	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Ram Govind Aryal	Computer Officer, Election Commission	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Avanindra Kumar Shrestha	Secretary, Public Procurement Monitoring Unit	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Mahesh Singh Kathayat	Head of Computer Division, Police Headquarters, Naxal	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Tribhuvan M S Pradhan	Chief, IT Section, Kathmandu Metropolitan City Office	Sharing As-is dept landscape and GEA requirements			√	√

Key Stakeholders	Designation / Depts	Activity	R	A	C	I
Mr. Deepak Timil Sina	MIS Director, Supreme Court	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Utsav R. Wagle	Software Developer, Supreme Court	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Sanjay Manandhar	Computer Engineer, Office of the Financial Comptroller General	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Sushil Pandey	Undersecretary, Office of the Financial Comptroller General	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Sudip Aryal	Computer Engineer, Department of Post	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Sharda Prasad Paudyal	Department of Post	Sharing As-is dept landscape and GEA requirements			√	√
Mr. Shakil Manandhar	Engineer, Department of Roads	Sharing As-is dept landscape and GEA requirements			√	√
Architects, PwC			√	√	√	√
Delivery Manager, PwC			√	√	√	√

3.6 Architecture Vision

An architecture vision would include the following

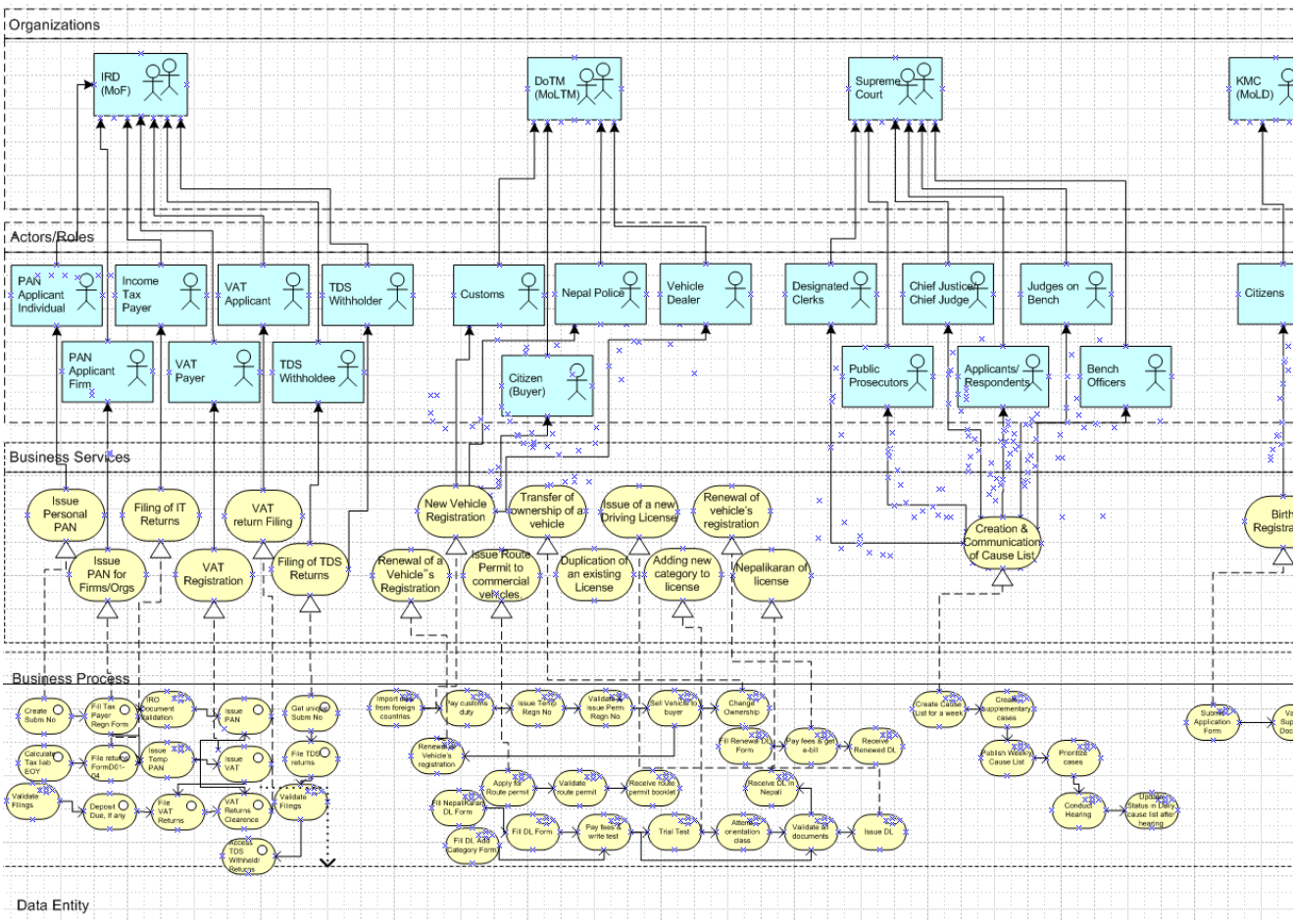
- Refined key high level stakeholder requirements

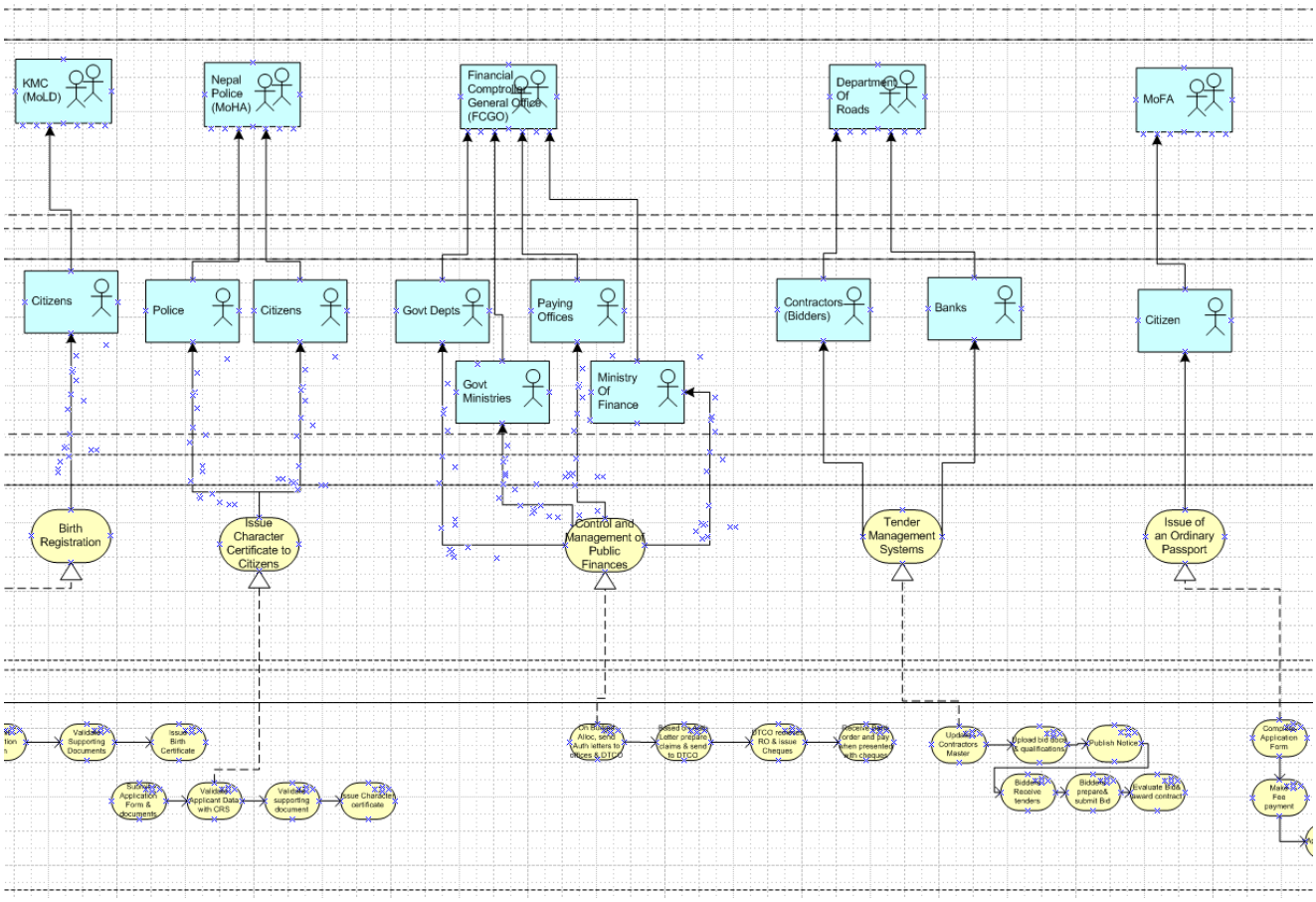
Rqmt ID	Requirement	Description
GEA_BU_01	Capture the business process maps of Whole-of Government structure	Fundamental organization of Government's work, embodied in Its processes and people, their relationships to each other and the environment, and the principles governing design and evolution
GEA_BU_02	Department Service goals and objectives	eGov services to be identified that could be re-used by the other department and ministries.
GEA_BU_03	e-Gov Services to identify the possible set of Web Service with respect to consumer and producer of services	Arrive at a As-is assessment of the possible set of Government Service processes and advocate the To-be process approaches.

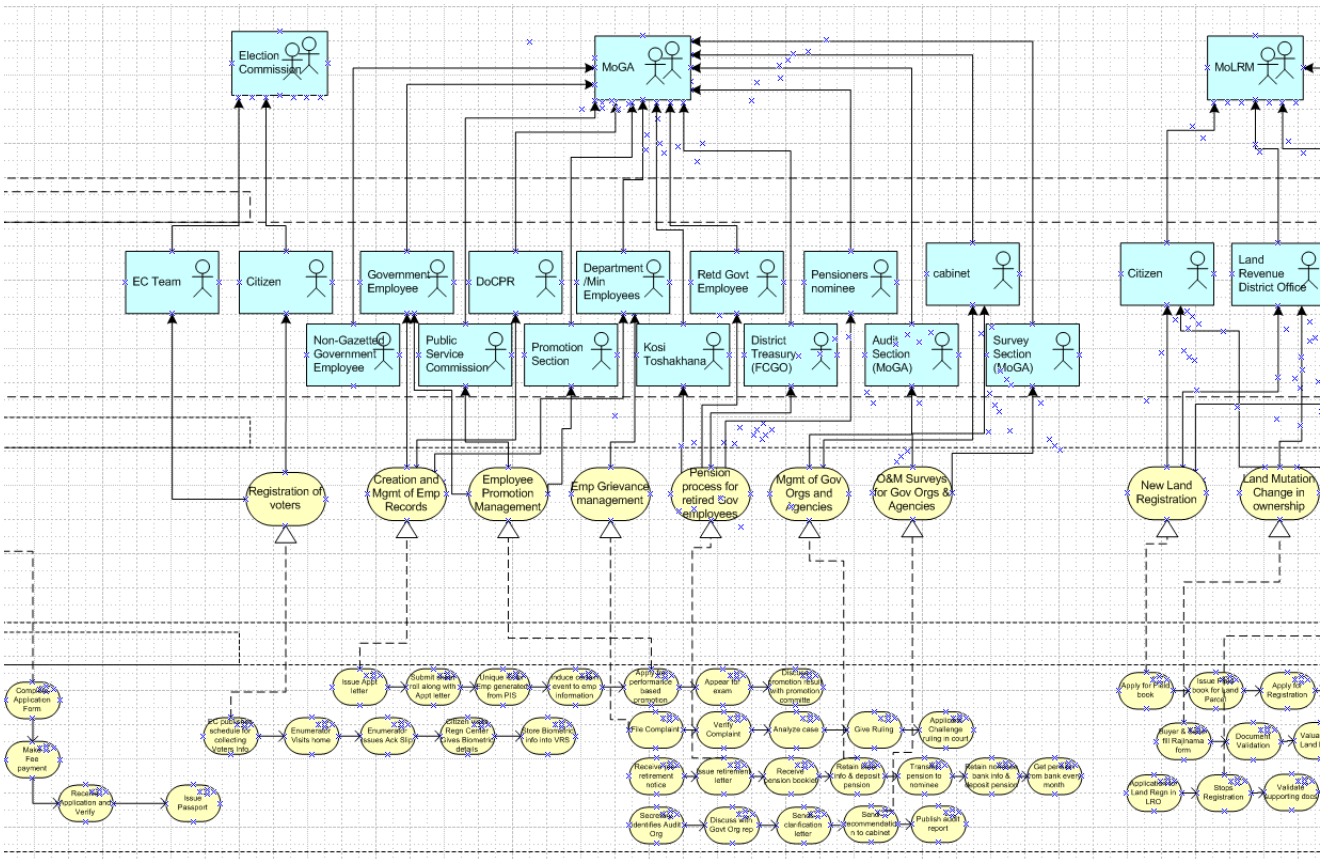
Rqmt ID	Requirement	Description
GEA_BU_04	Alignment of organization and functions	The services churned out from each department of the ministries would reflect the alignment of the functions of each department.

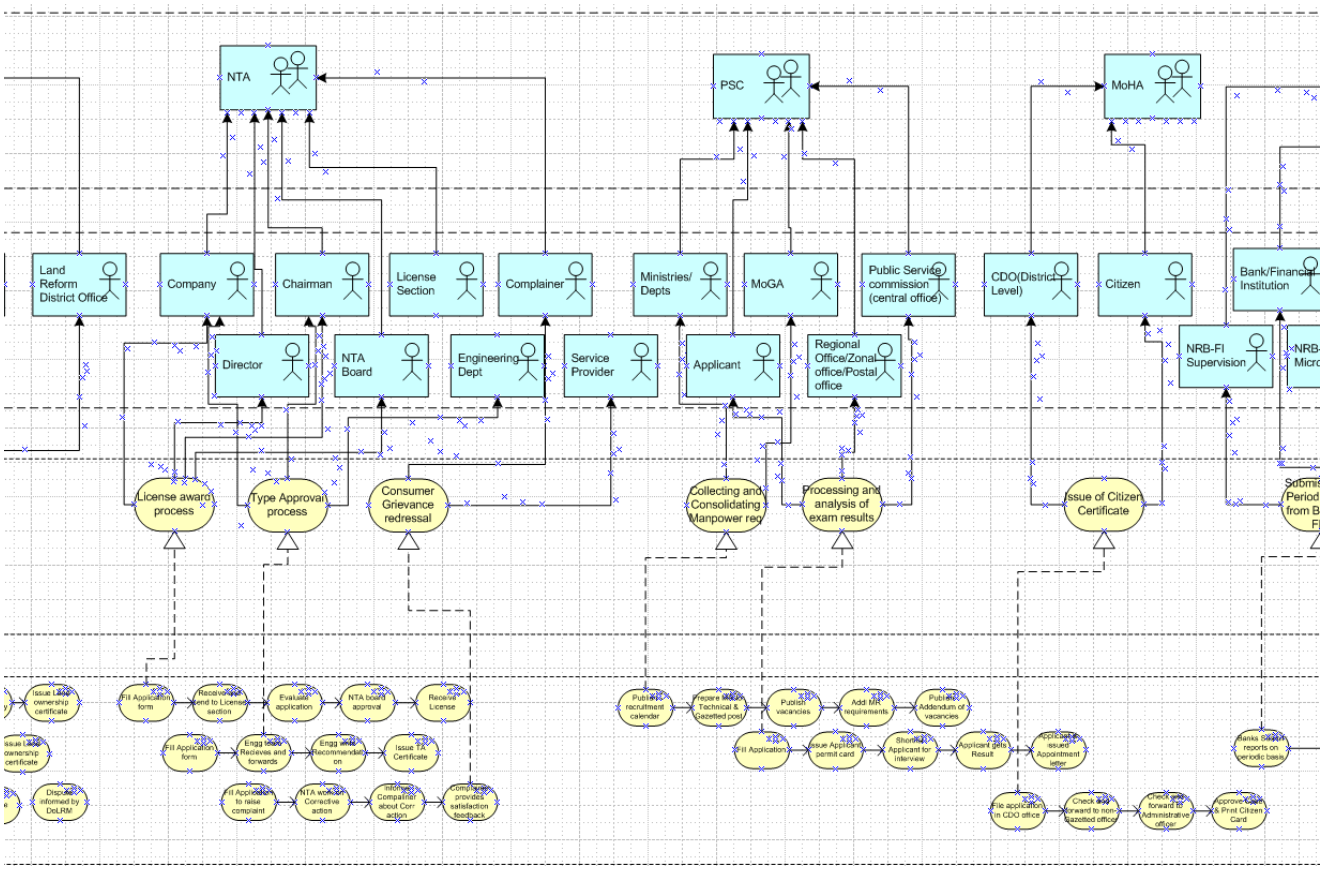
Baseline Business Architecture (Vision) v 0.1

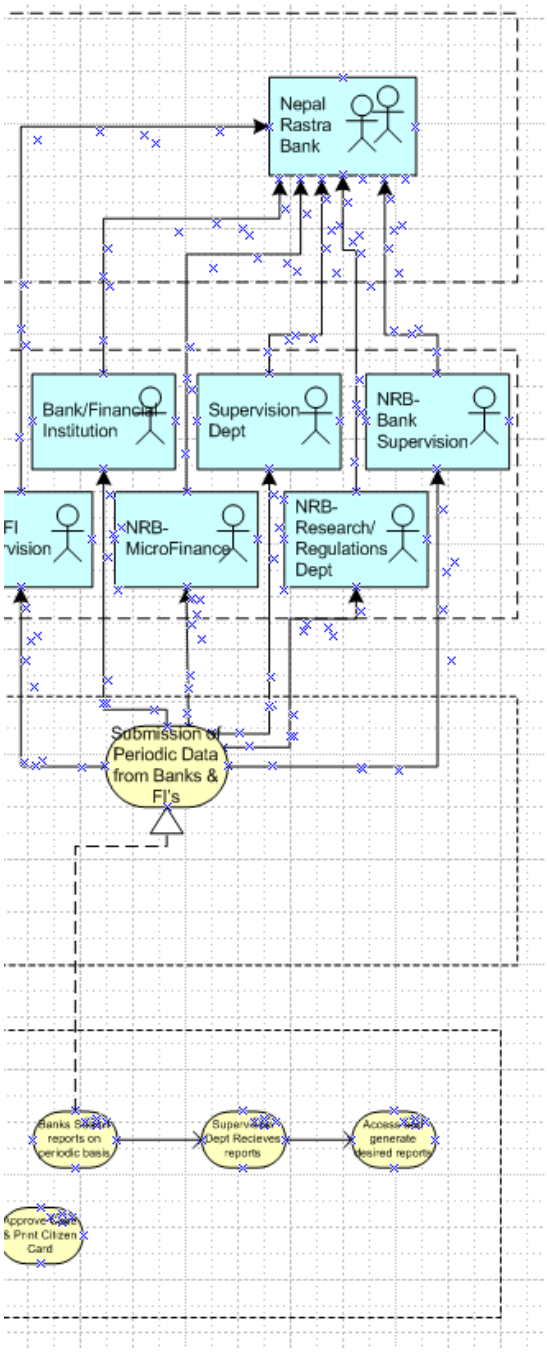
Following diagram has been split vertically from a vision document



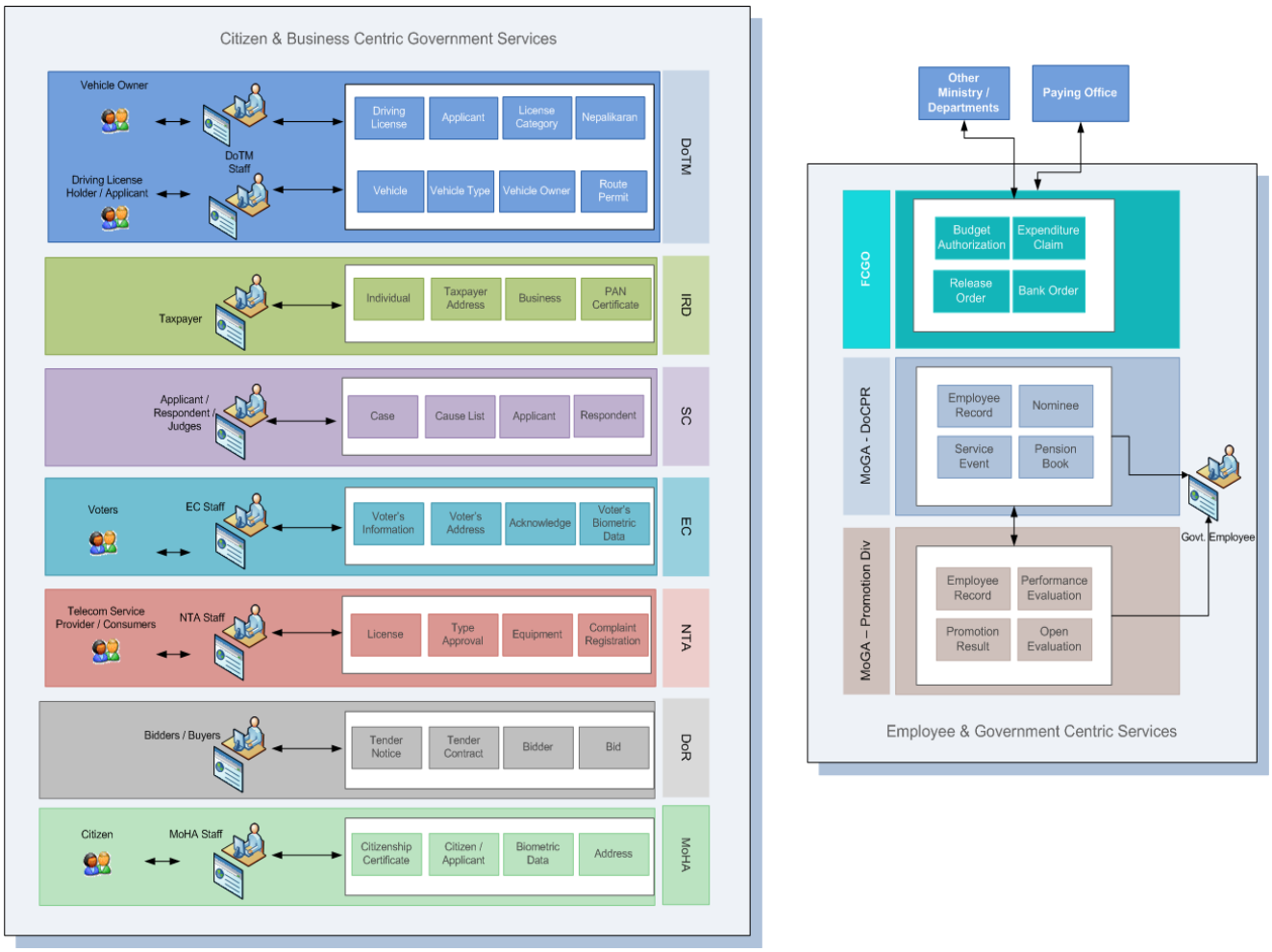

KMC (MoLD)
Nepal Police (MoHA)
Financial Comptroller General Office (FCGO)
Department Of Roads
MoFA
Citizens
Police
Citizens
Govt Depts
Paying Offices
Contractors (Bidders)
Banks
Citizen
Govt Ministries
Ministry Of Finance
Birth Registration
Issue Character Certificate to Citizens
Control and Management of Public Finances
Tender Management Systems
Issue of an Ordinary Passport


Election Commission
MoGA
MoLRM
EC Team
Citizen
Government Employee
DoCPR
Department /Min Employees
Retd Govt Employee
Pensioners nominee
cabinet
Citizen
Land Revenue District Office
Non-Gazetted Government Employee
Public Service Commission
Promotion Section
Kosi Toshakhana
District Treasury (FCGO)
Audit Section (MoGA)
Survey Section (MoGA)
Registration of voters
Creation and Mgmt of Emp Records
Employee Promotion Management
Emp Grievance management
Pension process for retired Sov employees
Mgmt of Gov Orgs and Agencies
O&M Surveys for Gov Orgs & Agencies
New Land Registration
Land Mutation Change in ownership


NTA
PSC
MoHA
Land Reform District Office
Company
Chairman
License Section
Complainer
Ministries/ Depts
MoGA
Public Service commission (central office)
CDO(District Level)
Citizen
Bank/Financial Institution
Director
NTA Board
Engineering Dept
Service Provider
Applicant
Regional Office/Zonal office/Postal office
NRB-FI Supervision
License award process
Type Approval process
Consumer Grievance redressal
Collecting and Consolidating Manpower req
Processing and analysis of exam results
Issue of Citizen Certificate



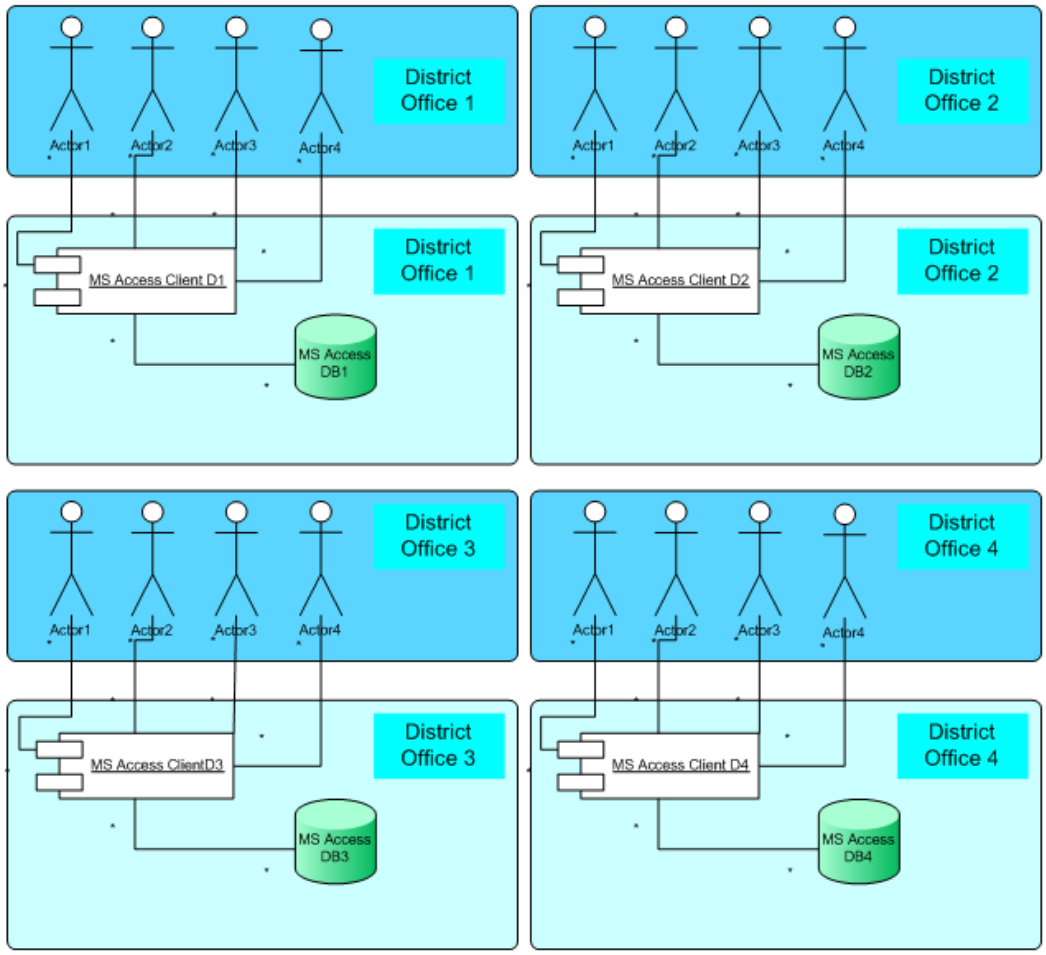
Baseline Data Architecture (Vision) v0.1



Baseline Application Architecture (vision) v0.1

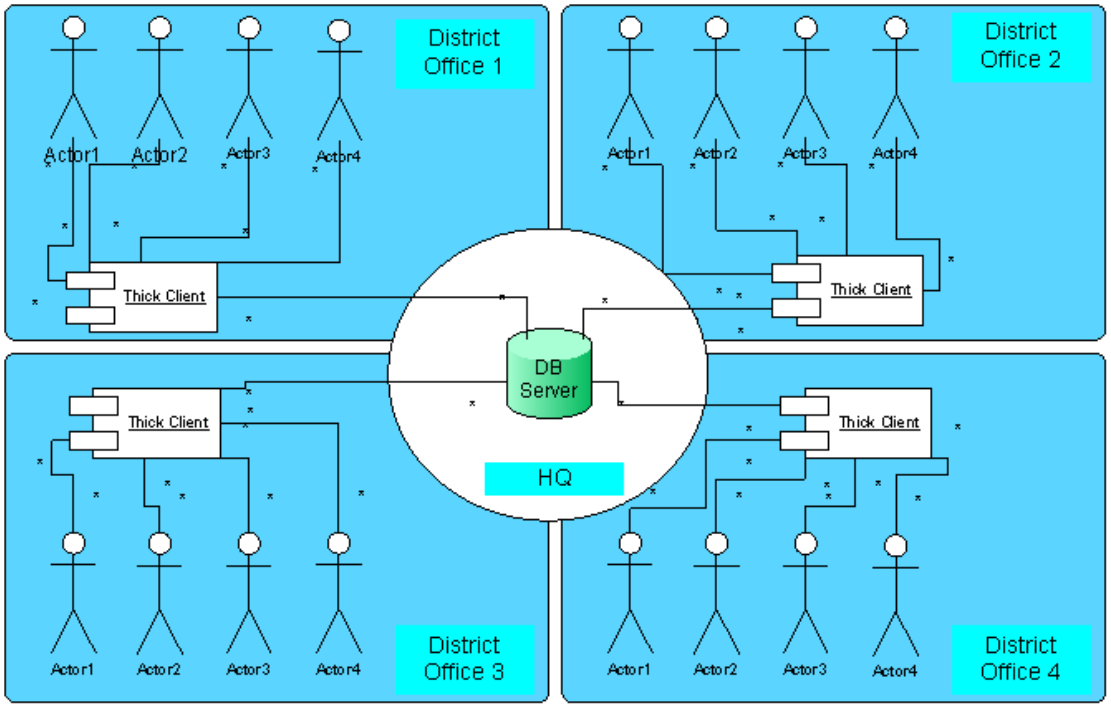
Type 1 Applications

The Type 1 Applications are monolithic applications that houses both the application and database servers execute in the single platform and single server/desktops.



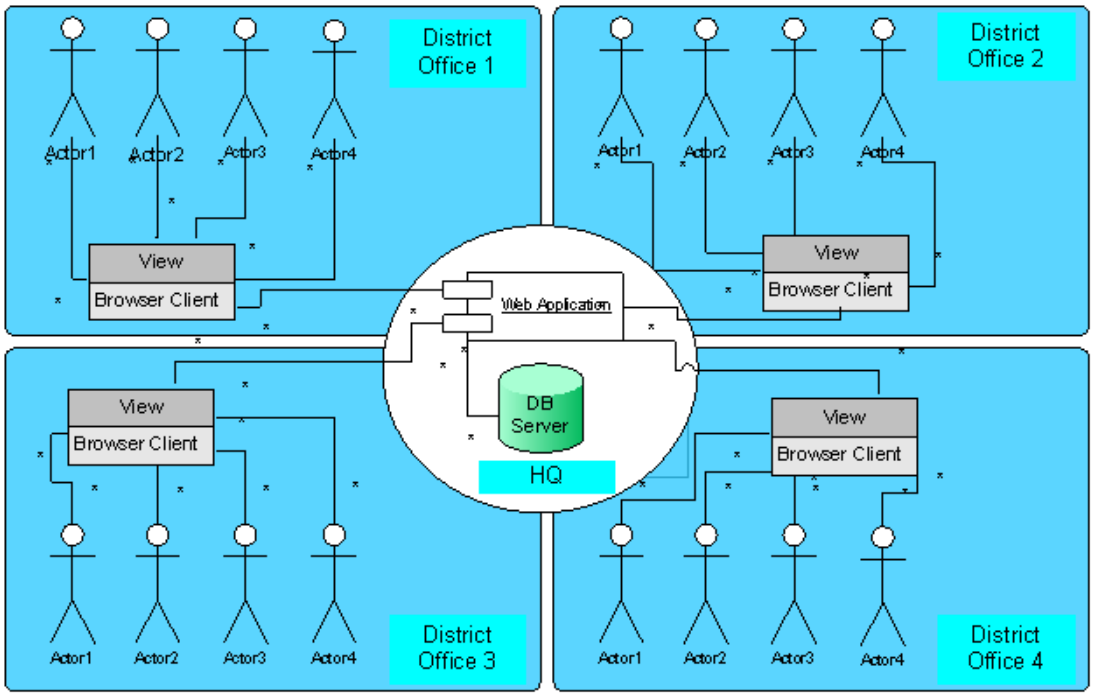
Type 2 Applications (Client Server Architecture)

The Type 2 Applications are client server applications, which have a common database for all clients connecting to it. However, the business processing logic remains in the client side of the applications.



Type 3 Applications (MVC Architecture)

The Type 3 applications are web enabled applications that 3 tier applications where the client is a browser and application resides on the web server or the application server, the call from the application server access the database server.



Type 4Applications (Hybrid Architecture)

The type 4 Applications are both client server based and web enabled applications that are required to be in this architecture due to the current infrastructure limitations across Nepal. In these type of application the field force/ District office with limited access to the connectivity to the centralized database switch to client server mode with lack of access to the central db and on obtaining connectivity switch to the online mode, by first synching up with the centralized DB and also have the features to transact online. This is a combination of Type 2 and Type 3 applications.

Baseline Technology Architecture (vision) v0.1

As per the survey conducted by PwC to understand the current state of IT infrastructure across departments it shows that while the FCGO, the MoGA and the Supreme Court of Nepal have relatively secure environments, in comparison to the other departments, there is a lack of resource management and resource optimisation tools. The current scenario is diverse, with practically minimalist infrastructure in departments like the Municipalities and at the same time departments like the department of Post and MoGA are significantly IT enabled and have a progressive IT adoption road-map.

This diverse spectrum of IT maturity requires that a significant capacity building exercise in terms of IT awareness and IT enablement be conducted to bring the departments at a minimum shared infrastructure level.

To broadly outline the relevant current state IT infrastructure, the present infrastructure landscape of the following 3 departments with relatively secured environment has been considered

1. Nepal Police
2. The Department of Posts
3. Ministry of General Administration

Nepal Police transacts in extremely confidential and secured data, however, the current resource management, network security, user management and physical security infrastructure are insufficient to provide even basic levels of security. We also recommend that the SWAN which is currently being leased from the NTC be an owned resource to transact on such important and critical data relevant to national security.

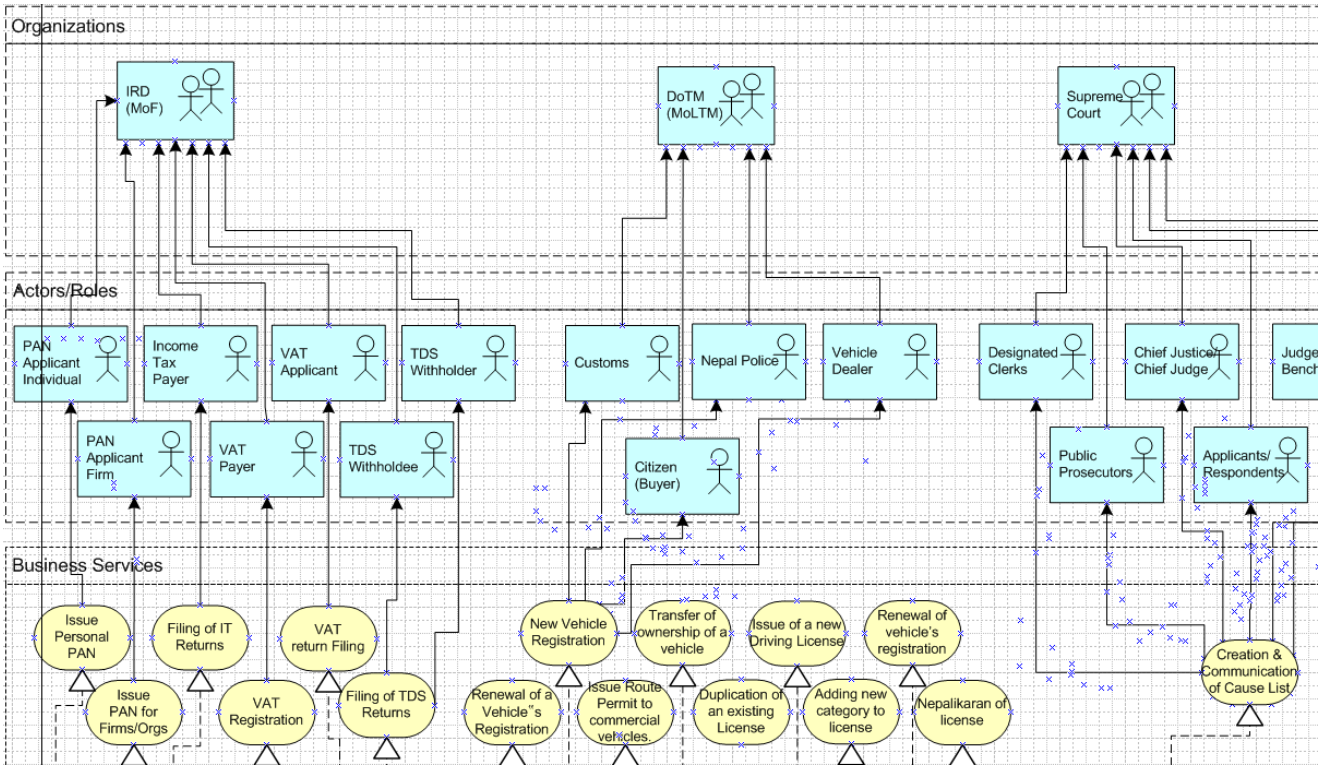
The Department of Posts is limited from the perspective of resource management, user management, and physical security. However, they have succeeded in implementing a variety of technologies relevant to various operations and have capacity and maturity to expand / integrate into a shared resource infrastructure.

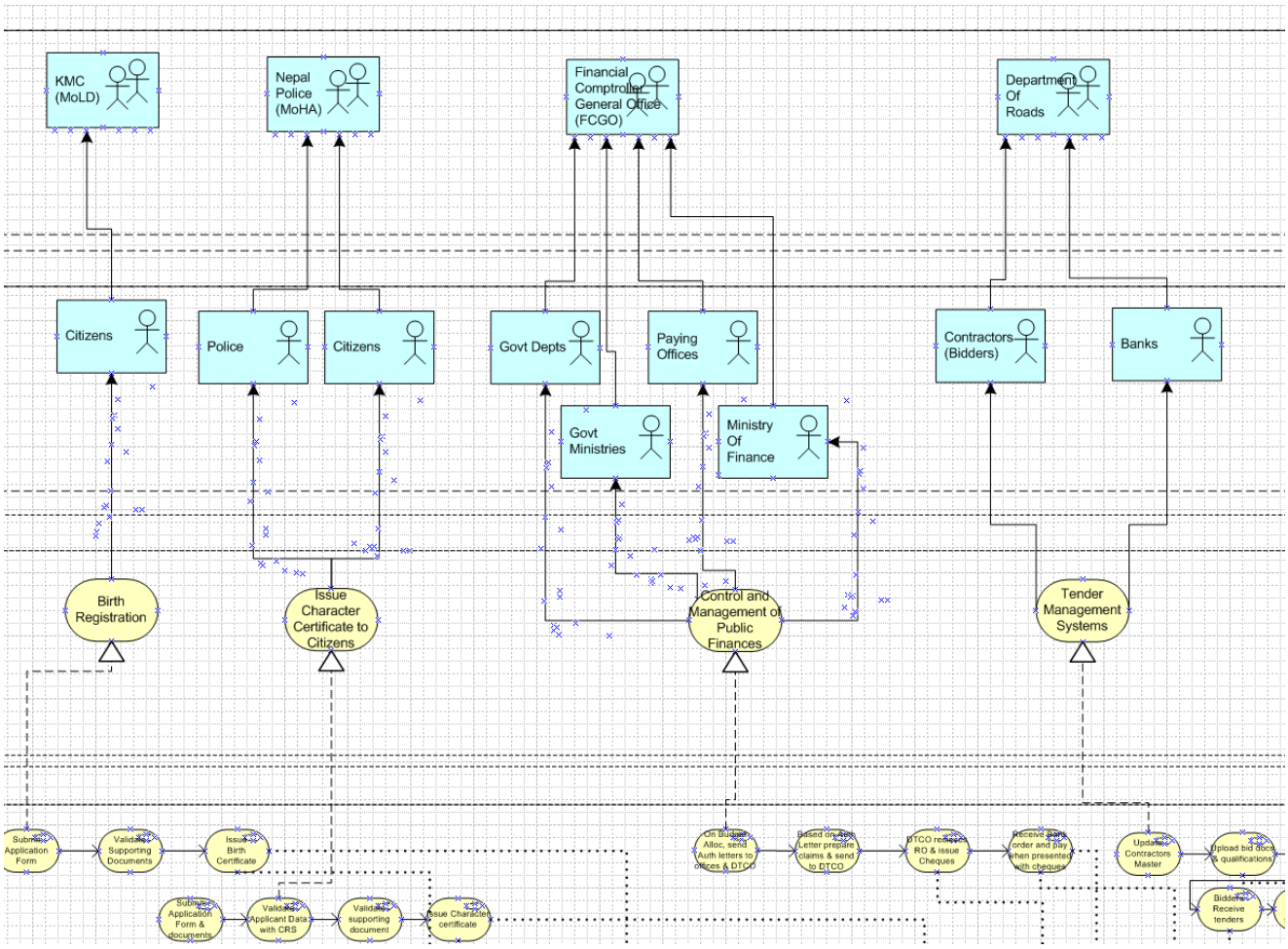
The Ministry of General Administration is strongly and securely connected to other ministries and departments within the Singh Durbar complex. There is infrastructure replication with Ministry of Finance to provide redundancy also. These are again relevant capacities that can be migrated into a shared resource infrastructure.

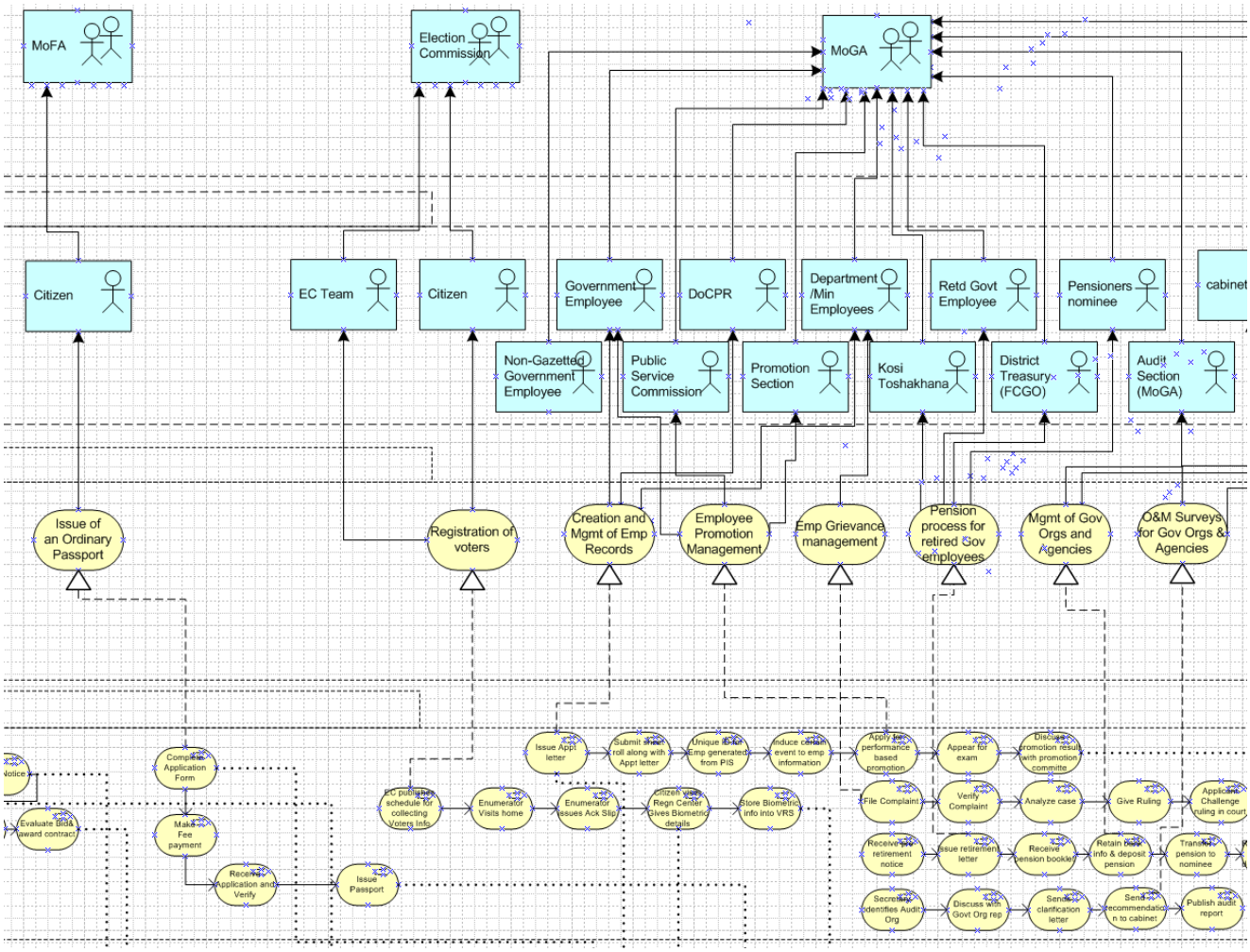
The other departments like Department of Roads and Department of Land Reforms and Management have operational infrastructure with a variety of components however, a significant number of these components are “end-of-life” and require up-gradation. Their IT capacity also needs to be enhanced in-terms of management tools and skill sets. These, thus become ideally suited to use the shared infrastructure instead of creating individual capacities for each of these departments.

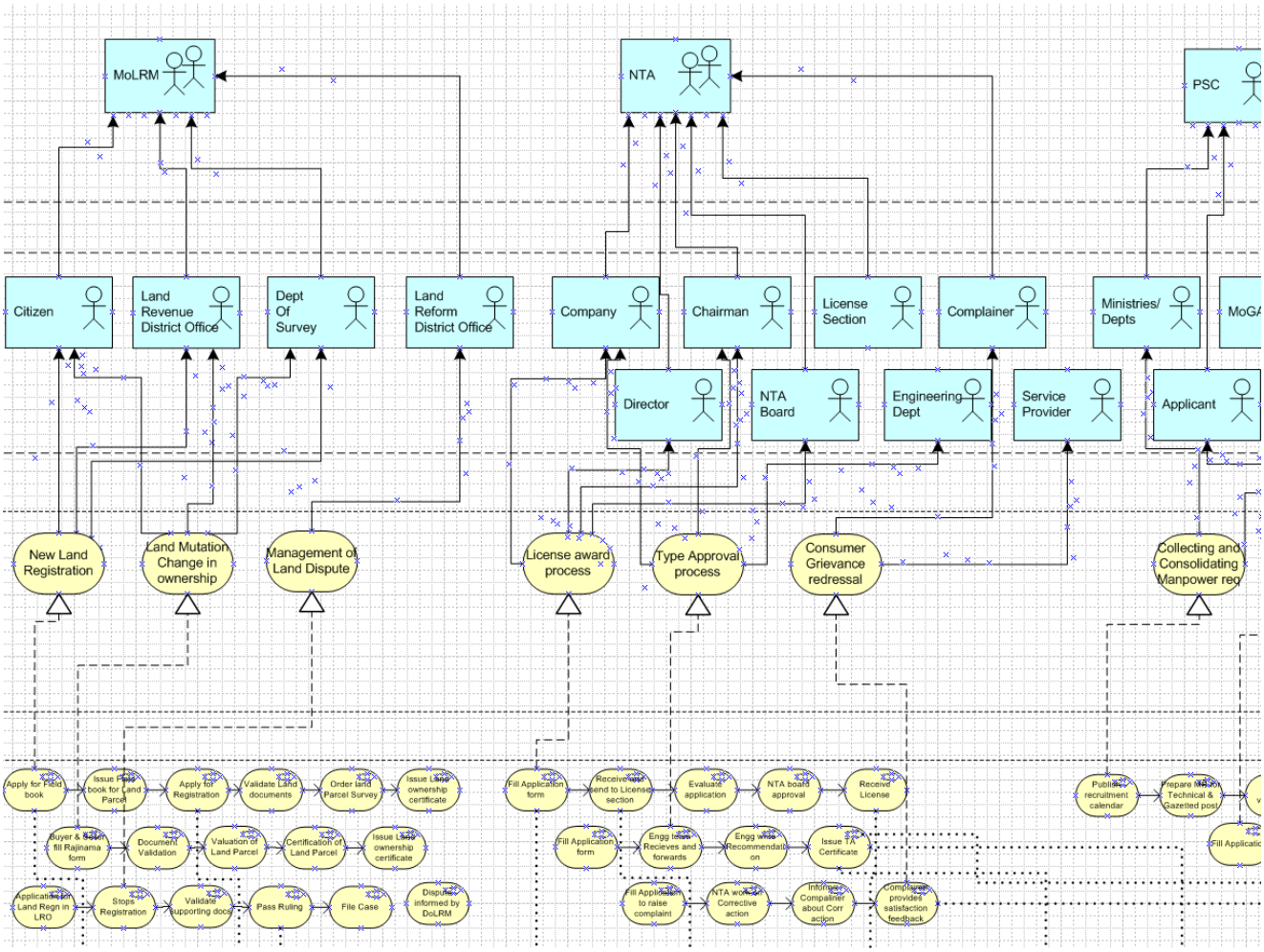
A very high level infrastructure diagram for the above three typical departments is provided in section 7.4.2 of this report.

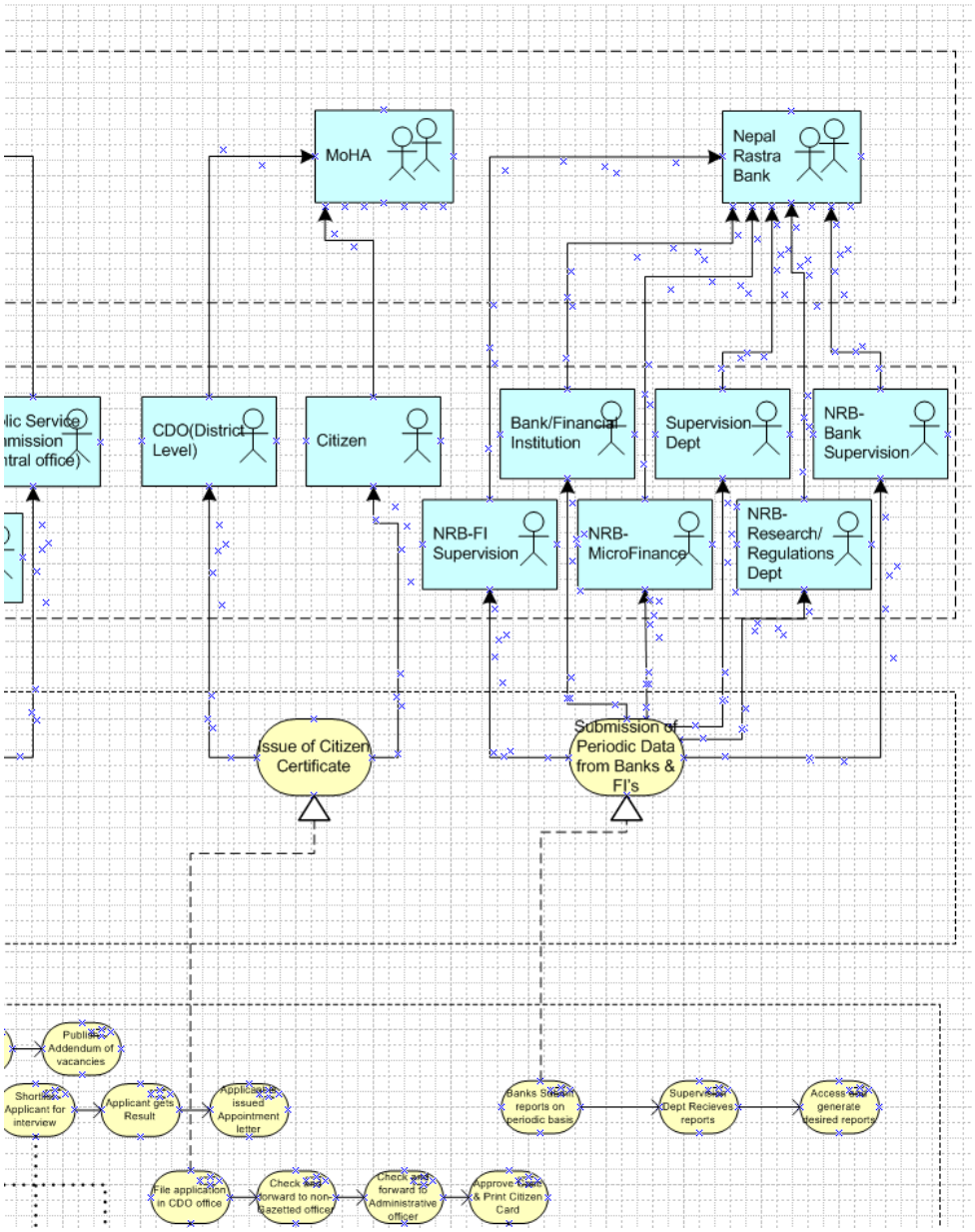
Target Business Architecture (vision) v0.1


Organizations
IRD (MoF)
DoTM (MoLTM)
Supreme Court
Actors/Roles
PAN Applicant Individual
Income Tax Payer
VAT Applicant
TDS Withholder
Customs
Nepal Police
Vehicle Dealer
Designated Clerks
Chief Justice/ Chief Judge
PAN Applicant Firm
VAT Payer
TDS Withholdee
Citizen (Buyer)
Public Prosecutors
Applicants/ Respondents
Business Services
Issue Personal PAN
Filing of IT Returns
VAT return Filing
New Vehicle Registration
Transfer of ownership of a vehicle
Issue of a new Driving License
Renewal of vehicle's registration
Creation & Communication of Cause List
Issue PAN for Firms/Orgs
VAT Registration
Filing of TDS Returns
Renewal of a Vehicle"s Registration
Issue Route Permit to commercial vehicles.
Duplication of an existing License
Adding new category to license
Nepalikaran of license

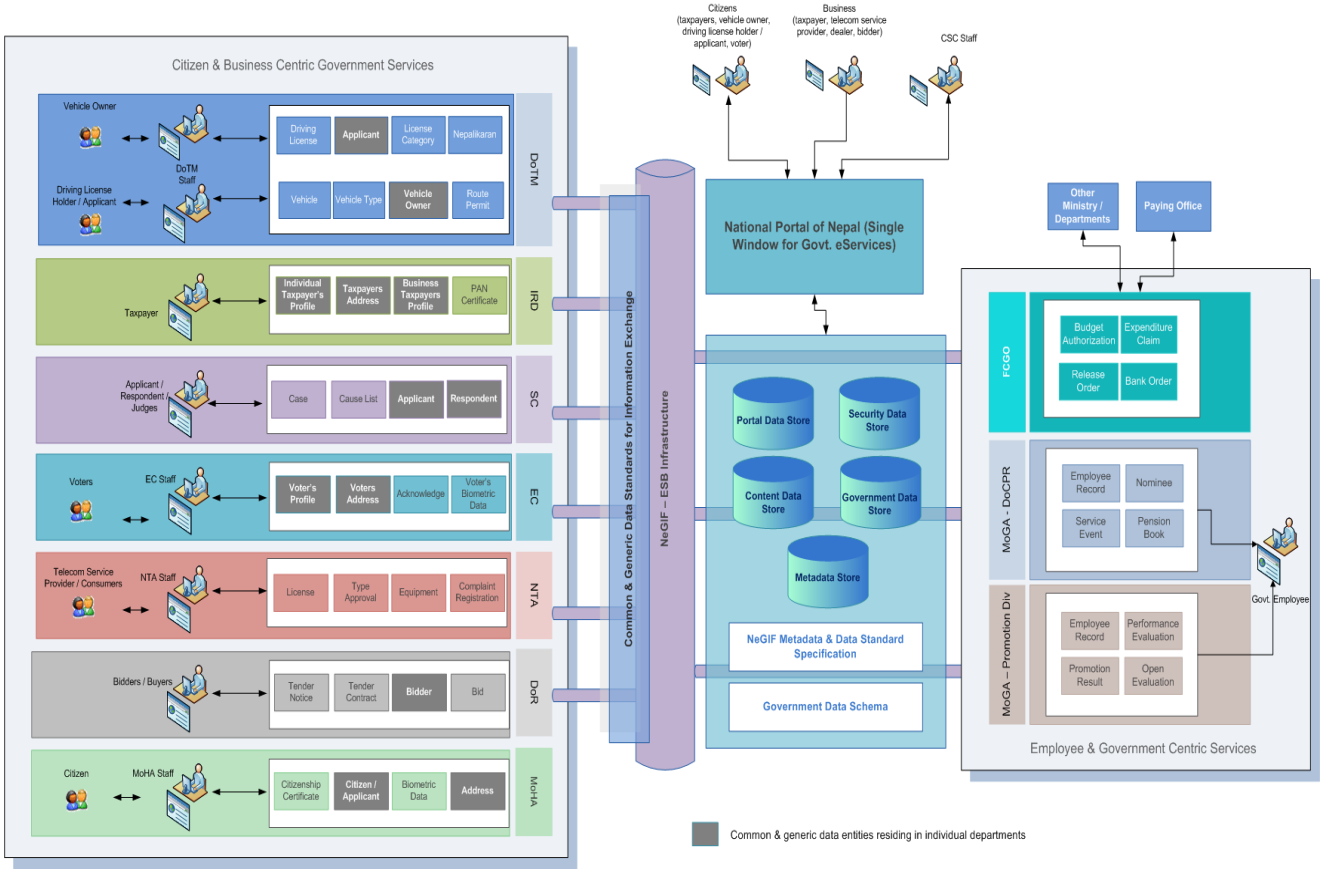

KMC (MoLD)
Nepal Police (MoHA)
Financial Comptroller General Office (FCGO)
Department Of Roads
Citizens
Police
Citizens
Govt Depts
Paying Offices
Contractors (Bidders)
Banks
Govt Ministries
Ministry Of Finance
Birth Registration
Issue Character Certificate to Citizens
Control and Management of Public Finances
Tender Management Systems


MoFA
Election Commission
MoGA
Citizen
EC Team
Citizen
Government Employee
DoCPR
Department /Min Employees
Retd Govt Employee
Pensioners nominee
cabinet
Non-Gazetted Government Employee
Public Service Commission
Promotion Section
Kosi Toshakhana
District Treasury (FCGO)
Audit Section (MoGA)
Issue of an Ordinary Passport
Registration of voters
Creation and Mgmt of Emp Records
Employee Promotion Management
Emp Grievance management
Pension process for retired Gov employees
Mgmt of Gov Orgs and Agencies
O&M Surveys for Gov Orgs & Agencies
Issue Appt letter
Submit draft roll along with Appt letter
Unique ID for Emp generated from PIS
Induce certain event to emp information
Apply for performance based promotion
Appear for exam
Discuss promotion result with promotion committe
Complete Application Form
EC publishes schedule for collecting Voters Info
Enumerator Visits home
Enumerator issues Ack Slip
Citizen visits Regn Center Gives Biometric details
Store Biometric info into VRS
File Complaint
Verify Complaint
Analyze case
Give Ruling
Make Fee payment
Receive Application and Verify
Issue Passport
Receive case retirement notice
Issue retirement letter
Receive pension booklet
Retain bank info & deposit pension
Transfer pension to nominee
Secretary identifies Audit Org
Discuss with Govt Org rep
Send clarification letter
Send recommendation to cabinet
Publish audit report

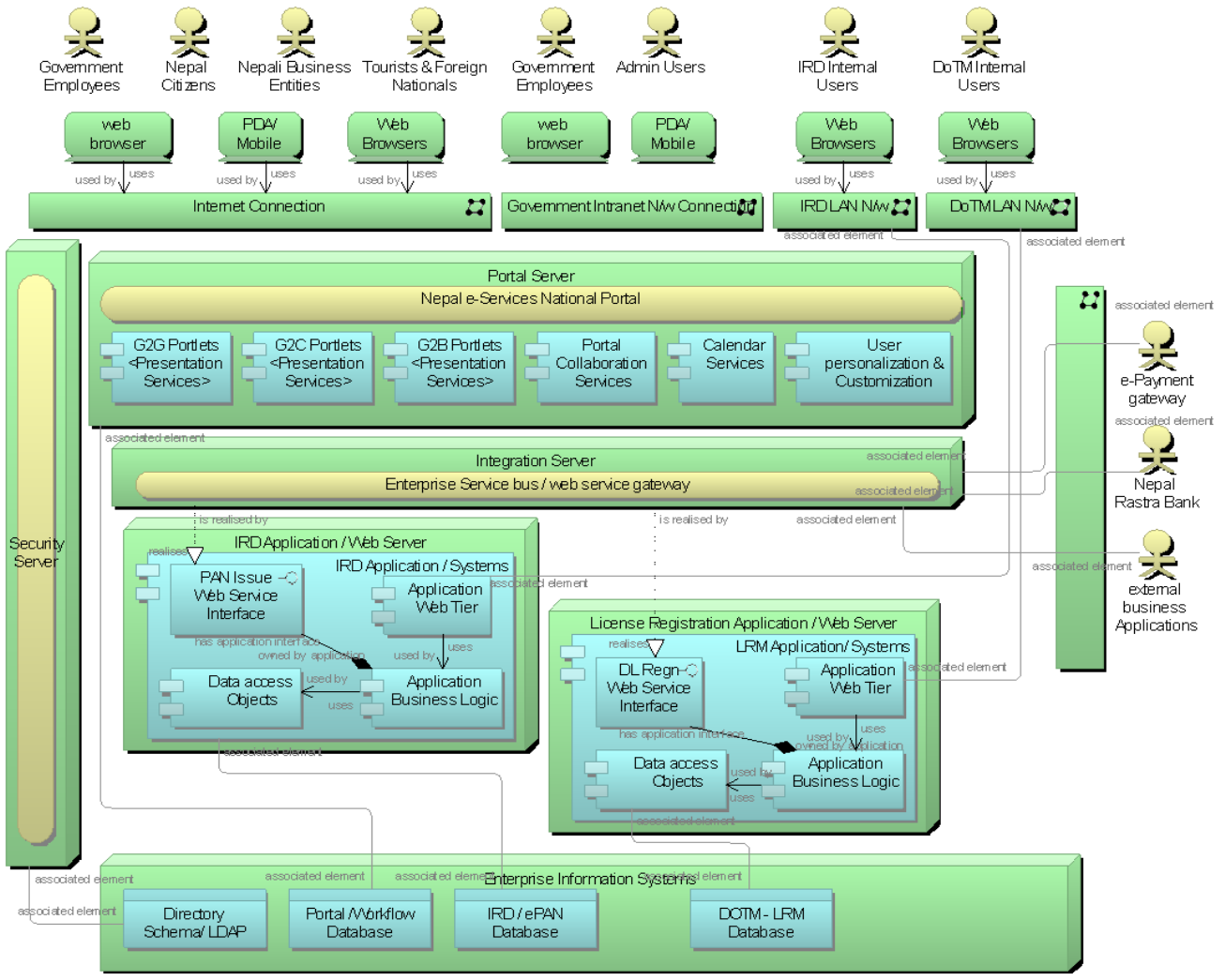

MoLRM
NTA
PSC
Citizen
Land Revenue District Office
Dept Of Survey
Land Reform District Office
Company
Chairman
License Section
Complainer
Ministries/ Depts
Director
NTA Board
Engineering Dept
Service Provider
Applicant
New Land Registration
Land Mutation Change in ownership
Management of Land Dispute
License award process
Type Approval process
Consumer Grievance redressal
Collecting and Consolidating Manpower req
Apply for Field book
Issue Field book for Land Parcel
Apply for Registration
Validate Land documents
Order land Parcel Survey
Issue Land ownership certificate
Buyer & Seller fill Rajinama form
Document Validation
Valuation of Land Parcel
Certification of Land Parcel
Issue Land ownership certificate
Application for Land Regn in LRO
Stops Registration
Validate supporting docs
Pass Ruling
File Case
Disputes informed by DoLRM
Fill Application form
Receive and send to License section
Evaluate application
NTA board approval
Receive License
Fill Application form
Engg team Recieves and forwards
Engg wins Recommendation
Issue TA Certificate
Fill Application to raise complaint
NTA work for Corrective action
Informed Compainer about Corr action
Complainer provides satisfaction feedback
Publish recruitment calendar
Prepare TA/DA Technical & Gazetted post



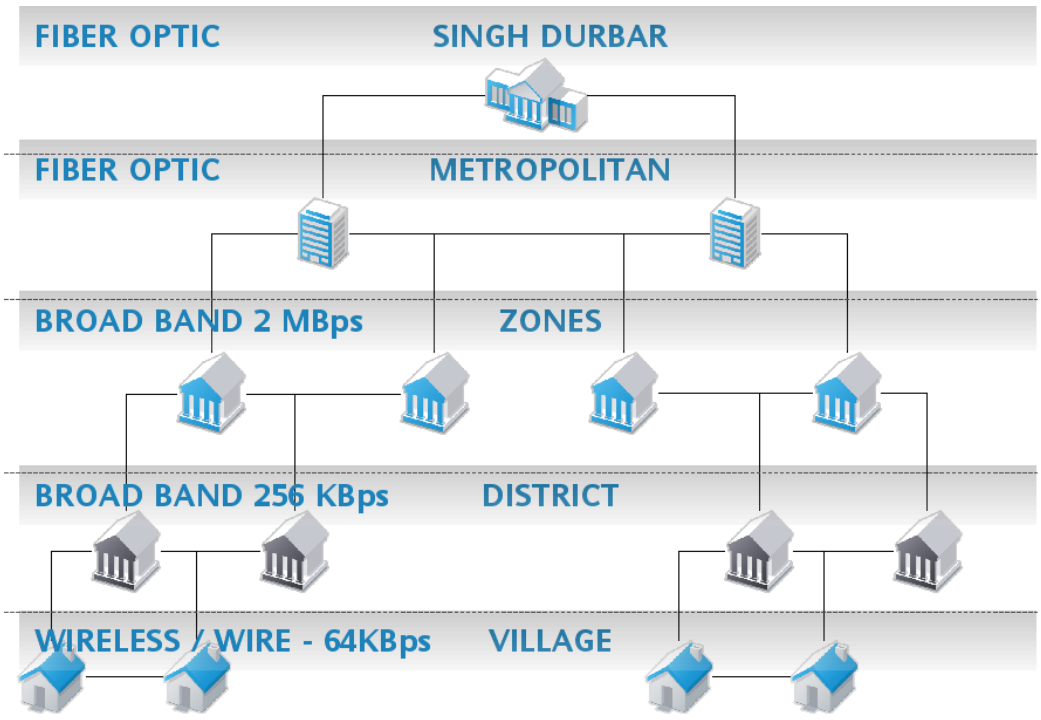
Target Data Architecture (vision) v0.1



Target Application Architecture (vision) v0.1



Target Technology Architecture (vision) v0.1

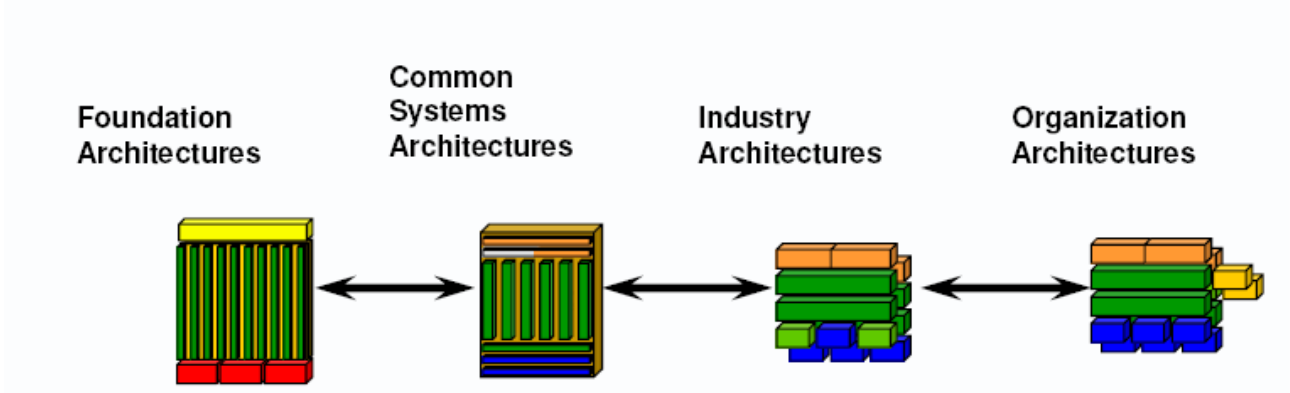


3.7 Enterprise Continuum

Enterprise Continuum is a categorization mechanism useful for classifying architecture and solution artefacts, both internal and external to the Architecture Repository, as they evolve from generic Foundation Architectures to Organization-Specific Architectures.

The following 4 architectures are part of an architecture continuum.

1. Foundation Architectures
2. Common System Architectures
3. Industry Architectures
4. Organisation Architectures



3.7.1 Foundation Architecture

A Foundation Architecture is

- An architecture of building blocks and corresponding standards
- Supports all the common systems architectures
- Supports the complete computing environment
- The Foundation Architecture contains many alternatives in each of the architecture building blocks

Following are the typical characteristics of Foundation architectures

Reflects general computing requirements

- Reflects general building blocks
- Defines technology standards for implementing these building blocks
- Provides direction for products and services
- Reflects the function of a complete, Repository robust computing environment that can be used as a foundation
- Provides open system standards, directions, and recommendations
- Reflects directions and strategies

The Foundation architecture for the Nepal GEA would be the technical reference model (TRM) for the governments embarking on the e-Gov initiatives and Standard Information base (SIB).

3.7.1.1 Technical Reference Model

The Technical Reference Model (TRM) is a component-driven, technical framework categorizing the standards and technologies to support and enable the delivery of Service Components and capabilities. It also unifies existing agency TRMs by providing a foundation to advance the re-use and standardization of technology and Service Components from a government-wide perspective.

Aligning agency capital investments to the TRM leverages a common, standardised vocabulary, allowing inter-department discovery, collaboration and interoperability. Nepal Government will benefit from economies of scale by identifying and re-using the best solutions and technologies to support their business functions, mission and target architecture.

Organised in a hierarchy, the TRM categorises the standards and technologies that collectively support the secure delivery, exchange and construction of business and application Service Components that may be used and leveraged in a component-based or service-oriented architecture (CBA or SOA, used synonymously from here forward). The TRM consists of:

- Service Areas - represent a technical tier supporting the secure construction, exchange, and delivery of Service Components. Each Service Area aggregates the standards and technologies into lower-level functional areas. Each Service Area consists of multiple Service Categories and Service Standards. This hierarchy provides the framework to group standards and technologies that directly support the Service Area.

- Service Categories - classify lower levels of technologies and standards with respect to the business or technology function they serve. In turn, each Service Category is comprised of one or more Service Standards.

- Service Standards - define the standards and technologies that support a Service Category. To support agency mapping into the TRM, many of the Service Standards provide illustrative specifications or technologies as examples.

A high-level outline of the TRM is shown in Figure below.

Service Access and Delivery			
Access Channels • Web browsers • Wireless/PDA • Collaboration/ Communication • Other Electronic Channels	**Delivery Channels** • Internet • Intranet • Extranet • Peer to Peer (P2P) • Virtual Private Network	**Service Requirements** • Legislative / Compliance • Authentication / Single Sign on • Hosting	**Service Transport** • Supporting Network Services

Service Platform and Infrastructure		
Support Platforms • Wireless / Mobile • Platform Independent • Platform Dependent **Software Engineering** • Integrated development environment • Software Configuration management • Modelling	**Delivery Servers** • Web servers • Media servers • Application servers • Portal server • Integration server • Enterprise service bus **Database / Storage** • Database • Storage	**Hardware / Infrastructure** • Servers / Computers • Embedded Technology devices • Peripherals • Wide Area Networks (WANs) • Local Area Networks (LANs) • Network Devices / Standards • Video conferencing

Component Framework			
Security • Certificates / Digital signatures • Supporting security services	**Presentation / Interface** • Static display • Dynamic server side display • Content rendering • Wireless / Mobile / Voice	**Business logic** • Platform Independent • Platform dependent **Data Interchange** • Data Exchange	**Data Management** • Database Connectivity • Reporting and Analysis

Service Interface and Integration		
Integration • Middleware	**Interoperability** • Data	**Interface** • Service discovery

• Enterprise Application Integration	format/Classification • Data types/ Validation • Data transformation	• Service Description/ Interface

3.7.1.2 Standards information base (SIB)

The Standards Information Base is structured according to the Service Categories in the Open Group Architecture Framework (TOGAF) Technical Reference Model:

- Data Interchange Services
- Data Management Services
- Graphics and Imaging Services
- International Operation Services
- Location and Directory Services
- Network Services
- Object-Oriented Provision of Services
- Operating System Services
- Security Services
- Software Engineering Services
- System and Network Management Services
- Transaction Processing Services
- User Interface Services
- Quality of Service

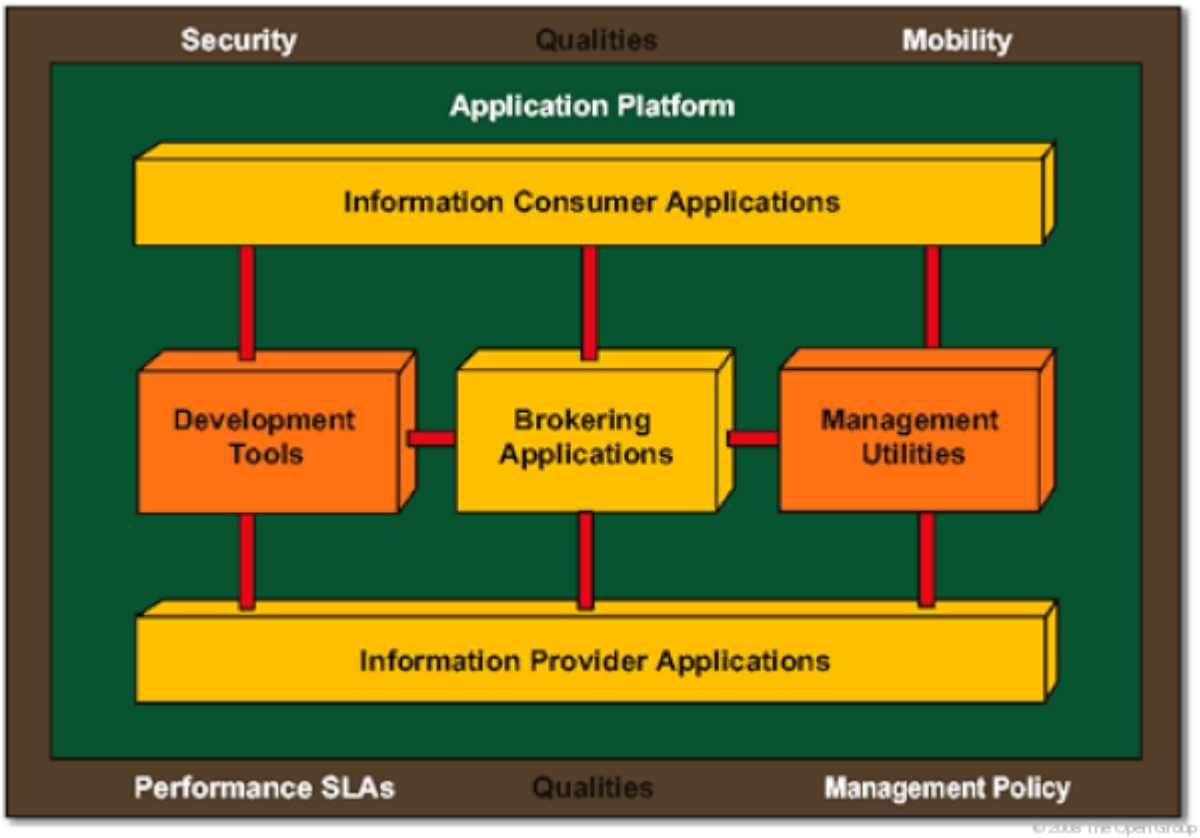
Reference: For detailed description of each element in the standards information base refer to the GEA Enterprise Architecture continuum and Architecture repository.

3.7.2 Common Systems Architecture

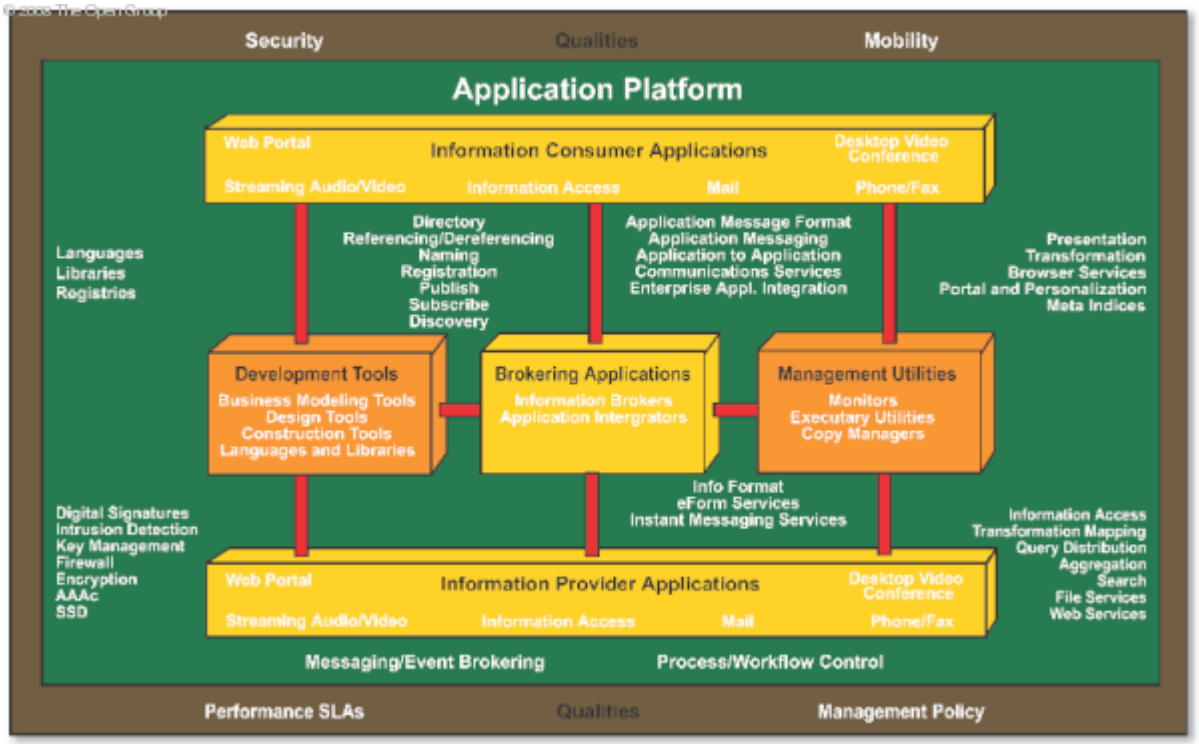
Common Systems Architecture guides the selection and integration of specific services from the Foundation Architecture and helps create architecture useful for building common and reusable solutions across a wide number of relevant domains.

Integrated Information Infrastructure Reference Model (III-RM) is a Common Systems Architecture that focuses on the vision of Boundary less Information Flow in the enterprise environments. This model also points to rules and standards to assist in leveraging solutions and products within the value chain.

The III-RM relates to and complements TRM. It also expands parts of the TRM, in particular, the business applications and infrastructure applications. It uses some of the services defined in the TRM.



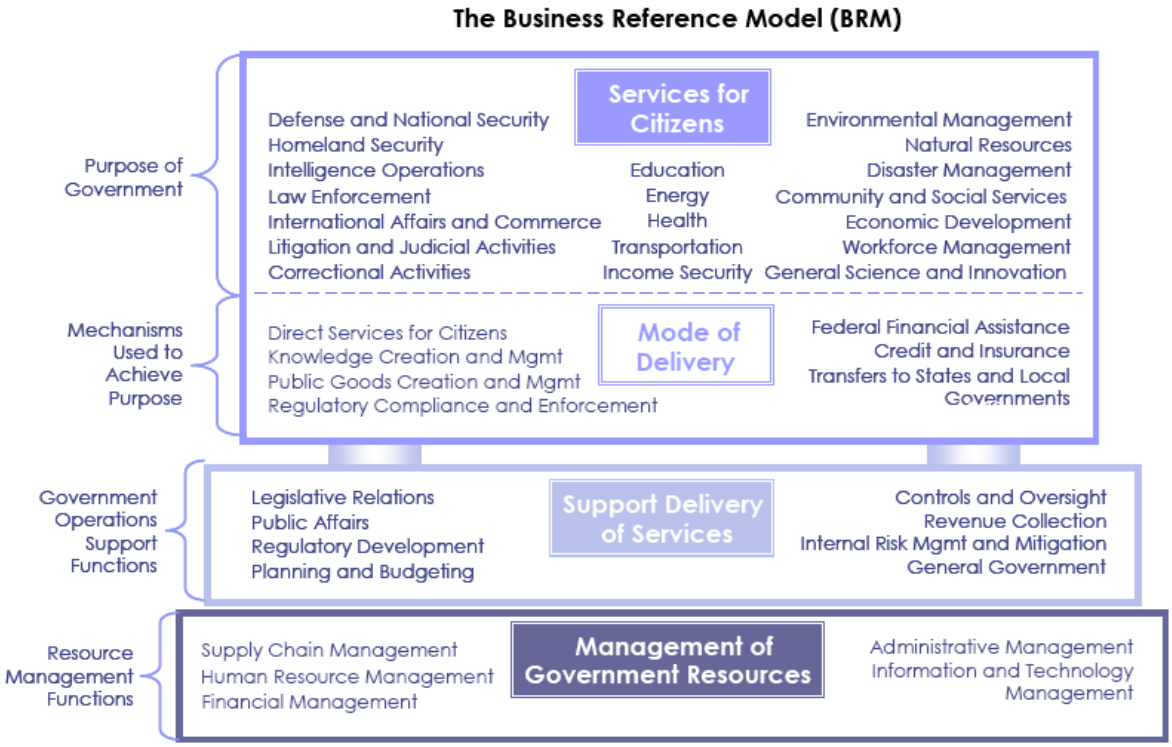
Detailed III-RM Taxonomy



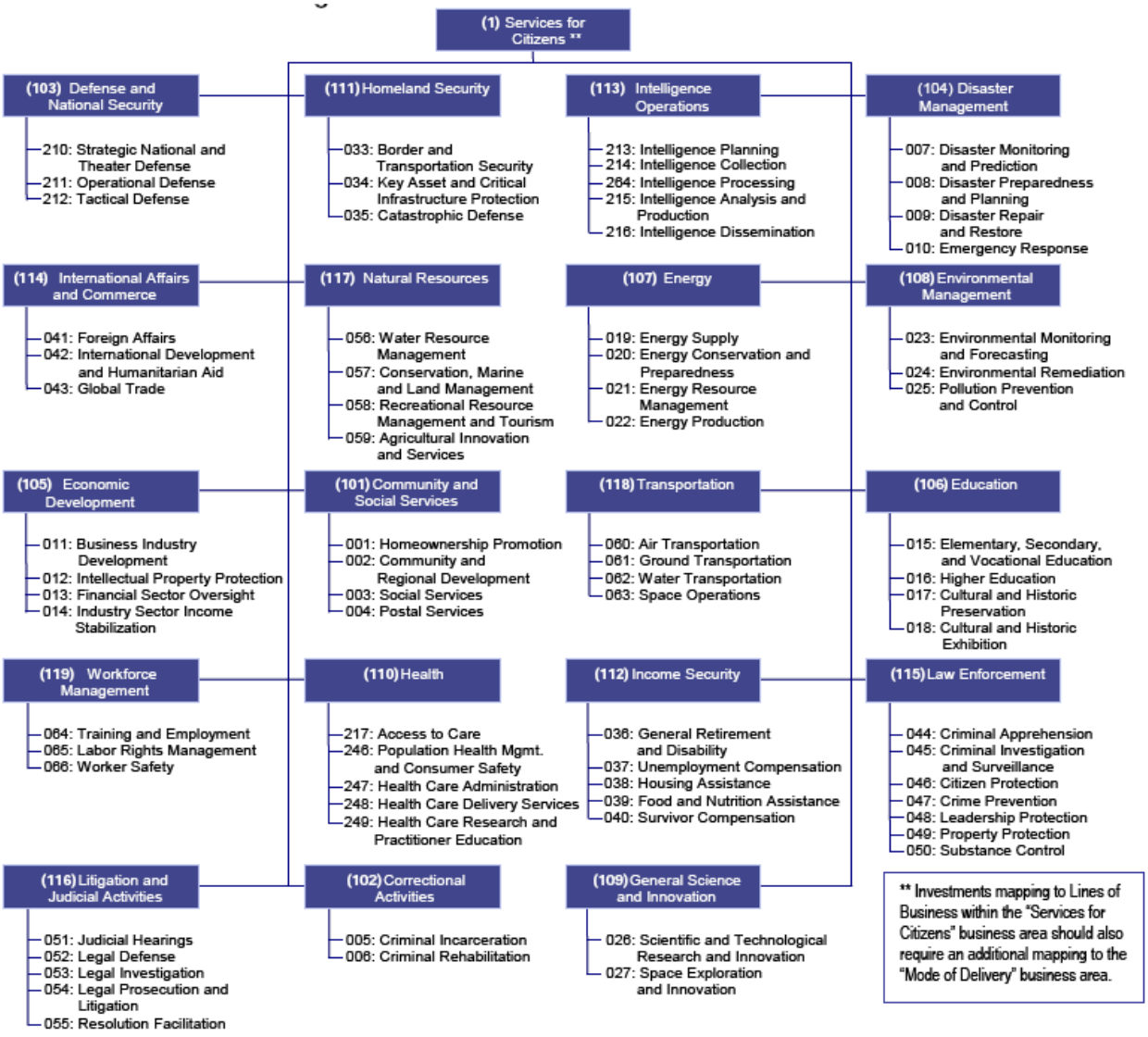
3.7.3 Industry Architectures

Industry Architectures guide the integration of common systems components with industry-specific components, and guide the creation of industry solutions for targeted organization problems within a particular industry.

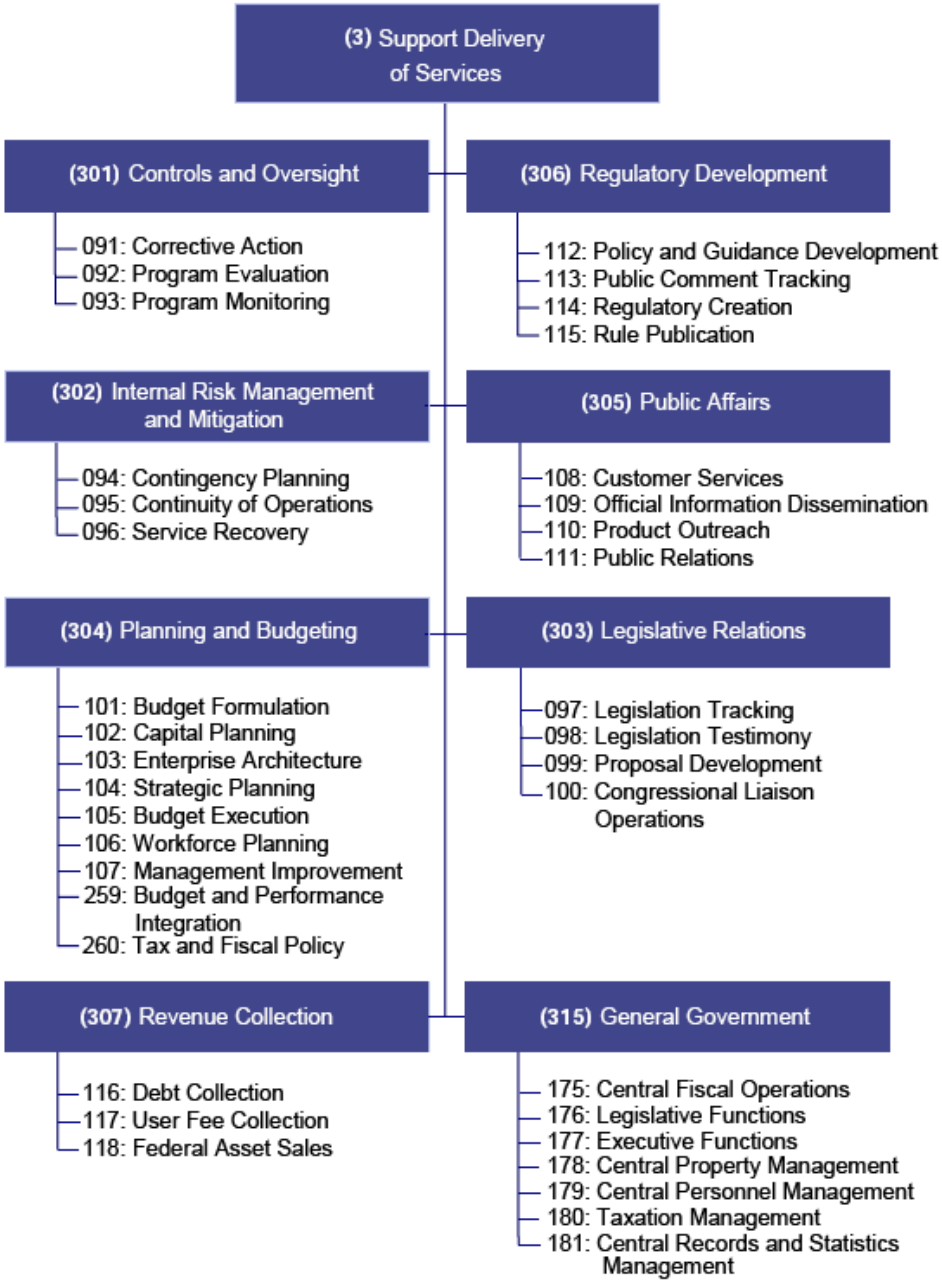
The typical business reference model for "Government" industry sector is illustrated below –



Services for Citizens - Some typical services for the "Services for the Citizens" business area of BRM for the "Government" sector is depicted below -

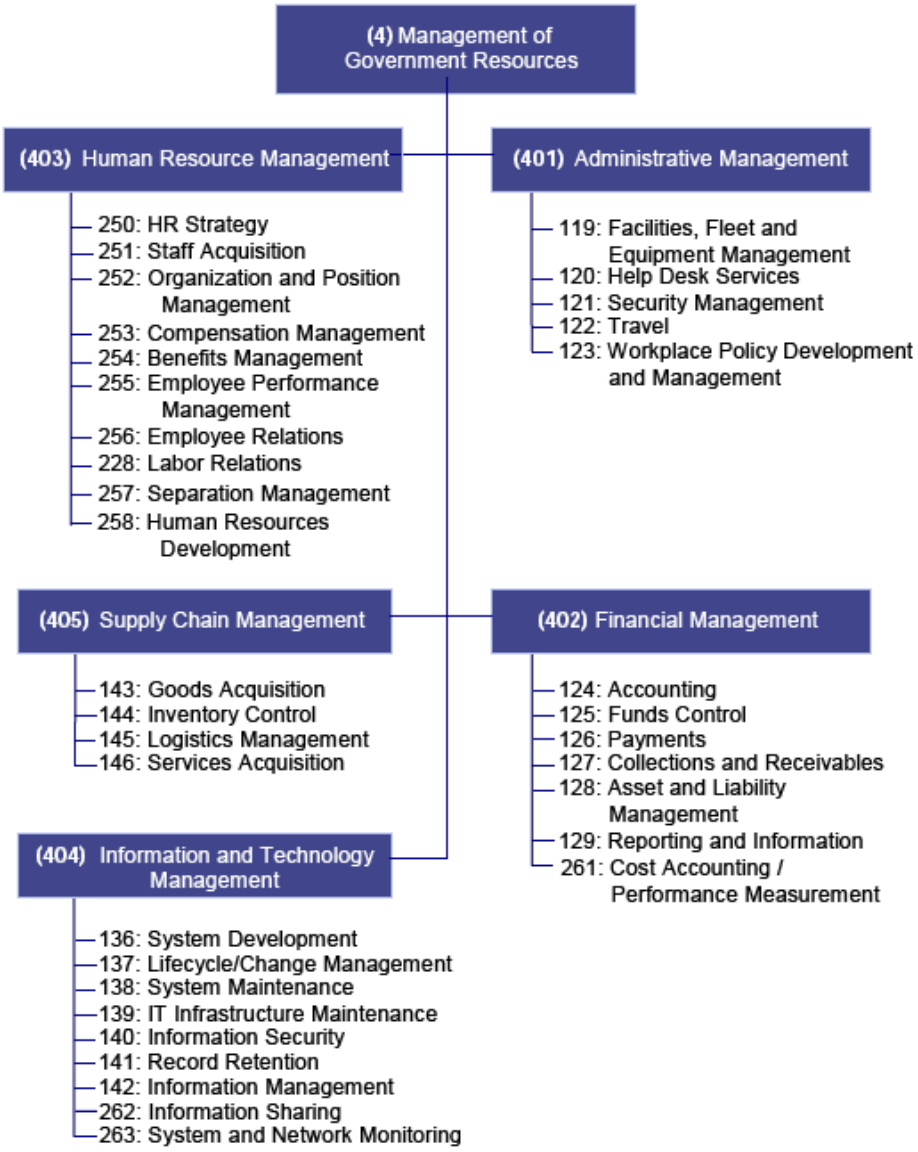


Support Delivery of Services - Some typical services for the "Support Delivery of Services" business area of BRM for the "Government" sector is depicted below -



Management of Govt. Resources - Some typical services for the "Management of Govt. Resources" business area of BRM for the "Government" sector is depicted below -

Figure 14: Management of Government Resources Business Area



3.7.4 Organization Architecture

Organization-Specific Architectures are the most relevant to the IT customer community, since they describe and guide the final deployment of solution components for a particular enterprise or extended network of connected enterprises.

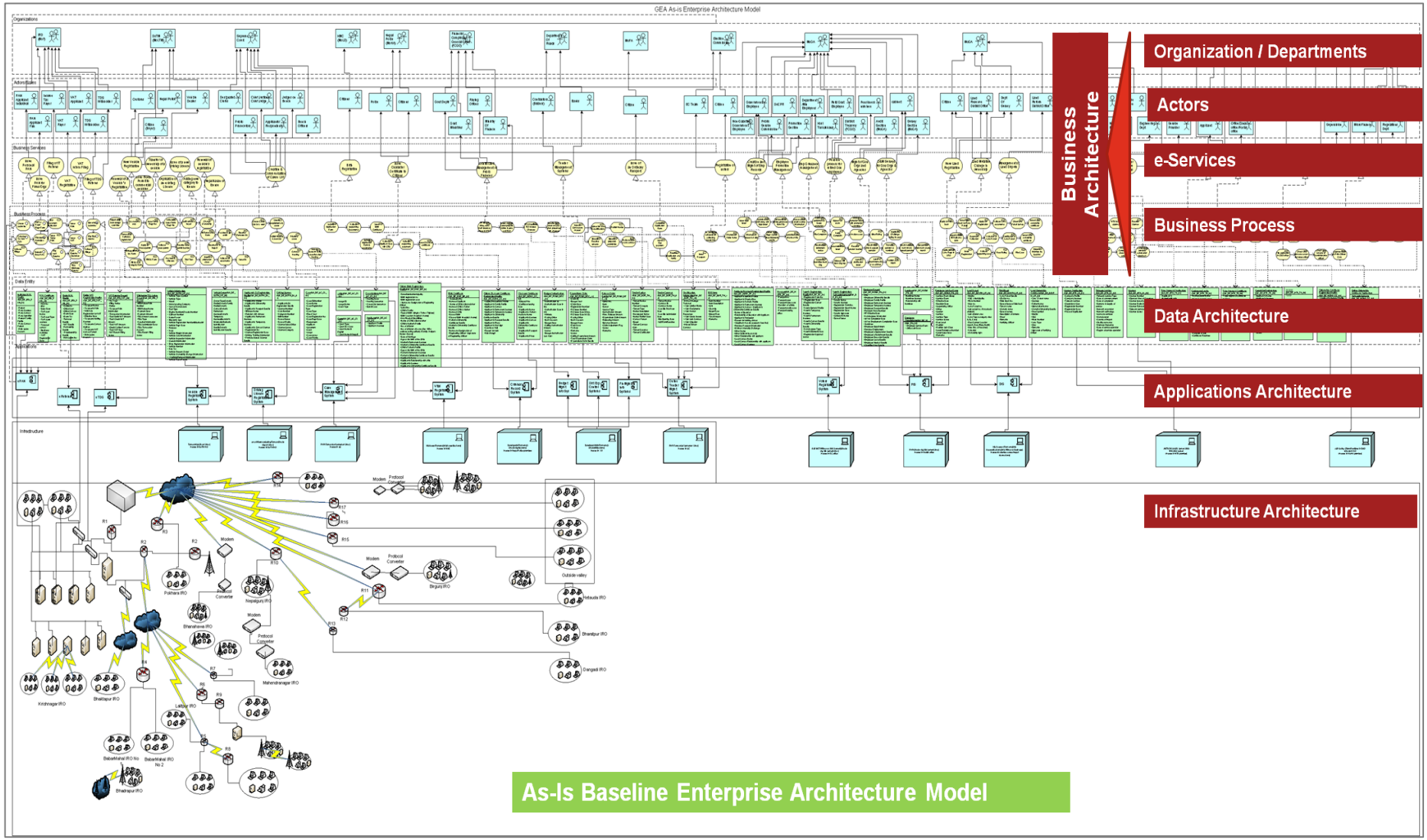
The Organization-Specific Architecture guides the final customization of the solution, and has the following characteristics:

- Provides a means to communicate and manage business operations across all four architectural domains
- Reflects requirements specific to a particular enterprise
- Defines building blocks specific to a particular enterprise
- Contains organization-specific business models, data, applications, and technologies

- Provides a means to encourage implementation of appropriate solutions to meet business needs
- Provides the criteria to measure and select appropriate products, solutions, and services
- Provides an evolutionary path to support growth and new business needs

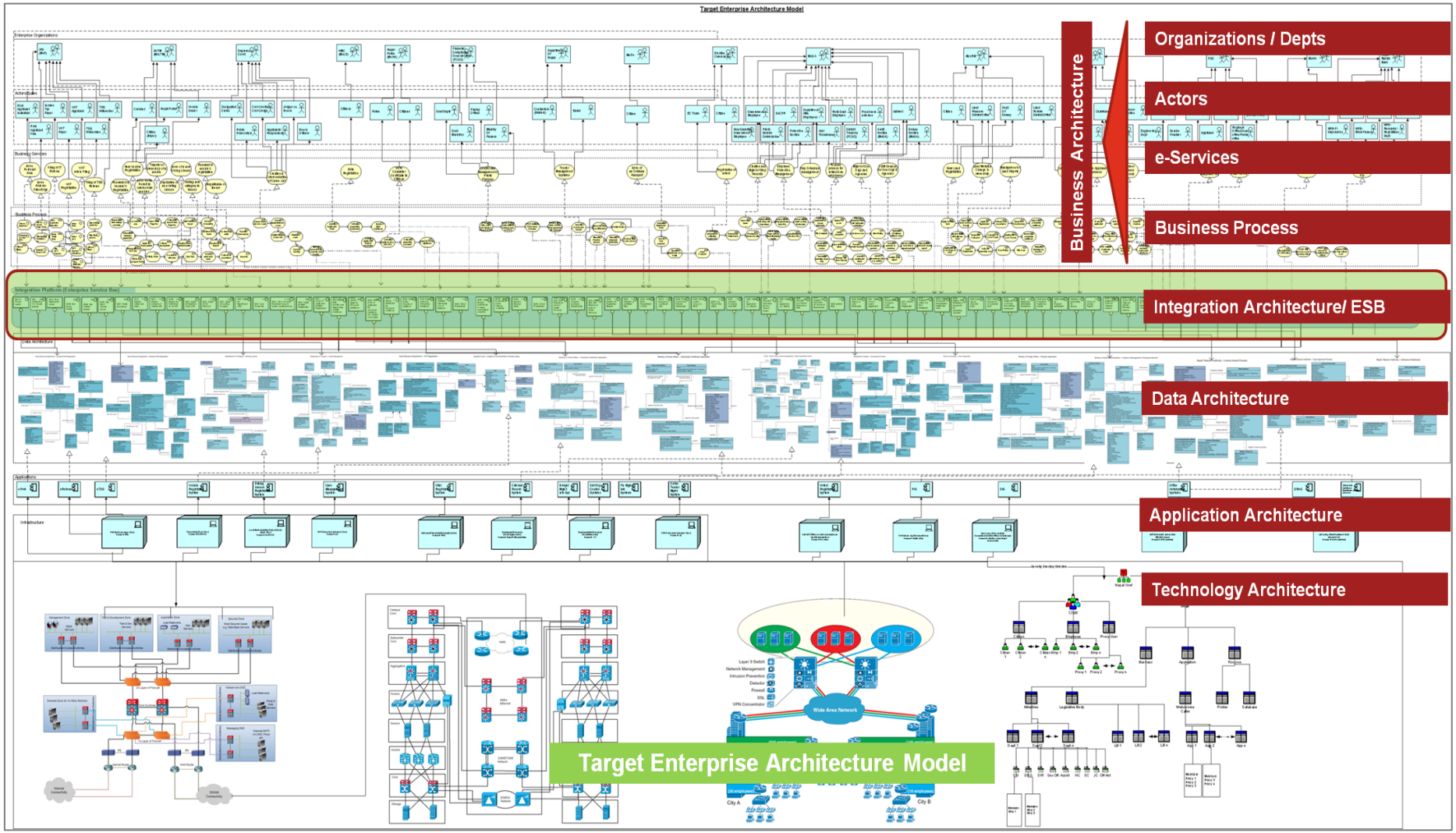
3.7.4.1 AS-IS Nepal Govt. Enterprise/Organization Architecture

The AS-IS Organization Architecture at an enterprise level for Govt. of Nepal is depicted below -


GEA As-is Enterprise Architecture Model
Business Architecture
Organization / Departments
Actors
e-Services
Business Process
Data Architecture
Applications Architecture
Infrastructure Architecture
As-Is Baseline Enterprise Architecture Model

3.7.4.2 TO-BE Nepal Govt. Enterprise/Organization Architecture

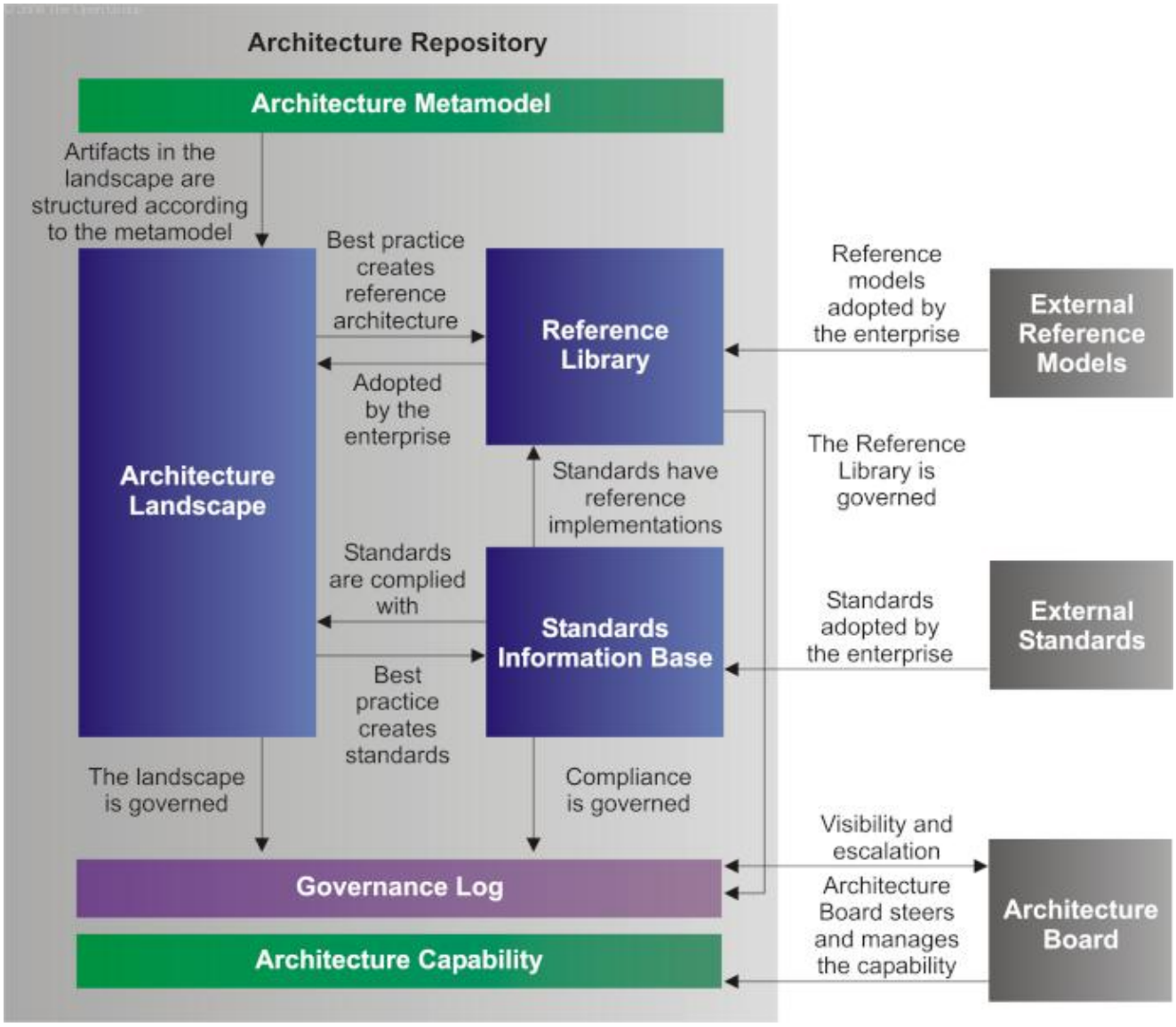
The recommended TO-BE Organization Architecture at an enterprise level for Govt. of Nepal is depicted below -


Target Enterprise Architecture Model
Business Architecture
Organizations / Depts
Actors
e-Services
Business Process
Integration Architecture/ ESB
Data Architecture
Application Architecture
Technology Architecture
Target Enterprise Architecture Model

3.8 Architecture Repository

Architecture repository is a system that manages all of the data of an enterprise, including data and process models and other enterprise information. It allows an enterprise to distinguish between different types of architectural assets that exist at different levels of abstraction in the organization.

It is a part of the wider Enterprise IT Repository which provides the capability to link architectural assets to components of the Detailed Design, Deployment, and Service Management Repositories.



The Six classes of architectural information in the repository are

1. Architecture Meta-Model - The Architecture Metamodel describes the organizationally tailored application of an architecture framework, including a method for architecture development and a metamodel for architecture content

2. Architecture Capability - The Architecture Capability defines the parameters, structures, and processes that support governance of the Architecture Repository.

3. Architecture Landscape - The Architecture Landscape shows an architectural view of the building blocks that are in use within the organization today (e.g., a list of the live applications). The landscape is likely to exist at multiple levels of granularity to suit different architecture objectives
    - Strategic Architecture
    - Segment Architecture
    - Capability Architecture

4. Standards Information Base - The Standards Information Base captures the standards with which new architectures must comply, which may include industry standards, selected products and services from suppliers, or shared services already deployed within the organization. Three classes are
    - Legal and Regulatory Obligations
    - Industry Standards
    - Organizational Standards

    The Open Group has a public database of open industry standards with links to conformant products

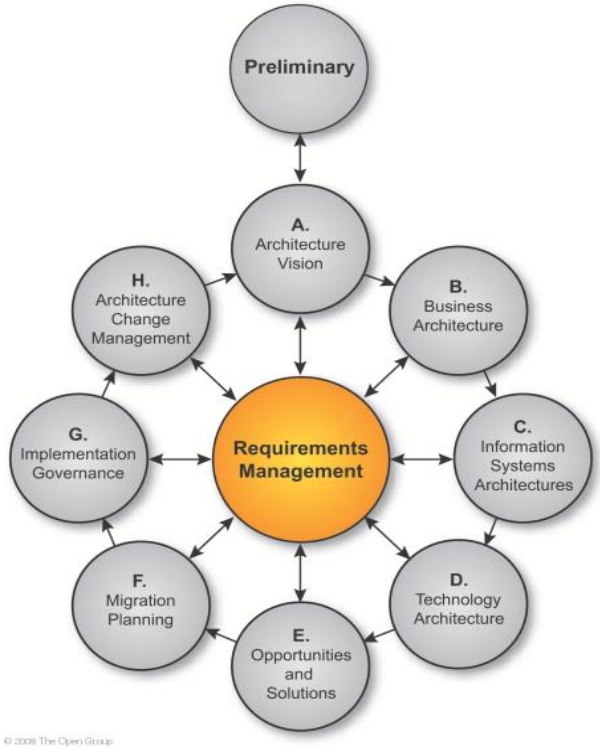
    Available for web enabled access http://www.opengroup.org/sib.htm

5. Reference Library - The Reference Library provides guidelines, templates, patterns, and other forms of reference material that can be leveraged in order to accelerate the creation of new architectures for the enterprise Can use the Architecture Continuum as method for classification

6. Governance Log - The Governance Log provides a record of governance activity across the enterprise
    - Decision Log
    - Compliance Assessments
    - Capability Assessments
    - Calendar
    - Project Portfolio
    - Performance Measurement

4. TOGAF ADM Phase – Requirements Management

4. Requirements Management



Phase Overview

Government Enterprise Architecture (EA) should be based on n-tier architecture, enabling a Service Oriented Architecture (SOA). Frameworks need to be developed for the following requirements, which will be applied for all government e-Service applications and to allow access to the government e-service platform. Any other additional recommendations are considered.

Software Services will be implemented in compliance with Web Services standard and XML based data exchange to guarantee their interoperability.

This high-level design fulfils application requirements for Government Intranet and G2C, G2B services. It should be extended later to other intranets (Education, Health and other sectors of Government) without major amendments.

4.1 Functional View

The functional view of Enterprise Application Architecture should show the major functional domains of the system and major dataflow.

The Enterprise Framework is split in 3 major domains:

- Application Infrastructure: this domain covers general purpose and administration applications and services that are not directly accessible by common users, but by Data Center Enterprise Architecture experts and implementing agency Administrators.
- Government Intranet: this domain covers all services and applications available to government staff through the G2G portal: email management, groupware tools, and any ministry service or application made available through portal.
- Government Websites: this domain covers all services and applications available to individuals or business employees through G2C and G2B portals. These services or applications could be hosted on Data Center Servers or on Ministry servers. In later case, integration of services to portals could be implemented at HTML level or at XML level. HTML integration is the simplest way. It means HTML code generated by Ministry web server is encapsulated in some portal container to be displayed without layout or graphical transformation. XML integration is done through Web Services, allowing full graphical and business integration in portal pages.
- Specified Ministry should be covered by a domain holding all applications hosted by ministry. These domains are not considered part of the Enterprise Architecture Framework, but are external domains to the Project. All work to be done within a ministry domain related to Enterprise Architecture

Framework Integration will be undertaken by related ministry, except for on-line services explicitly listed in Application requirements that will be developed within Project.

- Nepal Rastra Bank (NRB) or any authorized private, public or any other agency for e-payment who holds the future e-Payment system Gateway, should also be considered as an external domain to the Project.
- The Implementation view should show the main software components that constitute the Enterprise Architecture Application Framework and their technical implementation.
- All the components will be implemented on machines hosted in Data Center premises, according to Government Network design and communication services Specification.

Each machine identified in following diagram is a logical machine. A logical machine can be implemented as one or many servers with same software configuration but with some difference in hardware configuration.

Government Web Server should be the front-end of G2B and G2C portals. It hosts the HTTP server handling HTTP requests from and HTTP responses to Internet users. It hosts also portal integration features enabling encapsulation of HTML pages and integration of Web Services.

Government Intranet Server should have a similar role towards Government Intranet users.

Government Internet Gateway should host a proxy server with caching and IP address filtering features. It controls access rights of Intranet users to websites.

Government Application Server should run the business logic of all government wide applications and their data representation:

- Government Data Scheme Management
- Content and Document Management
- E-Mail System
- Groupware Tools

Government Application Server should also run the business logic of any G2G/G2C/G2B service or application hosted by Data Center.

Government Infrastructure Server should run a set of framework services:

- Authentication and Security Management
- Data Integration Services
- E-Payment Gateway

Government Infrastructure Server should also host all Operations and Administration applications.

Government Data Server should hosts all databases required for Application Framework.

Government Intranet Server, Government Web Server and Government Internet Gateway should be installed in a Demilitarized Zone (DMZ) and protected from Internet Users attacks by firewalls.

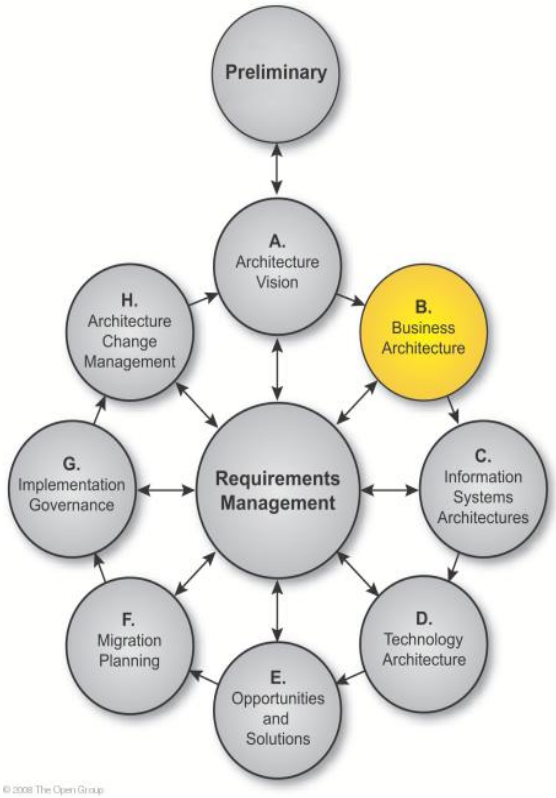
Government Application Server, Government Infrastructure Server and Government Data Server should be isolated and protected from DMZ by another firewall.

Any Service hosted by a ministry should be made available on any portal through a Web Service to be hosted on Ministry server.

Telecenters Users should have access to G2C and G2B portals through the Intranet Network.

5. TOGAF ADM Phase B - Business Architecture

5. Phase B: Business Architecture



Phase Overview

The Business Architecture identifies the business functions, processes, organization, and information flow for accomplishing the mission of a Nepal's eGovernment initiative. E-Gov solutions often involve business solutions that cross traditional functional or organizational boundaries - both within and across government organizations & agencies, and with outside constituencies such as citizens and business. Each ministry has its own service delivery model which is a mix of manual and electronic. However these services exist as silos due to lack of national integrated service delivery platform. As part of the future state business architecture recommendation, an integrated business model for service delivery was recommended.

The key principles behind the future state business architecture were –

- Service enablement across lifecycle events
- Integrated services across ministries / departments
- Single touch point for users to receive the services
- Services to be re-engineered and developed with internal workflow.

The Business Architecture identifies the business functions, processes, organization, and information flow for accomplishing the mission of a Nepal's eGovernment initiative. E-Gov solutions often involve business solutions that cross traditional functional or organizational boundaries - both within and across government organizations & agencies, and with outside constituencies such as citizens and business. Each ministry has its own service delivery model which is a mix of manual and electronic. However these services exist as silos due to lack of national integrated service delivery platform. As part of the future state business architecture recommendation, an integrated business model for service delivery was recommended.

To capture the high level Business Architecture for Government of Nepal GEA e-Services provided to the Citizens and within Governmental departments/ Ministries PwC conducted the following activities at an high level –

- Current state assessment of the short listed government services
- Perform gap analysis by benchmarking against leading best practices
- Recommend process re-design considerations for BPR

The key principles behind the future state business architecture were –

- Service enablement across lifecycle events
- Integrated services across ministries / departments
- Single touch point for users to receive the services
- Services to be re-engineered and developed with internal workflow.

As part of developing the business architecture for NGEA, PwC adopted the following approach for current state assessment and identifying the future state design considerations –

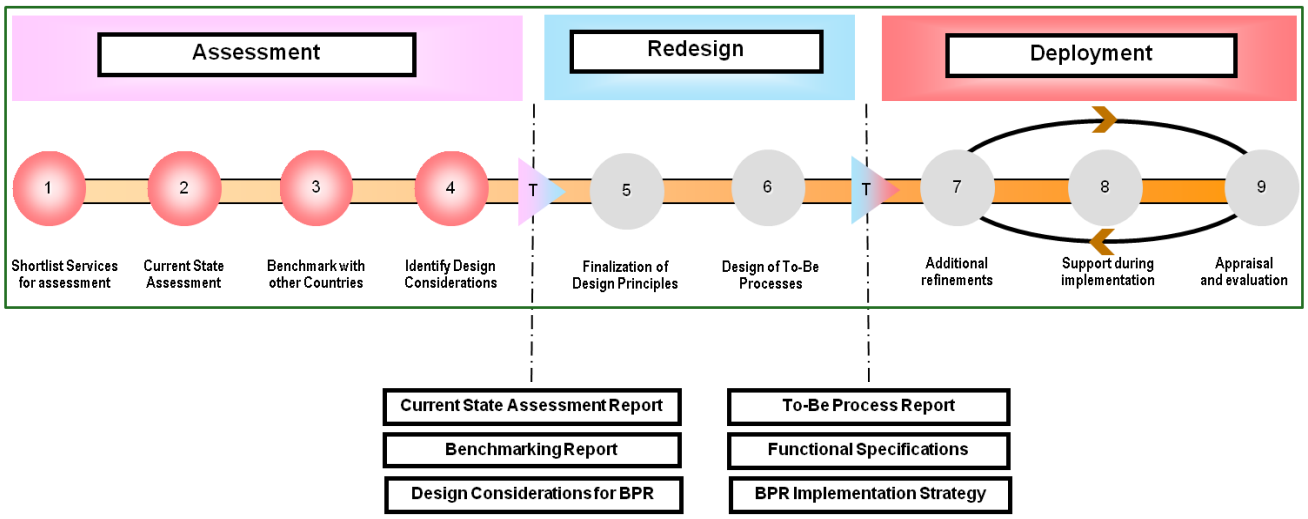


Figure: Overall Approach for Business Service Assessment & BPR

Current State Assessment

The approach adopted to arrive at the current state assessment of short-listed government services is shown below:

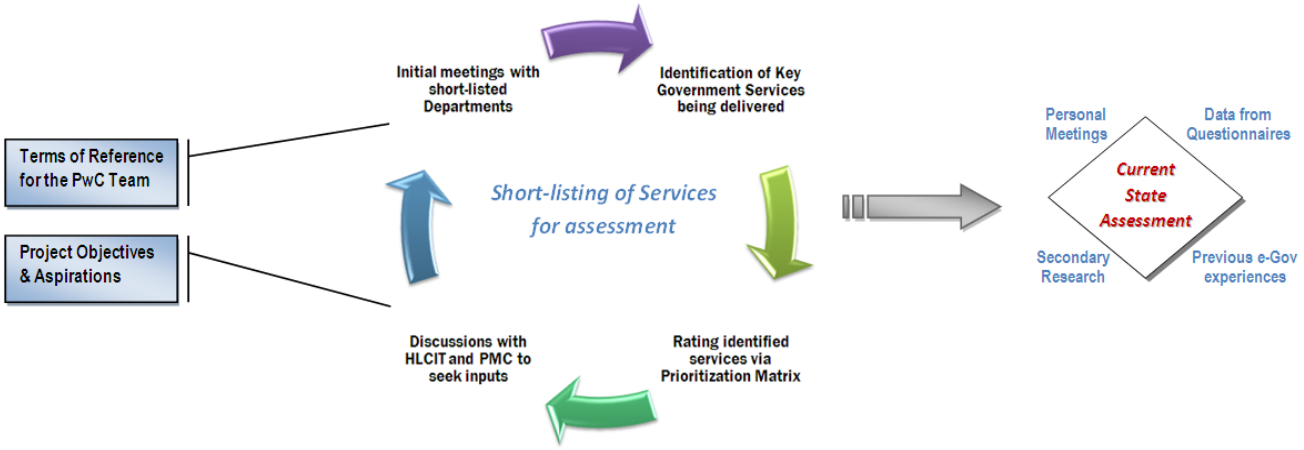


Figure: Approach for Current State Business Service Assessment

The end-result of these 4 tasks was the current state assessment of the final list of Government Services that were an appropriate mix of Citizen-facing Services (G2C), Business-facing Services (G2G) and Government-facing Services (G2G). Approximately 43 G2C, G2G and G2B Services were covered across 16 Ministries / Departments. The Current State Assessment done via Personal Meetings, Questionnaires and Secondary Research.

Design Considerations

The approach adopted to arrive at the design principles of short-listed government services is shown below:

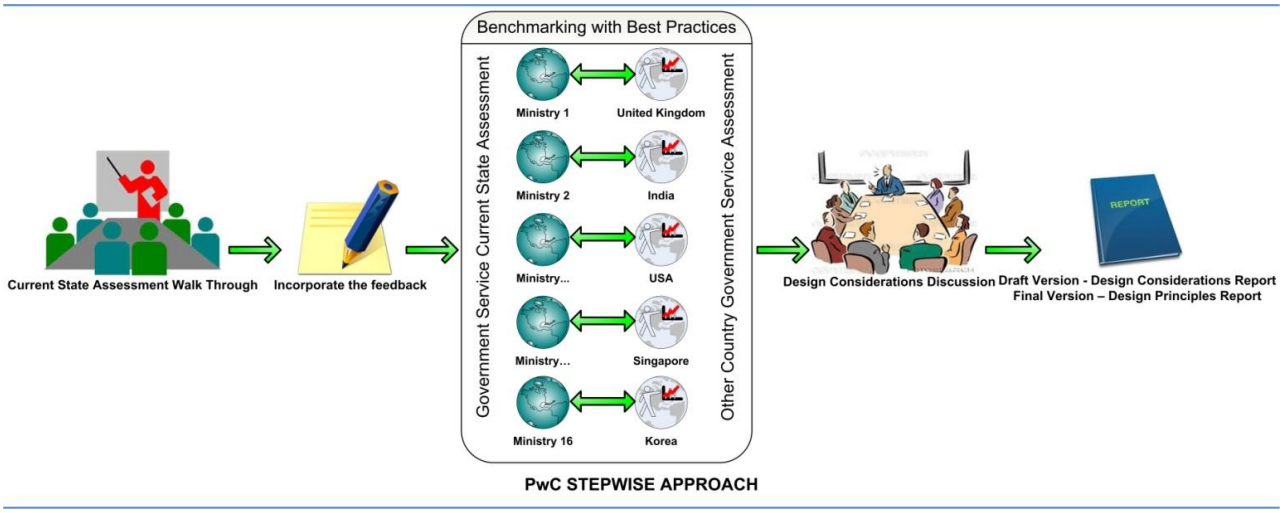


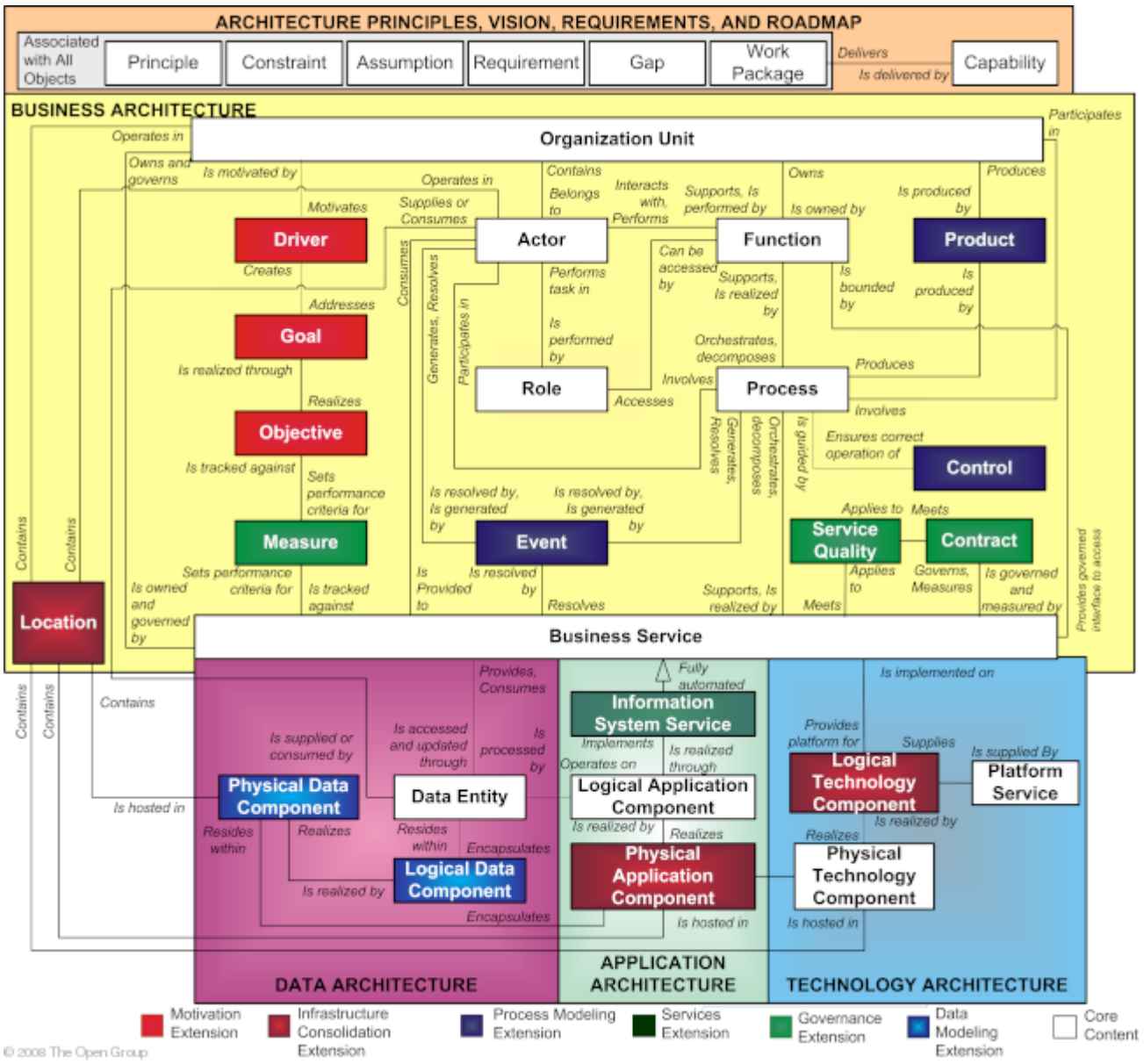
Figure Approach for Design Consideration Recommendation

After the submission of the current state assessment report, PwC team began their Current State Assessment Walk through with all 16 Government Agencies, to get it verified. Walkthrough results in creating the awareness among the Government Personnel and bridge the GAP of their process understanding.

After verification PwC conducted the benchmarking of Shortlisted Government Services with other relevant countries like India, United Kingdom, United States of America, Singapore, South Korea, etc and study the relevant best practices. Parallel to this activity PwC Team had discussion with consumers of these Government Services, like Citizen applying for Driving License, Vehicle Registration, Citizenship Certificate, Land Mutation, New Land Registration, New Passport, Government job, Retired Government employee applying for Pension Book, etc.

Benchmarking and Consumers feedback Analysis result in Design Considerations for the BPR. PwC Team formulates those Considerations as To-Be Recommendations or Design Considerations and shared with all 16 Government Agencies.

5.1 Meta Model Context – Reference Model



5.2 Baseline Business Architecture

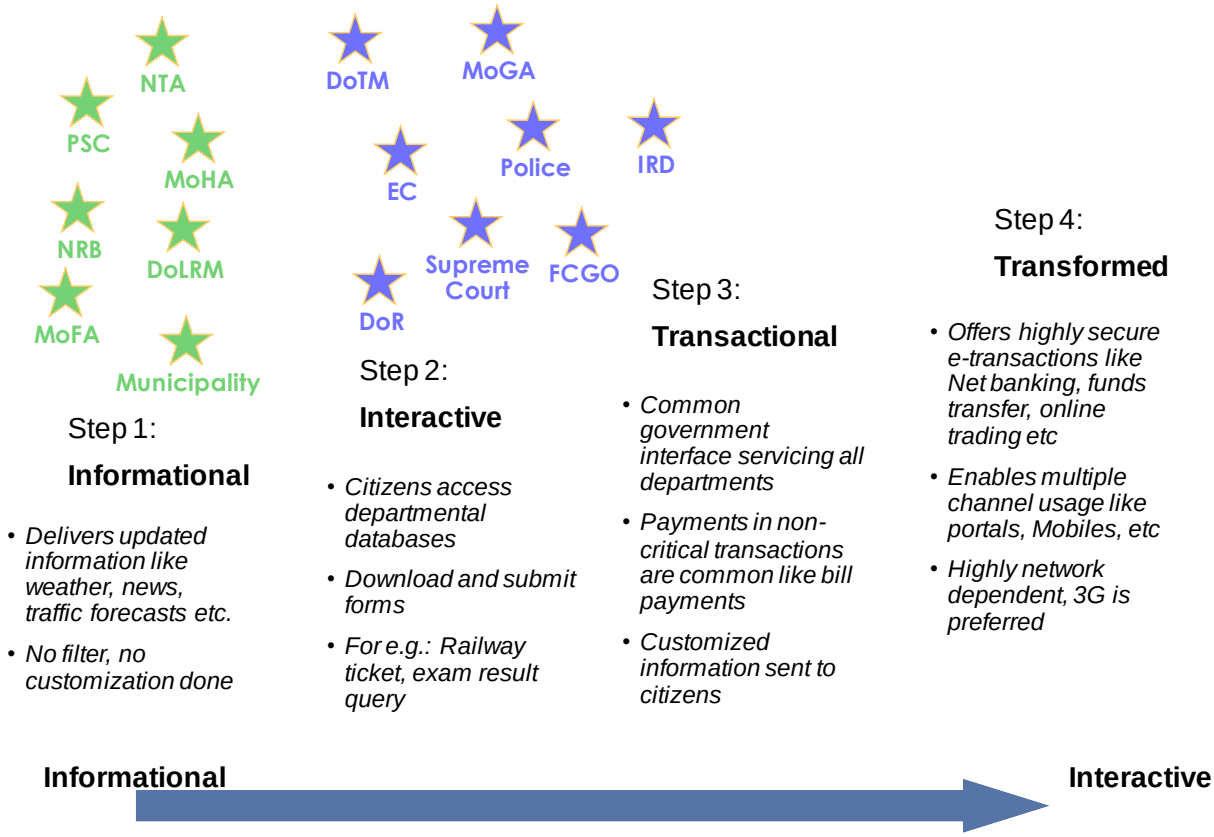
The current state assessment findings at a high level is summarized below -

Current State Assessment of Core e-Gov Infrastructure

Policies	A number of Policies are yet to be defined, including: • Specifications for Classification & Management of Govt. Data • Policies for Front-End, Middleware and Back-End Automation • Policies for Integrated Services • Funding Strategies & Business Models • Policies related to Digital Signature and e-Payment • Policies for Employment Generation through e-Governance
Technology	Required across the Government – uniform Connectivity, shared network for

	Service Delivery, secure Data Repositories, suitable Hardware Infrastructures (especially at grass-root levels)
People & Process	Required across the Government – standard & measurable parameters for Govt. Process Reengineering, predefined Citizen Charters / SLAs, suitable IT skills, easy (and economical) access to ICT Tools

Current State Assessment of Short listed Ministries / Departments



Refer to the "**Nepal GEA - Current State Assessment Report for Short-listed Government Services**" report for the detailed assessment report which provides the details of the identified business services with respect to the service background, process flows, input and output data matrix and the possible web services that could be churned from the present business & technology architecture landscape.

5.3 Target Business Architecture

The overall conceptual future state business architecture is depicted below –

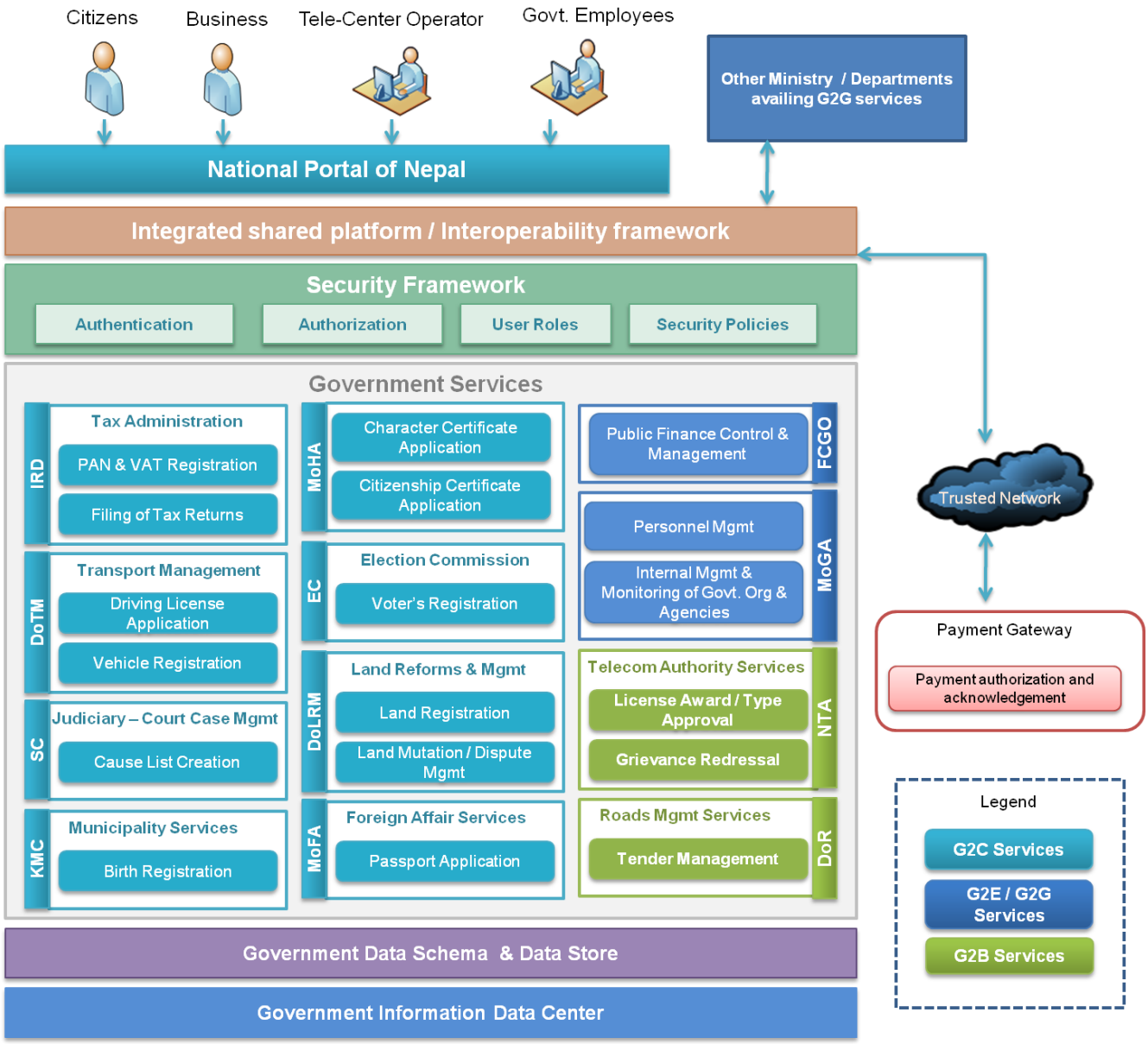


Figure: Nepal GEA Business Architecture

5.4 Gap Analysis – Design Consideration

High Level Design Considerations for BPR

With the current state assessment finding as the baseline business architecture, gap analysis and benchmarking against leading best practices was conducted to arrive at the proposed process design consideration. At a high level the recommended design considerations has been summarized below -

1. Simplification of Application Forms: with limited data inputs and auto-extracting of the data from relevant databases

2. Facility for Online submission of Service Requests: through Tele-Centres, National Portal and Mobile Devices
3. Smart Verification of Applicants' Data: by electronic-interfacing between various Ministries / Departments for cross-verification and sharing of citizens' data
4. Government-wide Training Strategy: for Government Personnel across various levels to ensure effective usage of computerized systems
5. Uniform Connectivity: Secure, 24x7 Connectivity across all levels of Government across all Ministries / Departments
6. National Data Repository: for secure and shared storage of all the Govt. Data from various Ministries / Departments
7. Digital Signatures: to ensure the legality and sanctity of computerized process and data generated via the same
8. Auto-generation of Transaction ID: for each & every online transaction for Application tracking and future reference
9. E-Payment model & leverage e-Payment gateway for electronic transfer of Service Charges into Govt. Accounts and for receiving monies from the Government. The standard model for e-Payment broadly involves the following steps –
    a. Government frames the e-payment policy and it is passed as a legal act through the parliament. This is initiated by the Central bank of the country e.g. Nepal Rastra bank.
    b. The policy governs the e-payment gateway and all electronic transactions made thereof. The security aspects are also covered in the policy.
    c. Government then assigns few banks to provide the payment gateway service who use VISA or MasterCard etc guarantee.
    d. The payment gateway needs to adhere to the security guidelines provided in the act. (Secured transactions are typically carried out through use of verisign others which these established banks may be using for the payment gateway).
    e. Now different departments can utilize these authorized payment gateways to provide online payment facilities to consumers of their departmental services. These payment gateways could be integrated with the departmental / national portals. Refer to the annexure for typical payment gateway operational flow.
10. Digital Copy of Certificates: for instant verification of various Documents / Instruments (e.g. Passport, Driving License, Land Certificate, etc.)
11. Shared Service Delivery Infrastructure: utilizing Tele-Centres by:
    a. Encouraging various Ministries / Departments to route their G2C, B2C and B2B Services via the Tele-Centres
    b. Devising suitable Business Models (e.g. PPP) to meet CAPEX & OPEX of Tele-Centres and to generate employment opportunities
    c. Ensuring optimum spread & reach (e.g. areas with high density of population to have more Tele-Centres, etc.)
    d. Standardizing Infrastructure & Connectivity Specifications for the Tele-Centres after taking suitable inputs from those Ministries / Departments whose services would be on offer via Tele-Centres
    e. Implementing suitable Communication Strategy to ensure that all are aware of the benefits on offer via Tele-Centres

Refer to the "**Nepal GEA - Design Principles Report for Short-listed Government Services**" report for the detailed design principles recommended by PwC for the shortlisted services assessed.

5.5 Business Architecture Roadmap Components

The High level roadmap represents the sequence in its priority of implementing the design consideration. The phases mentioned here are subjected different timelines as per the client's strategic plans. These are jus a sequential phases of implementation.

Phase A

1. Uniform Connectivity: Secure, 24x7 Connectivity across all levels of Government across all Ministries / Departments
2. Simplification of Application Forms: with limited data inputs and auto-extracting of the data from relevant databases
3. Facility for Online submission of Service Requests: through Tele-Centres, National Portal and Mobile Devices
4. Smart Verification of Applicants' Data: by electronic-interfacing between various Ministries / Departments for cross-verification and sharing of citizens' data
5. Government-wide Training Strategy: for Government Personnel across various levels to ensure effective usage of computerized systems

Phase B

1. National Data Repository: for secure and shared storage of all the Govt. Data from various Ministries / Departments
2. Auto-generation of Transaction ID: for each & every online transaction for Application tracking and future reference
3. Shared Service Delivery Infrastructure: utilizing Tele-Centres by:
    a. Encouraging various Ministries / Departments to route their G2C, B2C and B2B Services via the Tele-Centres
    b. Devising suitable Business Models (e.g. PPP) to meet CAPEX & OPEX of Tele-Centres and to generate employment opportunities
    c. Ensuring optimum spread & reaches (e.g. areas with high density of population to have more Tele-Centres, etc.)
    d. Standardizing Infrastructure & Connectivity Specifications for the Tele-Centres after taking suitable inputs from those Ministries / Departments whose services would be on offer via Tele-Centres
    e. Implementing suitable Communication Strategy to ensure that all are aware of the benefits on offer via Tele-Centres

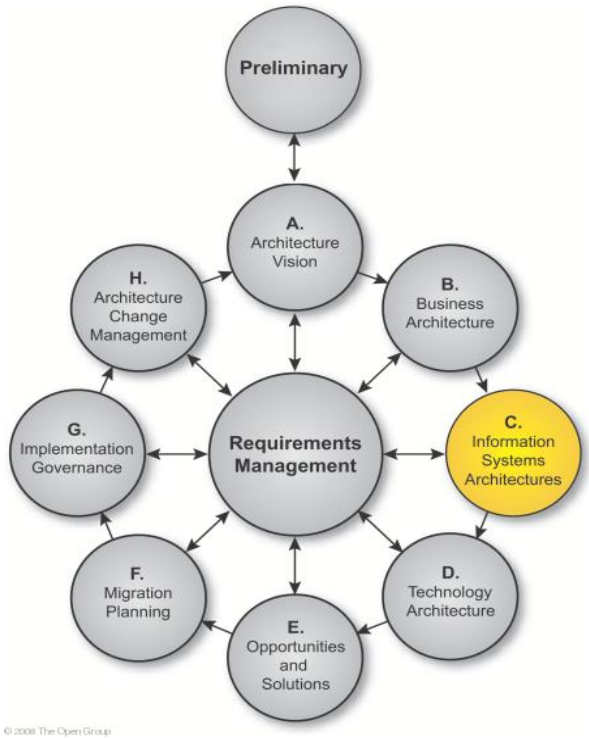
Phase C

1. e-Payment Gateway: for electronic transfer of Service Charges into Govt. Accounts and for receiving monies from the Government
2. Digital Copy of Certificates: for instant verification of various Documents / Instruments (e.g. Passport, Driving License, Land Certificate, etc.)

Reference: For detailed description of each element in the Business Architecture refer to the GEA Enterprise Architecture continuum and Architecture repository.

6. TOGAF ADM Phase C - Information System Architecture

6. Phase C: Information Systems Architecture



Phase Overview

The objective of Phase C is to develop Target Architectures covering both the data and application systems domains.

Information Systems Architecture focuses on identifying and defining the applications and data considerations that support an enterprise's Business Architecture; for example, by defining views that relate to information, knowledge, application services

Phase C.1 Data Architecture typically outlines the data principles, baseline data landscape, the recommended target data landscape, the common & segment specific data model & data standards for information exchange across departments, the information flow model, govt. data xml schema, etc

Phase C.2 Application Architecture typically covers the application principles, baseline application landscape, the recommended target architecture, the application standards and guidelines to be adopted across the enterprise.

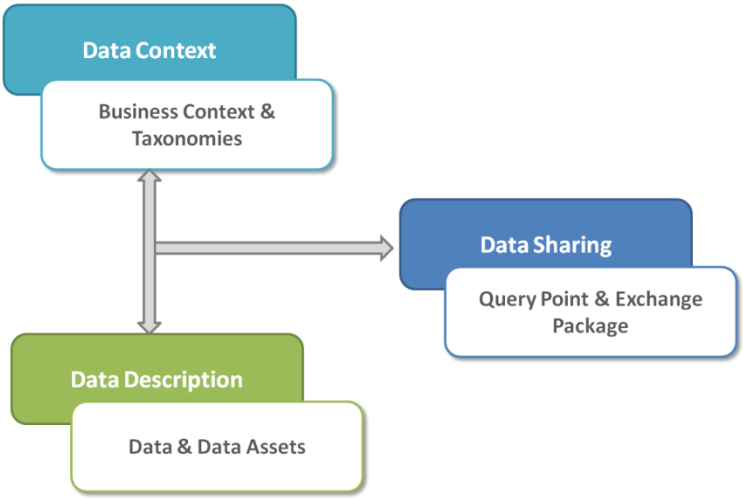
6.1 Phase C.1 - Data Architecture

The objective of creation of the government data architecture is to maintain an adaptable infrastructure designed to facilitate data access, definition, exchange, management, security & integrity at the enterprise level. The enterprise common & segment specific data entities and data standards identified will facilitate in data sharing & exchange. These data entities will serve as the major input in the Nepal Govt. data schemas for electronic interchanges of data across the government organization / units leveraging the proposed interoperability framework.

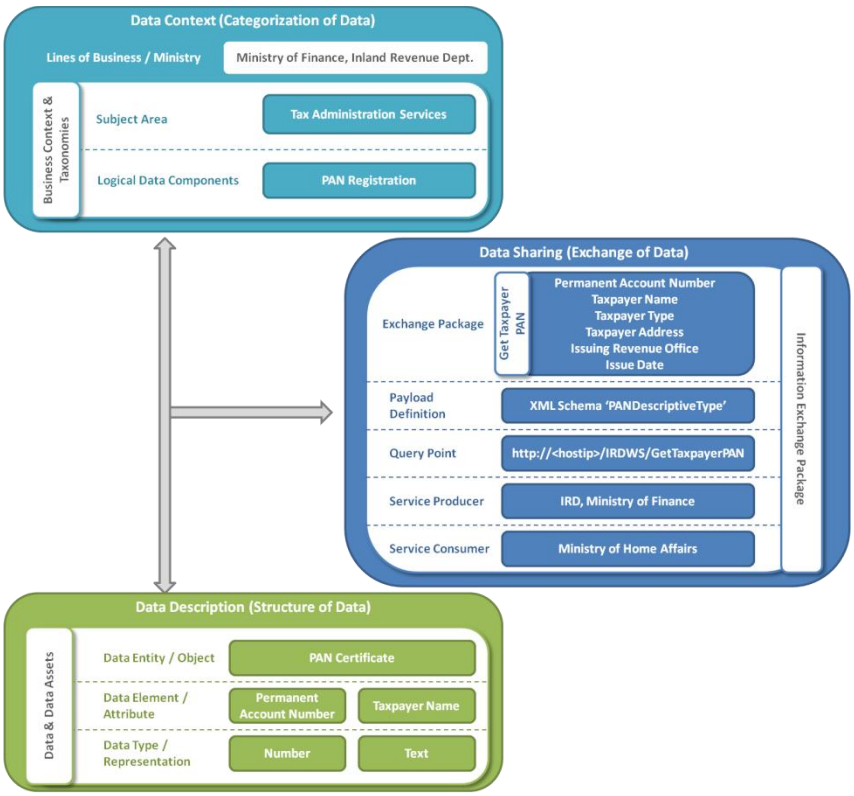
6.1.1 Data Reference Model

The Data Reference Model (DRM) provides a structure that facilitates the development of government data that can be effectively shared across govt. organization & unit boundaries for better & effective government service delivery improve decision-making and improve mission performance. The DRM is a service-oriented model that provides the pathway for "Services to Citizens" to become operational. At the same time, the DRM provides an impetus for govt. organizations to better understand their data and how it fits in the total realm of government information.

The 3 standardization areas of DRM are shown below –



An overall example of the above DRM structure from the Nepal GEA perspective considering a specific Inland Revenue Department (IRD) data entities, its categorization, structure definition and exchange package service is illustrated below –



6.1.2 *Data Architecture Principles*

Data Architecture Principles

- Data is an Asset
- Data is shared
- Data is created, accessible and shareable
- Data has an owner/trustee
- Data security and permission
- Standard, Common vocabulary and data / metadata definitions.

Principle # 1	
Name	Data is an asset
Statement	Information / Data are a national asset that has high value to the Govt. of Nepal as data is the foundation of all decision making. Hence effective and careful data management is of high importance and priority to the Govt. of Nepal to ensure where it resides, can rely upon its accuracy, and can obtain it when and where we need it
Rationale	• Effective data management would ensure effective decision making & improved performance. Besides organizing and managing the key data assets of the enterprise drive the business processes needed to run the government

Principle # 2	
Name	Data Creation, Accessibility & Availability
Statement	Creation: All enterprise information / data should be captured once at the point of its creation / source. New / updated data entry should be restricted to the designated source system who is the owner of the data Accessibility: Data should be accessible to users to perform their respective business functions. Effective use of information must be considered from an enterprise perspective to allow access by a wide variety of users. Availability: Government wide enterprise data should be made readily available (real-time), so as not to delay the business processes, and will enable appropriate timely sharing across the organization.
Rationale	• Keying information once and re-using it across the enterprise will reduce costs, promote the efficiency, accuracy, consistency of data and assures quality • Wide access to data leads to efficiency and effectiveness in decision-making, and affords timely response to information requests and service delivery. Staff time is saved and consistency of data is improved • Readily available enterprise data will facilitate timely data access at every level of the organization and provide timely response to information request and effective service delivery

Principle # 3

Name	Data is Shareable
Statement	Government wide enterprise data should be shared across government organizations and units / departments. Users should have access to the necessary shared data required to perform their respective business functions. Shared data should be centrally controlled and managed at the appropriate organizational level
Rationale	• Electronically shared data will result in increased efficiency when existing data entities can be used, without re-keying, to create new entities. Users will rely on authorized sources of more accurate and timely managed data thereby help in improved decision making.

Principle # 4	
Name	Data Ownership & Primary Data Source
Statement	Each data entity / item must be owned by a government unit. The government unit should be responsible for data definitions, domain, values, integrity and security. Owner should be identified for each data entities and its related data services Primary Data Source: All government wide enterprise data entity should have an authoritative, official, primary data source that is the location for all create, update and delete actions. All copies of enterprise data will be considered secondary and will not be updated as part of business transactions
Rationale	• Lack of a well-defined data ownership will lead to confusion as to who can change the data. Identifying the govt. unit with ownership of its respective data entities avoids ambiguity and creates clear responsibility and accountability for all data. • Identifying the data owners will clearly define the point of contact in the respective govt. unit who will be responsible and accountable for all changes in the data entities & data services and the approval of the same. • In order for enterprise data to be managed effectively, there can be only one primary source for each data entity so that data entity could be traceable back to the source system. Otherwise, inconsistent, erroneous and out-of-date data may result • Data integrity is at its highest level when the central management of changes to data is done by an authoritative source of record.

Principle # 5	
Name	Data Security & Permission
Statement	Data should only be available to users who require the information as part of their role. Provision should be there to provide role-based access to data
Rationale	• Open sharing of information and the release of information via relevant legislation must be balanced against the need to restrict the availability of classified, proprietary, and sensitive information • Ensures compliance with legislation and government data & security polices • The role based authorization will enable the right level of information to be

	shared across departments and ministries.

Principle # 6	
Name	Standard, common vocabulary and data / metadata definitions
Statement	There should be a standard, common and consistent definition of data / metadata across the enterprise which should be understandable and available to all users. Enterprise data & metadata standards should be defined to ensure seamless interoperability while interchanging data e.g. definition of e-GMS / eGIF, & Metadata Standards. Every data item important for data exchange across the enterprise should have metadata. A centralized server-based source of metadata is preferred
Rationale	• The data to be exchanged across the government should have a common definition with an agreed format and meaning of the data items. A common vocabulary will facilitate effective communications and enable sharing of data. In addition, it is required to interface systems and exchange data. • Provides metadata modelling, consistency and quality • Centralized metadata provides single point for maintaining the metadata

6.1.3 Baseline Data Architecture

The first stage in defining the data architecture is capturing the enterprise conceptual data architecture for the Government Enterprise Architecture (GEA) of Nepal. It provides a planning level view which shows the various information subject areas, the logical data component grouping along with the high level data entities within the logical component groups.

The conceptual data model provides a specification of the highest-level data entities that support Govt. of Nepal business processes and it relevance from data sharing & exchange perspective across the interoperability framework. This conceptual data model provides an overarching framework to organize more detailed data architecture efforts and provide a common taxonomy for describing data assets across the government.

6.1.3.1 Data Classification Scheme

Aligning with the DRM "Data Context" standardization area, the data classification scheme as identified for the Nepal GEA is based on the subject area context at the highest level with logical grouping of data entities with it as depicted below -

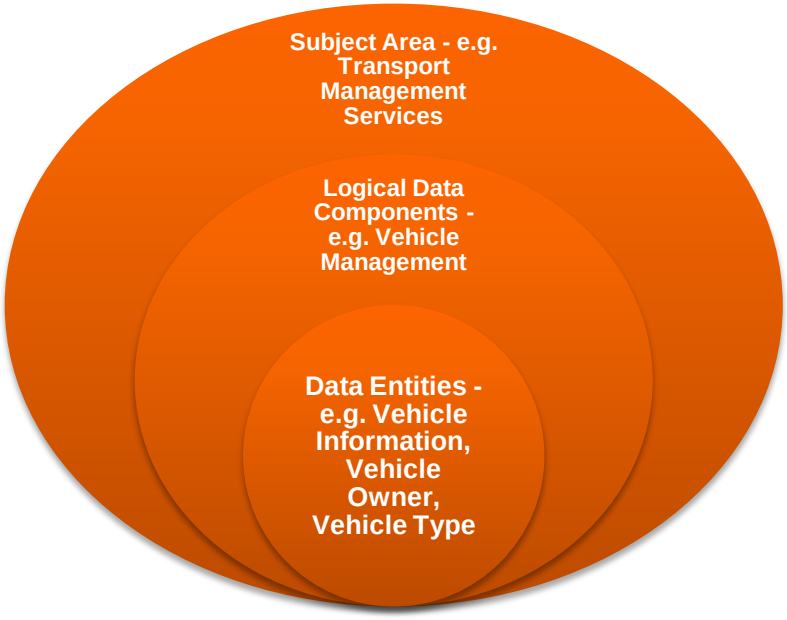
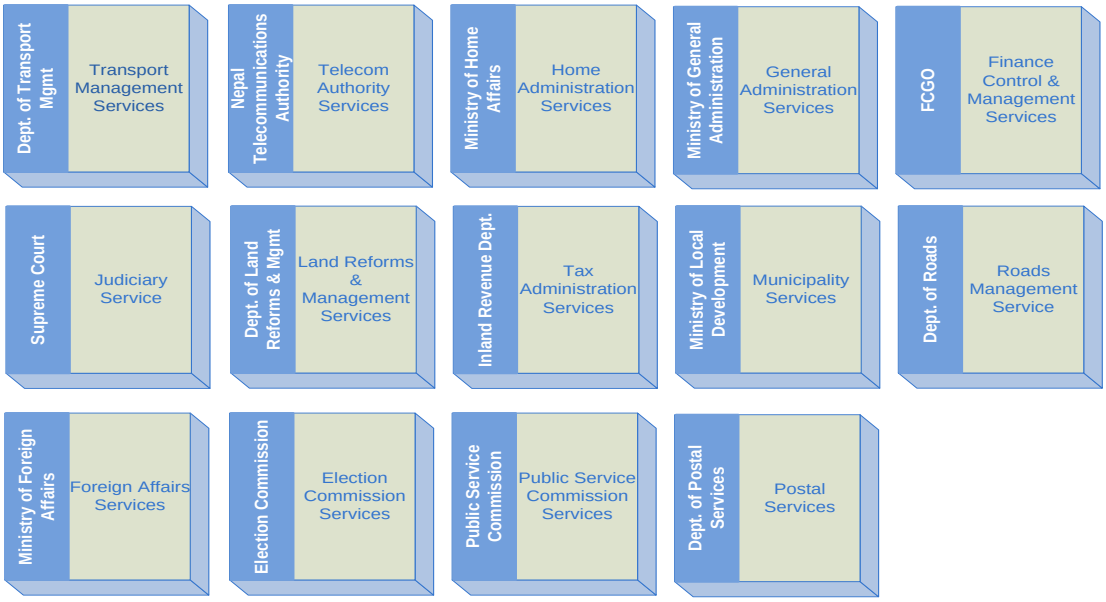


Figure: Data Classification Approach

Subject Area

Subject area provides a high-level set of categories that groups the logical data components and data entities based on the business / domain area they most closely align with, the stakeholders they impact, the extend or degree to which they are dependent on each other and the need to be managed as a unit.

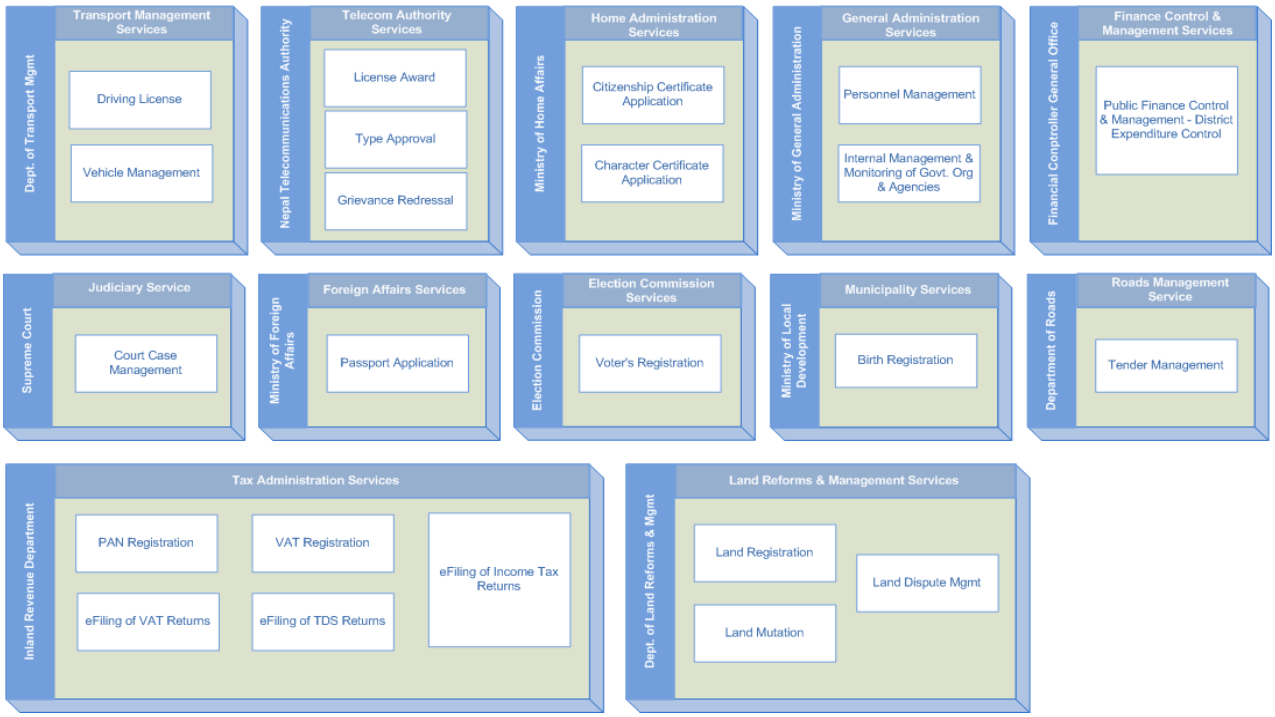
Based on the Nepal's government organization structure and their domain area classification, the information / data has been categorized broadly under the following subject areas as depicted below –



6.1.3.2 Logical Data Components

The logical grouping of data components within each subject area provides a boundary zone that encapsulates related data entities to form a logical grouping. Creation of logical data components groups data entities into encapsulated modules for governance, security, and deployment purposes.

Based on the above subject area classification, the data entities has been further grouped under logical data components groups as depicted below –



6.1.3.3 Conceptual Data Model

As part of the process of defining the common data standard, PwC studied the data model of individual departments (for the short-listed services) and abstracted out the common data entities used across the departments e.g. individual profile, company profile, address, contact etc. A generic common data model was proposed at the conceptual / business level based on industry standard best practices that describe the core generic data entities at the enterprise level to be exchange & shared across govt. organizations.

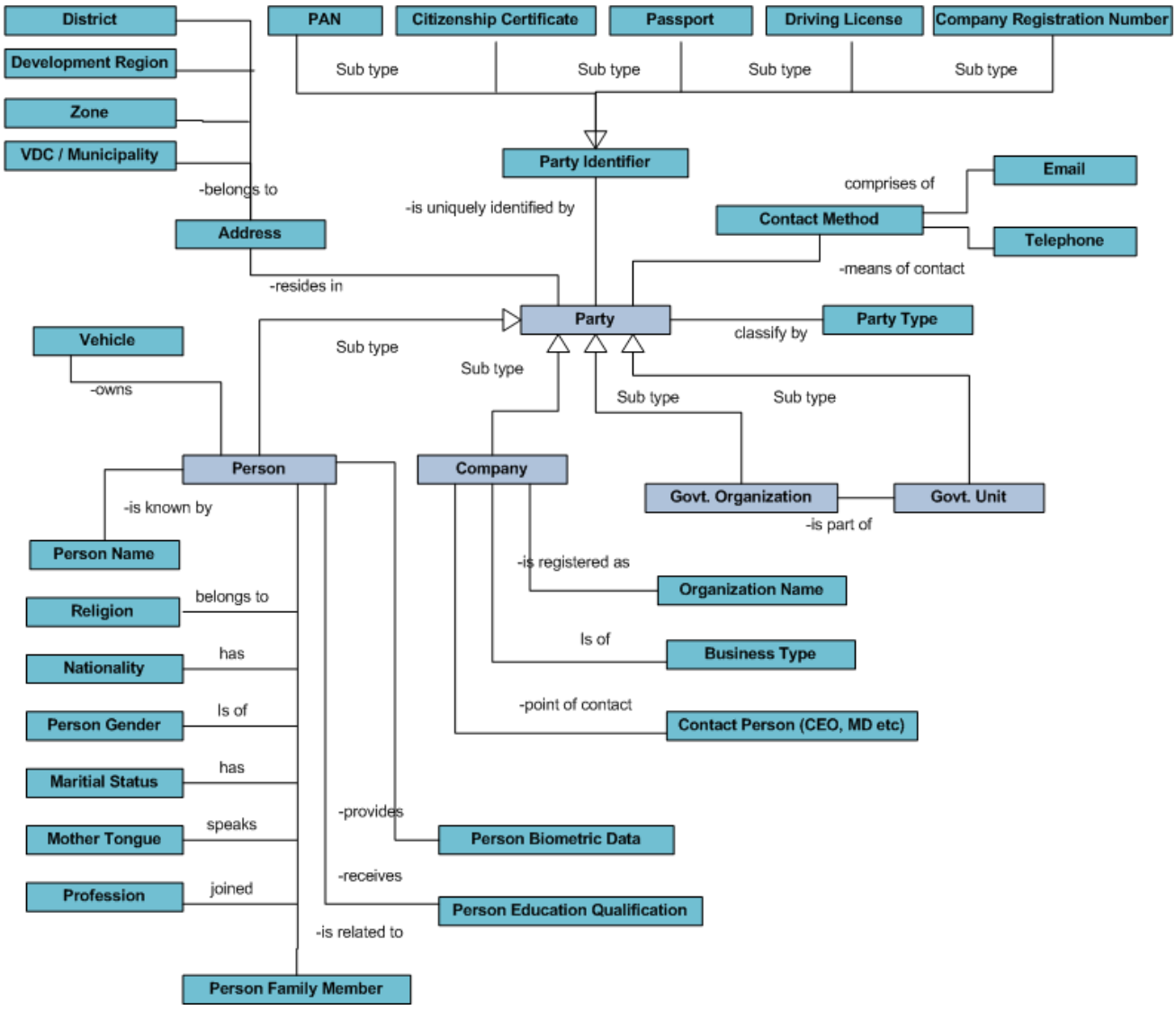


Figure: Nepal GEA Conceptual Data Model

- Pls. note the high level data entities identified in this section does not cover the entire business processes of each department but are for the short listed services from 16 departments as identified in the AS-IS assessment report.
- These data entities and its data standards identified are more relevant from the data sharing & exchange perspective and are to be used in the Nepal Govt. data schemas for electronic interchanges of data across the government organization and units leveraging the proposed interoperability framework

6.1.3.4 Logical Data Architecture

Current State Data Landscape

The following diagram provides a snapshot of the present data landscape with respect to some of high level data entities that resides in the respective owner system.

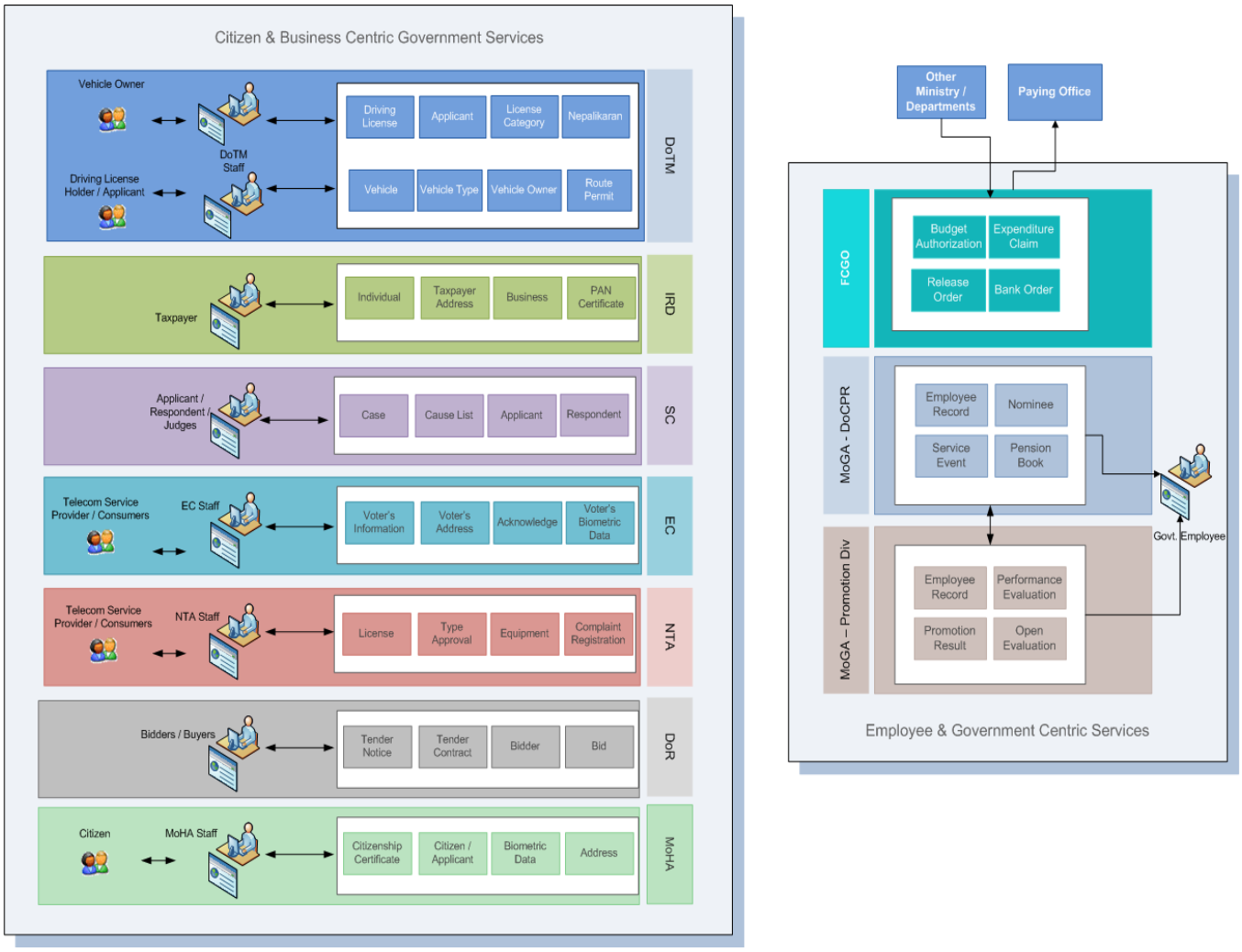


Figure: Nepal GEA - Current State Data Landscape

6.1.4 Target Data Architecture

The following diagram provides a snapshot of the proposed target data landscape leveraging the National Portal, GEA infrastructure and NeGIF platform to enable data sharing & exchange across govt. organizations & citizens.

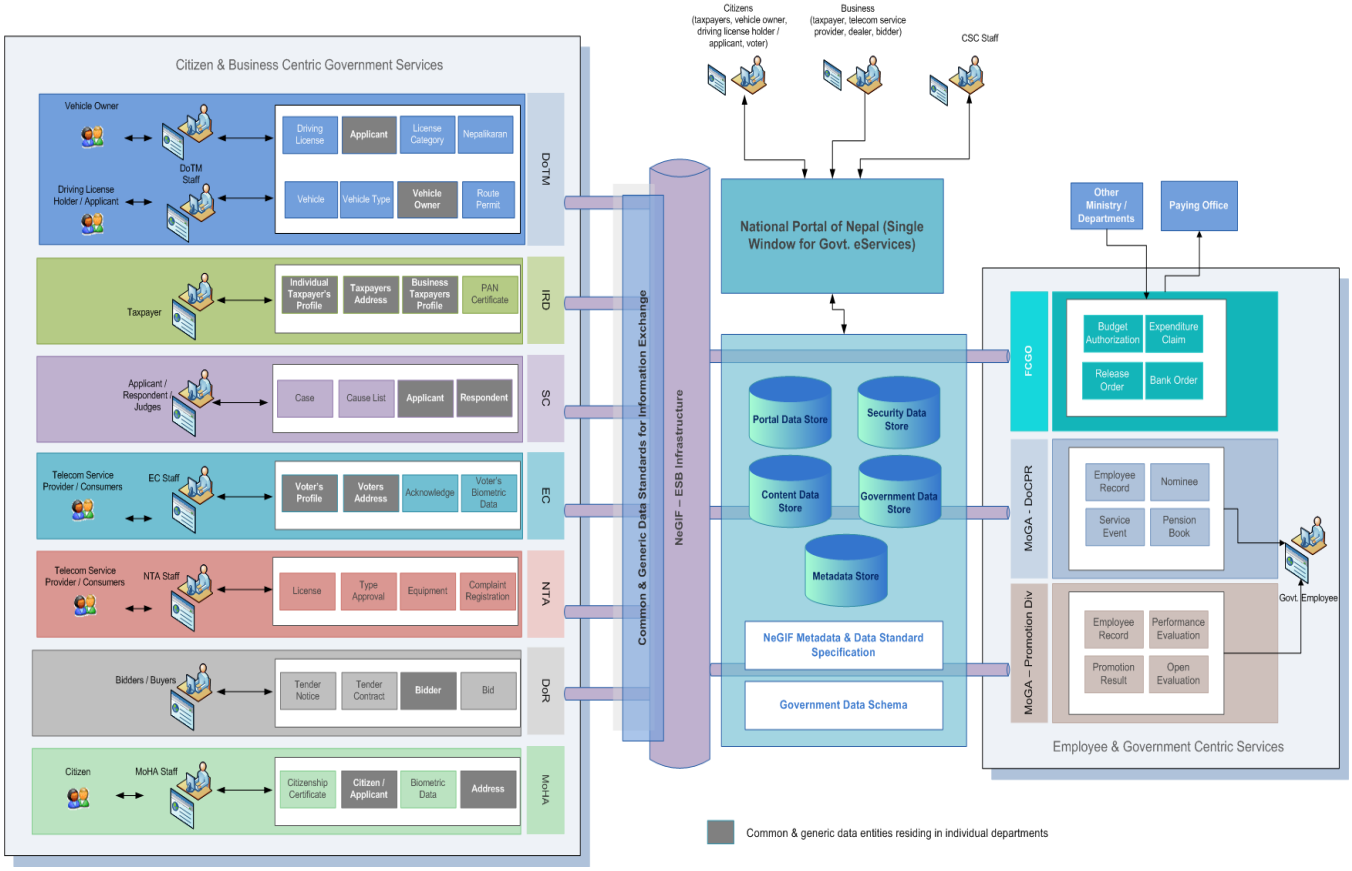
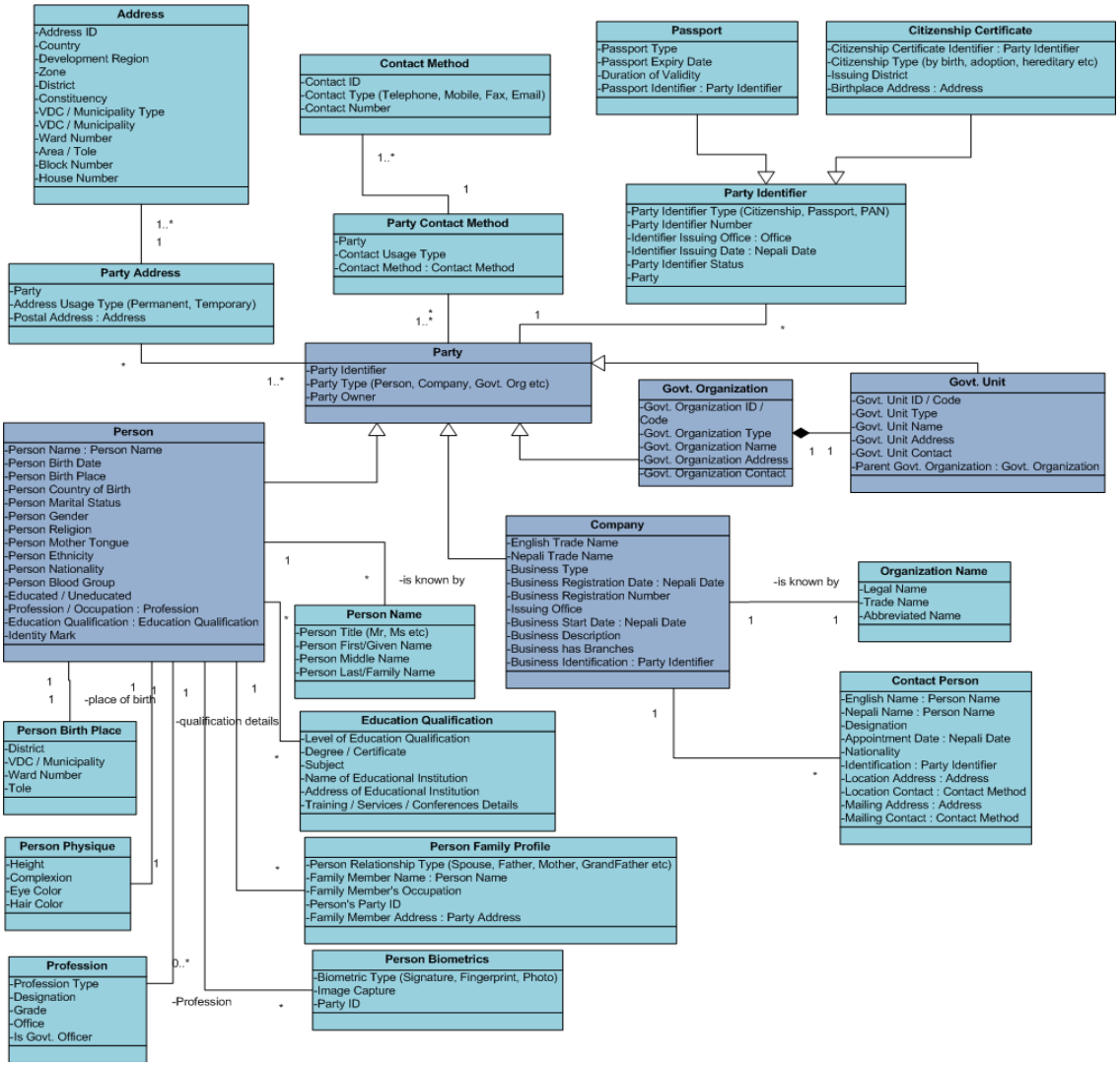


Figure Nepal GEA - Future State Data Landscape

6.1.4.1 Logical Data Model

The Enterprise Core Logical Data Model has been derived from the Enterprise Core Conceptual Data Model providing the logical view of the common conceptual data model. The logical view will describe the conceptual data entities in more details with respect to –

- Identifying the data elements / attributes for each data entity,
- Defining the data type with respect to the XML data definition type for each data elements / attributes
- Applying normalization, applying generalization / inheritance where applicable defining super type and specialized sub type data entities
- Absorbing relationships as attributes
- The subsequent Govt. Data XML Schema for describing the common data entities required for data sharing & exchange across the interoperability framework will be based on this specification.



6.1.4.2 Information Flow Model

Information Flow Model shows the key information / data exchanges (e.g. vehicle information, taxpayers PAN etc) between government units / departments and with the outside world. The Information flows represents the movement of required flows of information / data across the government organisation without representing any physical implementation. The information flows will access a number of distinct web services and department specific data stores.

The information flow model for citizen and business centric services are depicted below -

Citizen Centric Services (G2C)

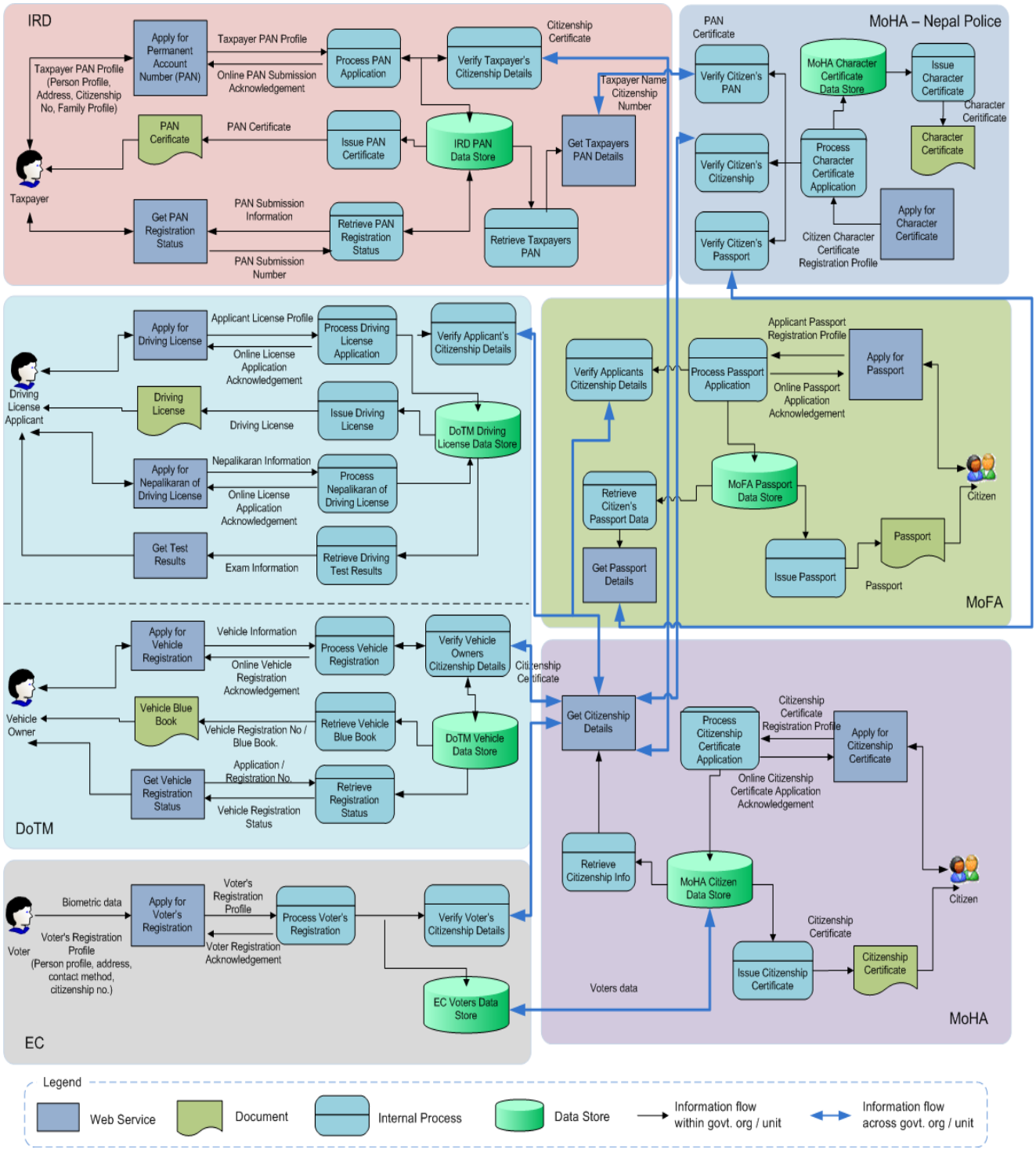


Figure - Information Flow Model for Citizens Centric Services

Business Centric Services (G2B)

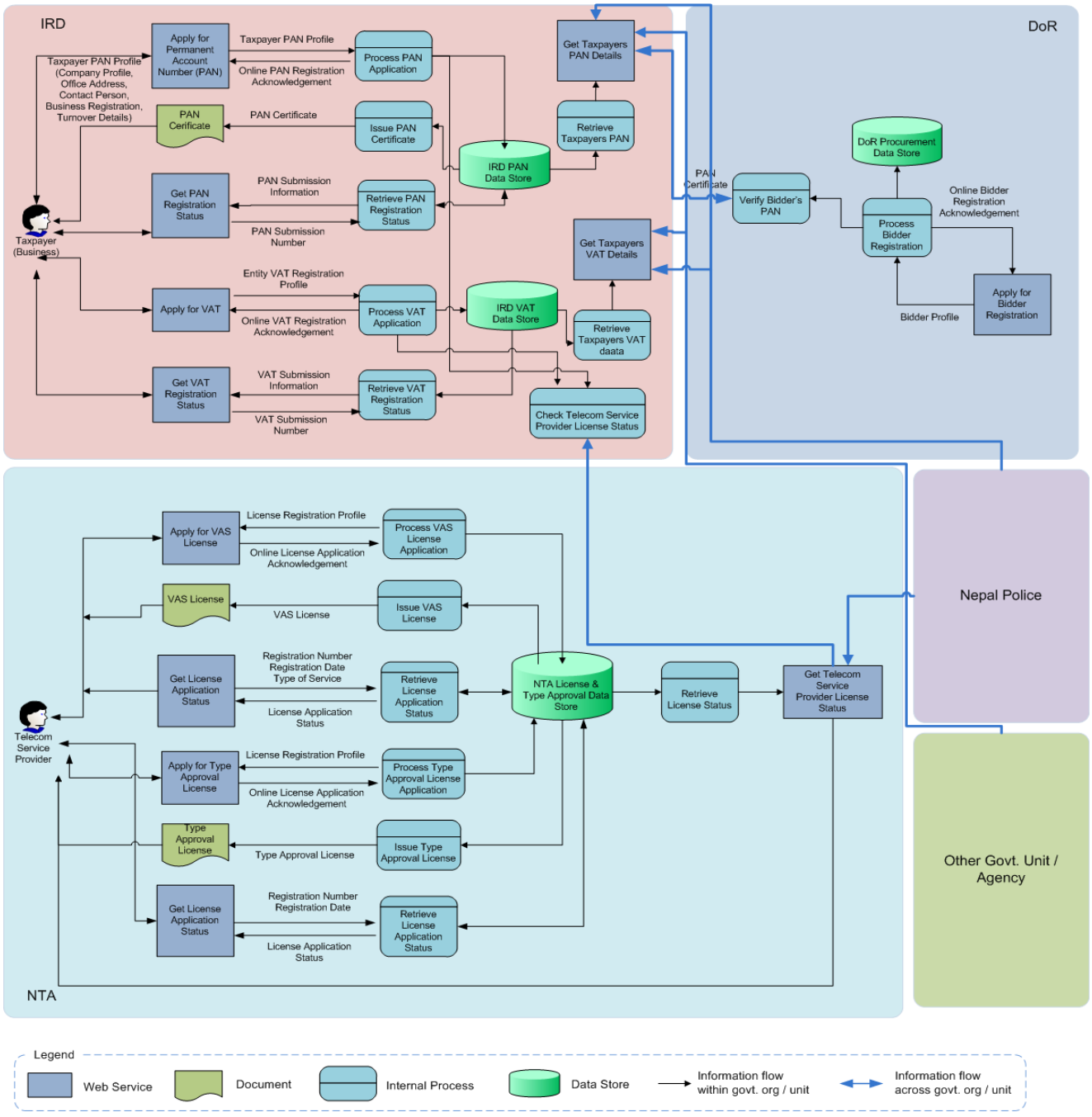


Figure - Information Flow Model for Business Centric Services

Employee Centric Services (G2E)

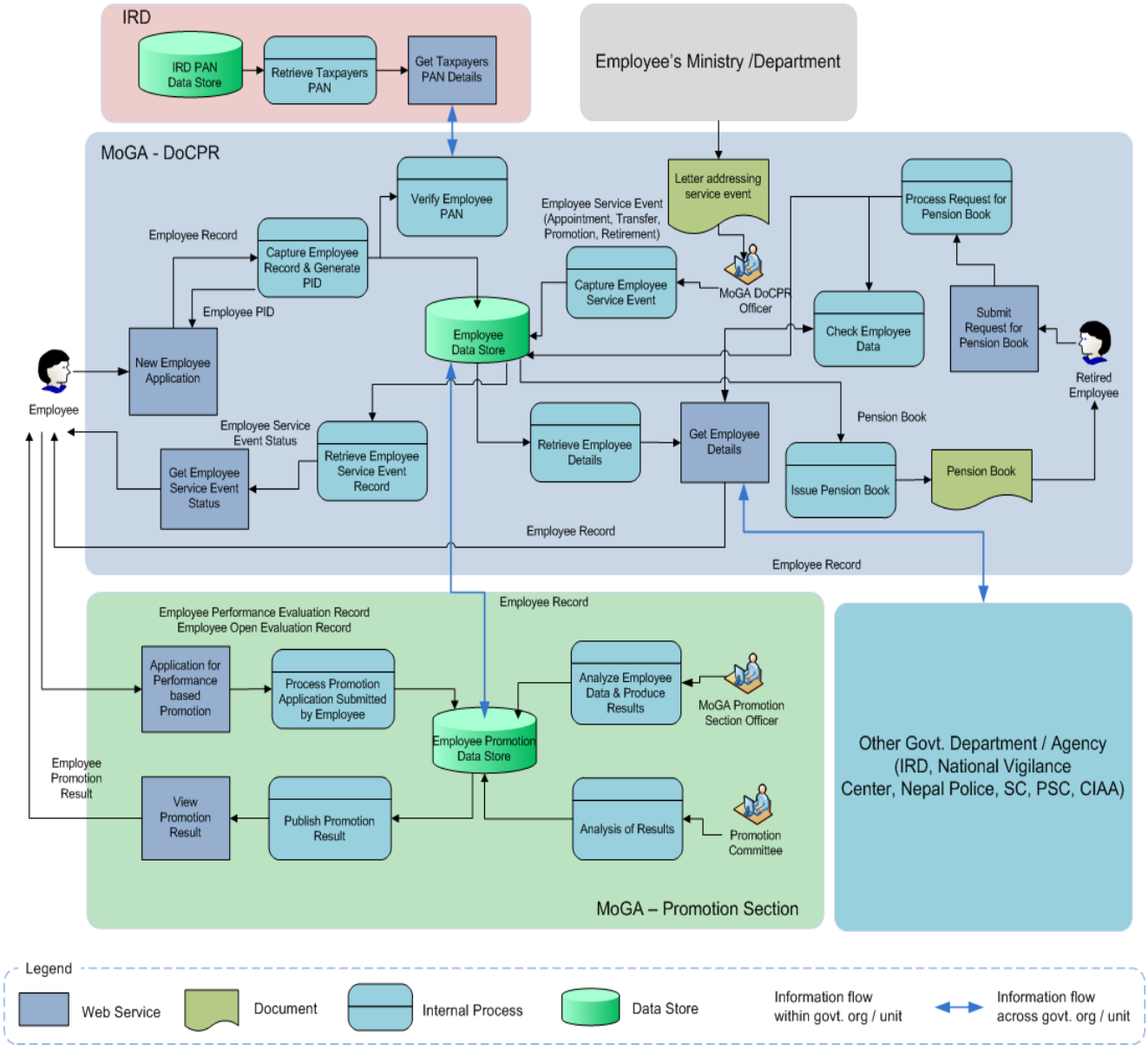


Figure - Information Flow Model for Employee Centric Services

6.1.5 Gap Analysis

- At present due to lack of adequate network infrastructure the data entities that resides in each of the departments are solely used in silos by the respective departments. Data / information exchange across the organization is not possible thereby violating the data sharing principles. The only data exchange across departments is between MoGA, DoCPR and MoGA promotion division that exchange employee records.
- Similar citizens and business general profile, family profile, address and contact information are captured in multiple locations and maintained within the department specific scope
- No well defined data principles, polices and guidelines to be used across the government organizations
- Lack of common enterprise data standards

6.1.6 Data Architecture Roadmap Components

Phase-A

1. Establishing the data architecture principles that will serve as the key architectural input or drivers to the government organizations for the design of the future state data architecture.
2. Establishing the organization level ESB based integration infrastructure that will provides a platform for data exchange across departments. This eliminates the information silos and enables seamless data access & sharing across the government.
3. Defining enterprise core common data entities & data model which represents the core generic data entities to be used across the various govt. units / departments of the Govt. of Nepal for data sharing & exchange across the interoperability framework
4. Establishing the government NeGIF data & metadata standards for the core common data entities for use across government will enable easier, more efficient exchanging and processing of data. It will also remove ambiguities and inconsistencies in the use of data across the government ministries, departments & govt. agencies. These standards apply to all systems that are mandated in the NeGIF and are for use in all other public sector interfaces as well
5. Finalize the target data model for the IRD segment incorporating any additional data entities that would be required over and above the baseline data entities to support the to-be process re-engineering consideration as suggested by PwC team
6. Definition of Govt. data schema in XML format for data sharing & exchange across the interoperability framework which will be based on the above *common* data specification. All departments that would expose its govt. services as eServices would have to adhere to the recommended common data exchange specification as defined in the Govt. Data XML Schema & the exchange package (or web service contract definition) to enable seamless information flow across eGIF
7. Formalizing a data governance model & structure

Phase-B

1. Defining segment specific data entities & data model required for data sharing & exchange across the interoperability framework for the 16 short listed departments in scope.
2. Supporting & guiding the data governance team in defining new segment specific data entities, updating the common data entities, govt. data schema & data standards as and when new departments will be ready to integration with the Nepal GEA infrastructure to expose new eServices
3. Definition of Govt. data schema in XML format for segment specific data specification for data sharing & exchange across the interoperability framework. Specific departments that would expose its govt. services as eServices would have to adhere to the recommended *segment/department specific* data exchange specification as defined in the Govt. Data XML Schema & the exchange package (or web service contract definition) to enable seamless information flow across eGIF

Phase C

1. Definition of a centralized Master Data Management Hub solution that attempts to centralize and standardize the national master data set by accurately consolidating, cleansing, de-duplicating and reconciling the master data residing across disparate data silos. This will help maintain a single, trusted, accurate, complete and consistent view of the citizens & business records across government units which could be the single point of reference for other departments thus allowing quick & easy identification of citizens at any touch point.

Reference: For detailed description of each element in the Information Data Architecture refer to the GEA Enterprise Architecture continuum and Architecture repository.

The "**Nepal GEA – Data Architecture**" report and its supporting documents will provide the detailed information pertaining to data architecture

6.2 Phase C.2 - Application Architecture

Phase C.2 Application Architecture typically covers the application principles, baseline application landscape, the recommended target architecture, the application standards and guidelines to be adopted across the government organizations.

6.2.1 Application Architecture Principles

Application Architecture principles

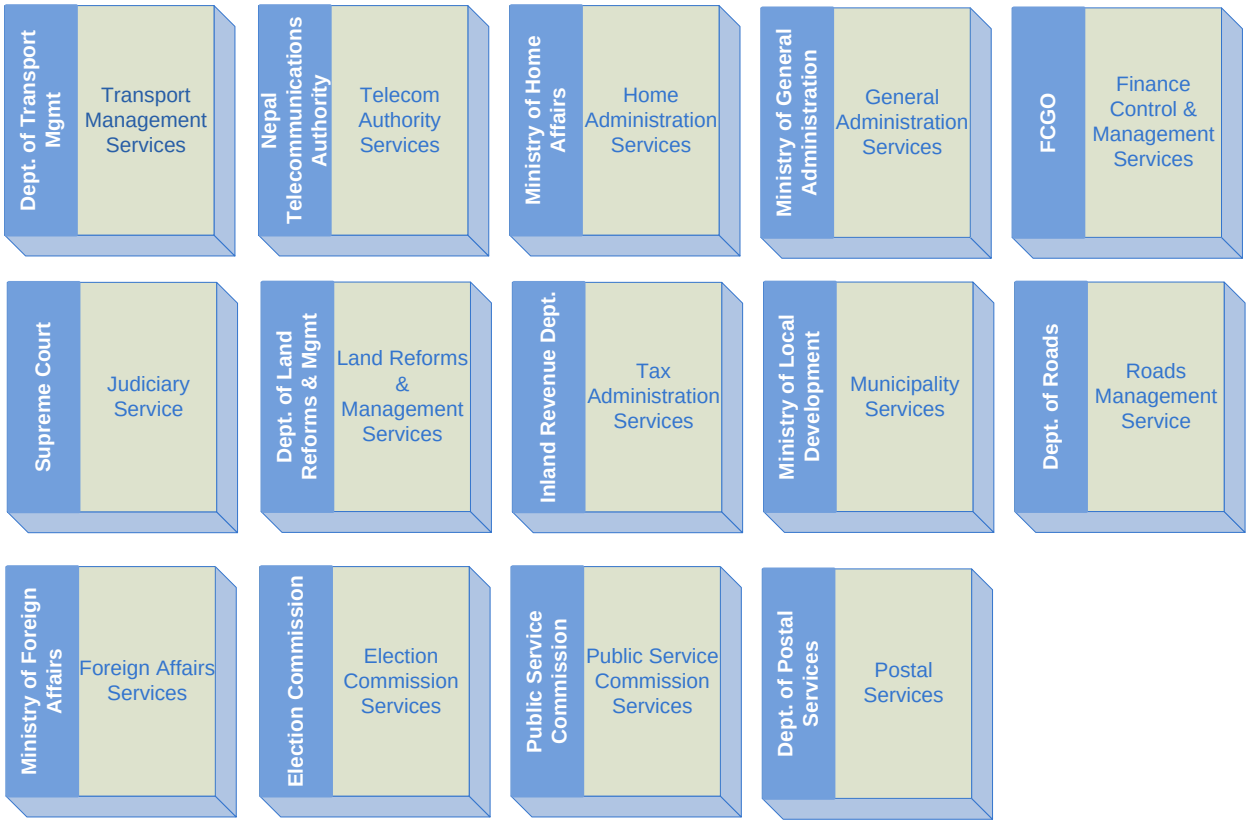
- Modular and component based
- Ease of use and re-use

Principle # 1	
Name	Modular and component based
Statement	Adopt a modular and component based architectural solution, aligned to business processes, that conforms to established open standards with well defined roles & responsibilities. Components should be independent of the physical topology of the system
Rationale	Reduces total cost of ownership and avoids vendor lock-in
Implications	• Avoid proprietary solutions and technologies if possible • Consider adhering to W3C, e-GIF etc technical standards, Consider use of latest web services, XML and integration standards • Internet based web standards and technology should be preferred as the basis for all solutions

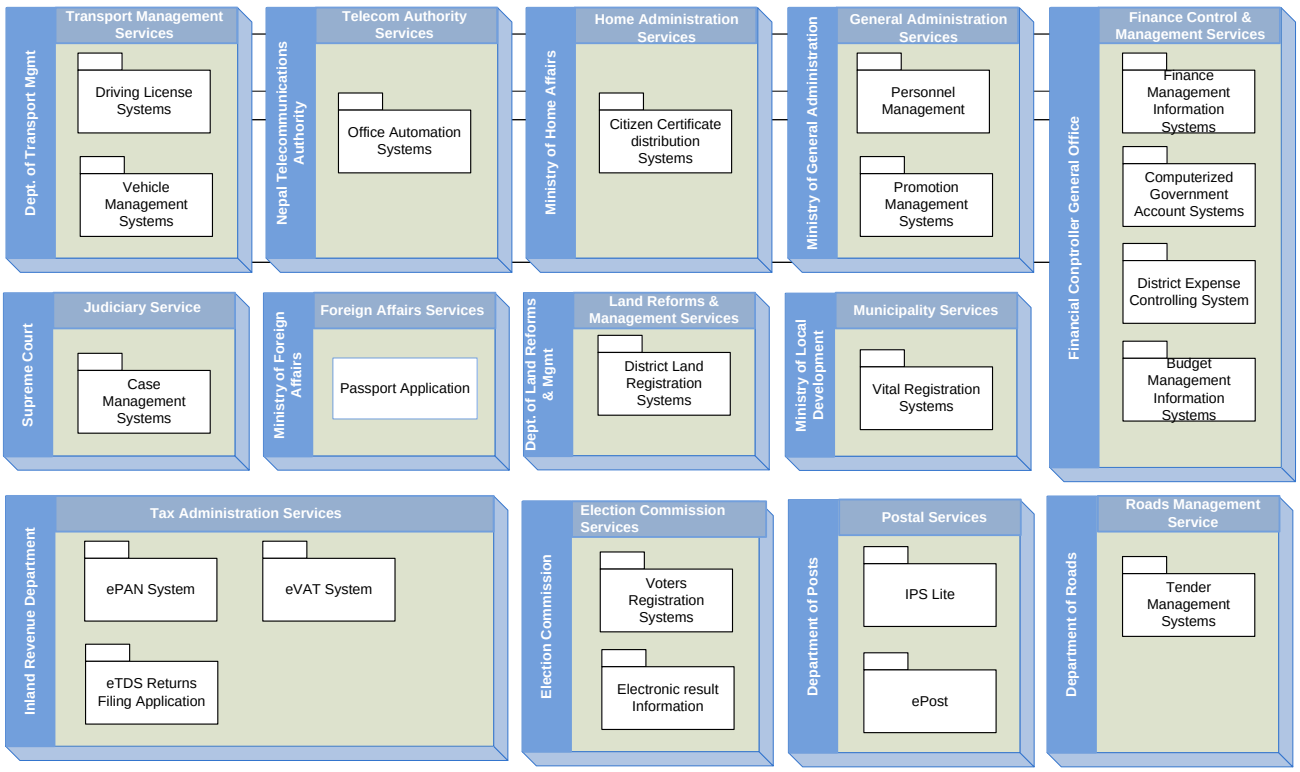
Principle # 2	
Name	Ensure Simple, Reuse, Flexible & Extensible Solution
Statement	Common services components should be implemented once and re-used when required. Services/Solutions should be flexible and extensible to respond, accommodate and adapt to unanticipated requirements easily. Consolidate & simplify technology applications wherever possible to minimize

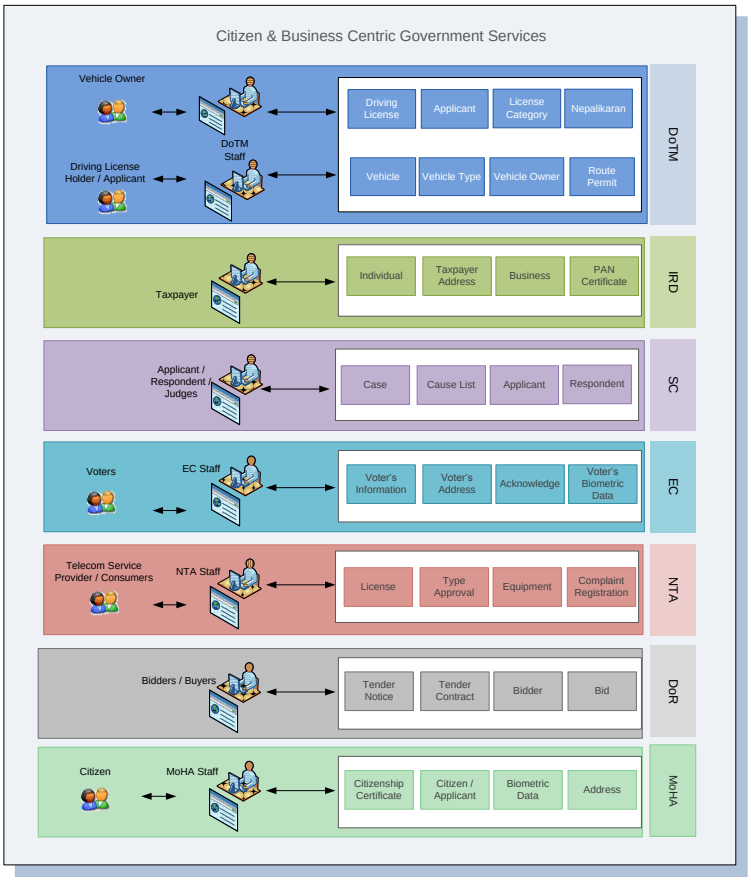
	complexity
Rationale	• Provides a simpler and more cost-effective solution • Reduces development time and makes the solution easier to maintain with change in requirements. • Creates a more flexible and robust solution • Reduced duplication through consolidation of existing systems/services • Improve reliability and scalability with fewer points of failure
Implications	• Software should use meta-data to configure itself (using declarations rather than coding) • Services should be loosely coupled and solutions asynchronous in nature • Ongoing application, database and server consolidation may be required

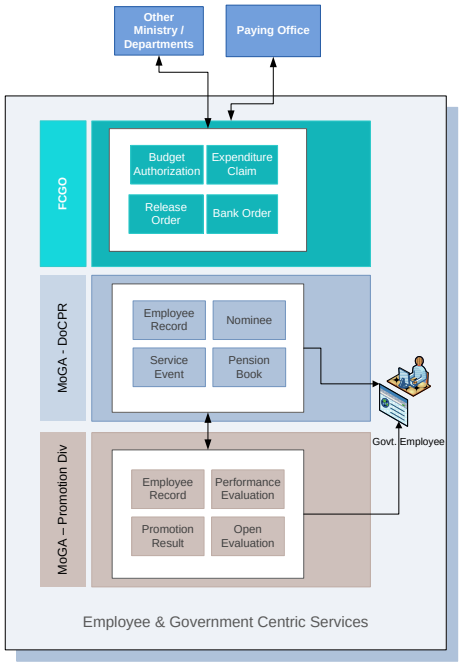
6.2.2 *Baseline Application Architecture*



6.2.3 As-is Application Landscape





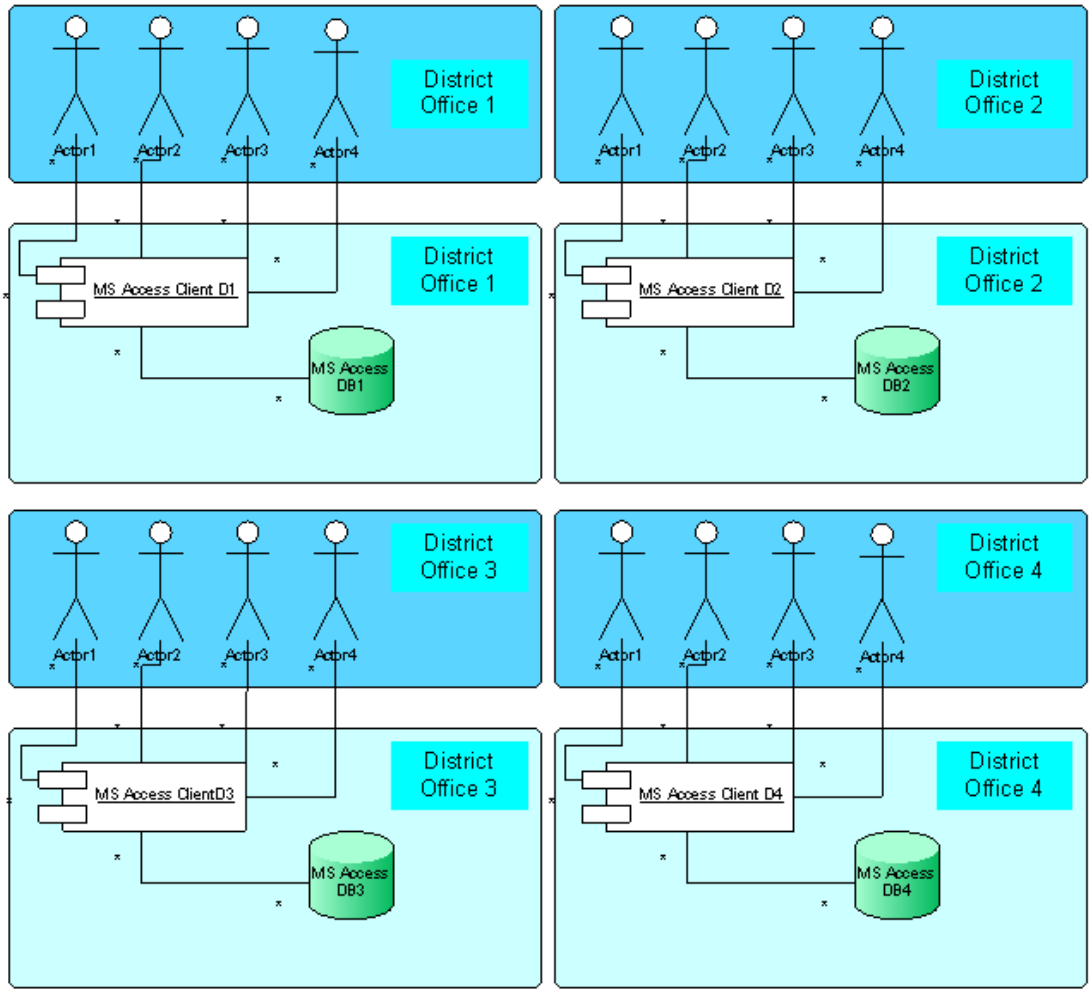


From the above the table 1 of GEA Applications inventory, the current applications of the GEA Nepal project could be classified into 4 different types of applications.

6.2.3.1 Type 1 Applications

The Type 1 Applications are monolithic applications that houses both the application and database servers execute in the single platform and single server/desktops. These are the applications that do not have centralized database systems for all users across the country, but infact individual database for every single location of users. This could lead to individual districts having a different schema of databases for the same application.

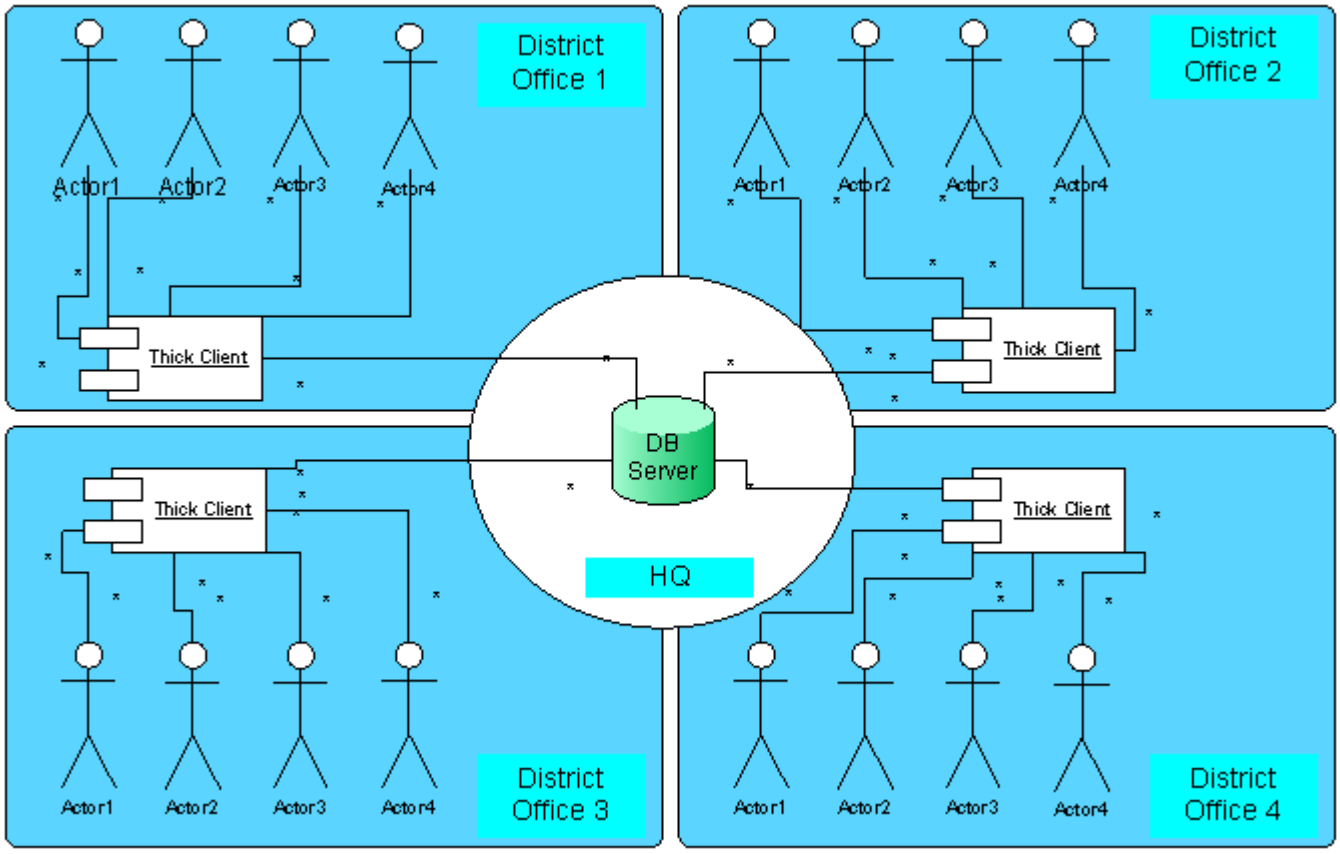
For Ex: Applications built on MS Access platforms, where the client is MS Access and the database is also on MS Access. The applications on these platforms are District Land Information Systems by DoLRM, Vital registration Systems of KMC.



6.2.3.2Type 2 Applications (Client server Architecture)

The Type 2 Applications are client server applications, which have a common database for all clients connecting to it. However, the business processing logic remains in the client side of the applications. These are normally thick clients with all the business logic for processing the data and transactions remaining in the client side of the application. Updating the newer version of the clients would lead to huge exercise with these kinds of applications, as the updated applications would need to be updating all the clients.

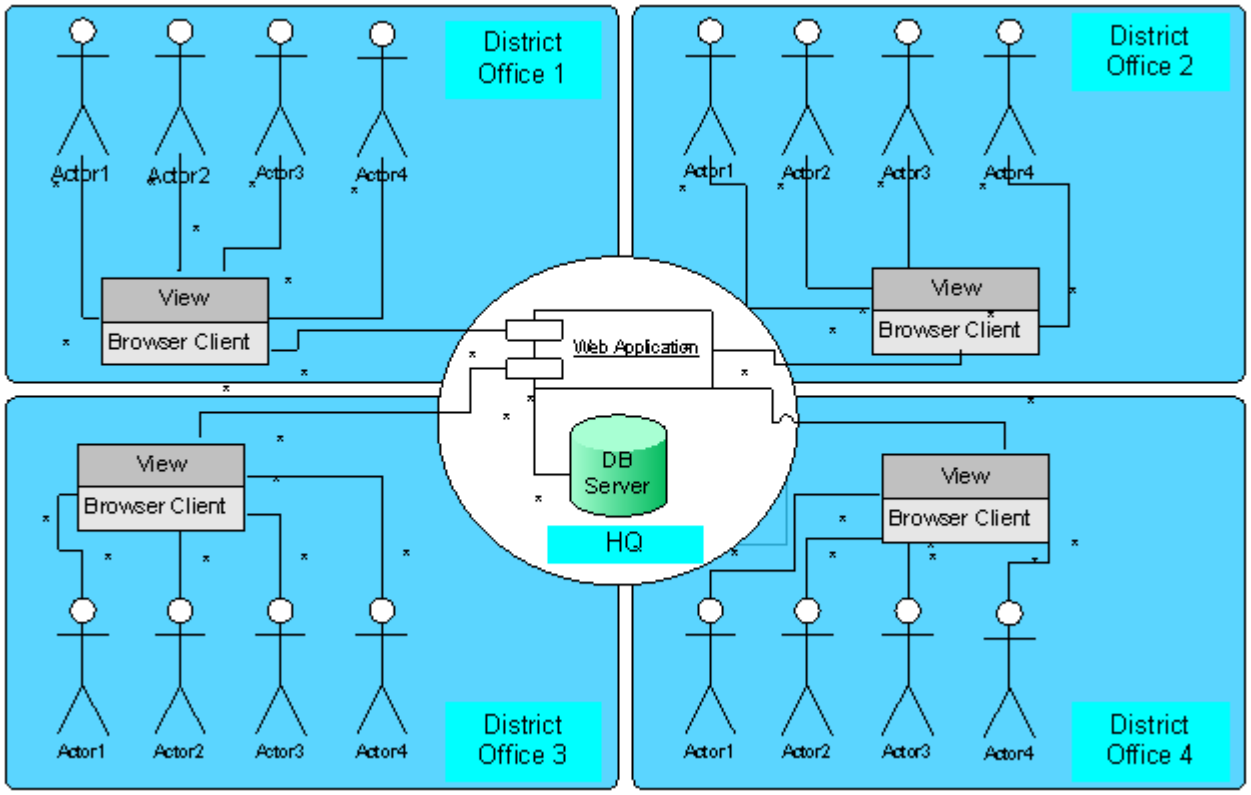
For Ex: Applications built on Oracle Developer From6 and Oracle 10g like the Criminal Record Systems of Nepal Police, DECS system of FCGO uses Oracle developer 2000 and Oracle 8i DB, Case Management Systems (For HQ only) Visual Basic Client and Oracle 10g backend,. These applications have processing logic on the client end of the application.



6.2.3.3Type 3 Applications (MVC Architecture)

The Type 3 applications are web enabled applications that 3 tier applications where the client is a browser and application resides on the web server or the application server, the call from the application server access the database server. The client-Web/Application server- Database server makes it 3 tier application. The Http requests from the browsers invoke the application components on the web/application server and the call is then routed to post a sql query on the database in the database server.

For Ex : Applications built using PHP, JSP & Java (J2EE Stack) , ASP.NET/C#(MS Stack) , and any database on the backend which could be Oracle, SQL Server, MySQL etc. Vehicle Registration system, Driving license Registration Systems of DoTM, e-PAN, e-VAT, e-TDS of IRD, PIS of DoCPR/MoGA, e-Procurement by DoR,



6.2.3.4Type 4 Applications (Hybrid Architecture)

The type 4 Applications are both client server based and web enabled applications that are required to be in this architecture due to the current infrastructure limitations across Nepal. In these type of application the field force/ District office with limited access to the connectivity to the centralized database switch to client server mode with lack of access to the central db and on obtaining connectivity switch to the online mode, by first synching up with the centralized DB and also have the features to transact online. This is a combination of Type 2 and Type 3 applications.

For Ex: Applications built using Swing client , and JSP /J2EE stack for the application server side and Oracle DB for the back end like the Citizenship certificate distribution system software from MoHA, Voters Registration Systems from Election Commission with district level application developed in C# and central level application being web based application with ASP.Net /C# being the application server side and oracle 10g being the backend server. These systems while on the Client server model has a local database on the laptop like the Oracle Express edition, on connection to the central application synchronizes with the central database.

6.2.4 Target Application Architecture

6.2.4.1 Functional View

The Functional view represents the list of all e-services from a functional perspective. We will address the functional perspective from e-services angle and these e-services would be mapping to the respective department application. This diagram represented here primarily provides a relationship of the e-services with the application through which they are made available. In this stack, the e-services are client facing. These services are made available through multiple applications in the background. These applications are made services by web service enabling the existing and new applications. The integration / Enterprise service bus is the glue to it.

Client Tier forms the list of the actors who would be interacting with the systems, it would be primarily the citizens, businesses and government themselves. Based on the roles different type of e-services would be made available. The different varieties of services are categorized into G2C (Government to Citizens), G2B(Government to Businesses) and G2G(Government to Government) services. These services are accessible to different roles based on their authorization levels.

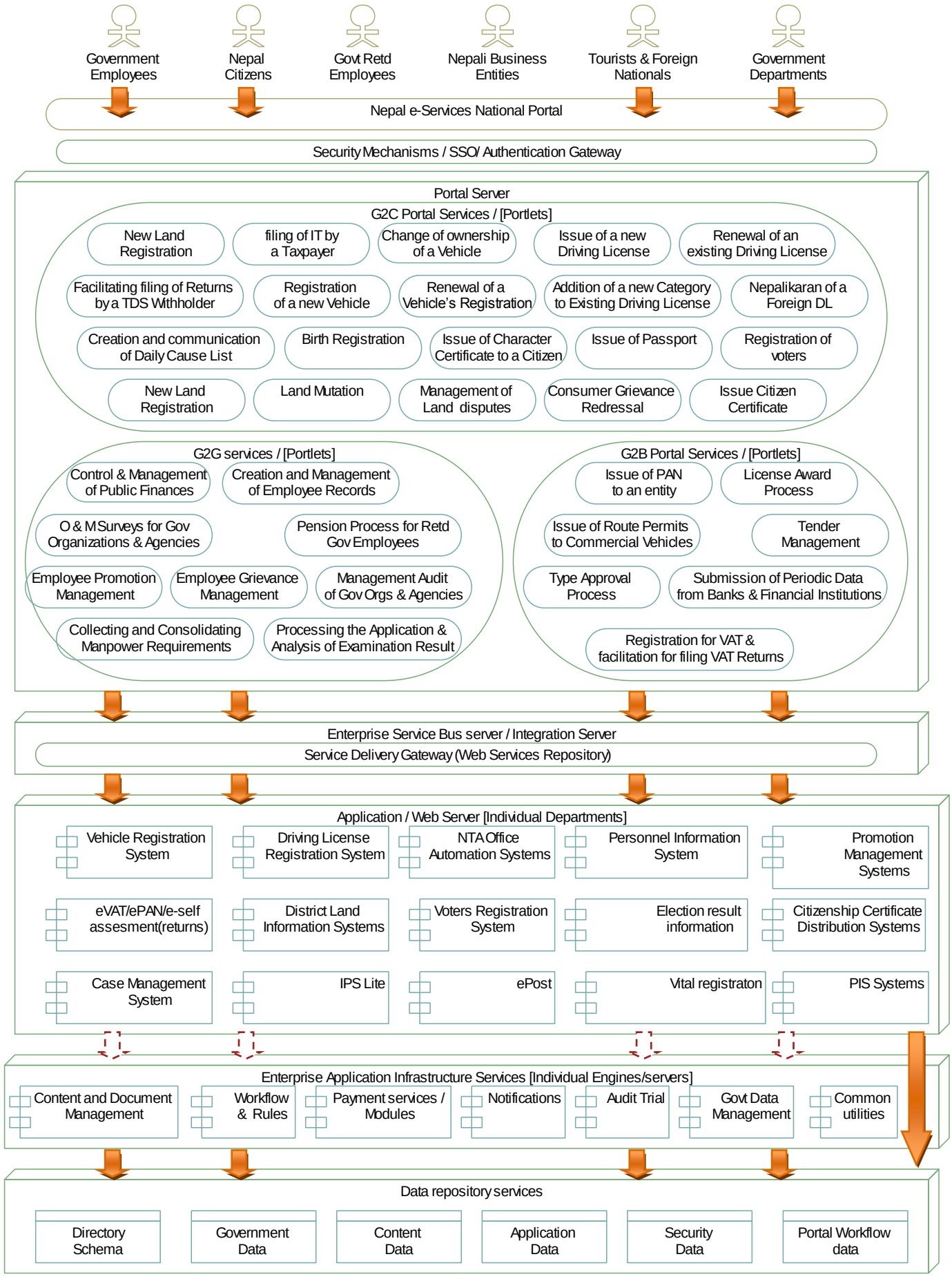
Presentation Tier is represented by the portal server which would be hosting the portlets, where each e-service would map to one or more portlets. Portlets execute in a portal Server, the clients on the system typically access the portlets to invoke e-service.

Integration Server, exposed all the web services from each application. These web services are then consumed by the portlets over the WSRP protocols. In this case the applications are the producers of the service. They register their web services on the ESB and one or more portlets could now consumer this producer web service. The web service from each producer application does not have any implementation logic on this layer. The web services on the ESB are hosted as the WSDL file that represents the service signature of a particular service.

The layer below the integration server represents individual application that could be hosted in the different location in the government departments data centres. Each application would need to expose their web services layer in the business logic level, in-order to keep the synchronicity between the direct / internal application user and the user from the portal.

The application infrastructure services layer is a generic set of application services that the application could use a set a of common application service. This layer could a host a common set of service that could be used across multiple applications.

The applications from each department would access their data from their respective databases. This layer also has databases and file repository that would include documents, files, databases that would host application data, portal data, data for the security infrastructure.


Government Employees
Nepal Citizens
Govt Retd Employees
Nepali Business Entities
Tourists & Foreign Nationals
Government Departments
Nepal e-Services National Portal
Security Mechanisms / SSO/ Authentication Gateway
Portal Server
G2C Portal Services / [Portlets]
New Land Registration
filing of IT by a Taxpayer
Change of ownership of a Vehicle
Issue of a new Driving License
Renewal of an existing Driving License
Facilitating filing of Returns by a TDS Withholder
Registration of a new Vehicle
Renewal of a Vehicle's Registration
Addition of a new Category to Existing Driving License
Nepalikaran of a Foreign DL
Creation and communication of Daily Cause List
Birth Registration
Issue of Character Certificate to a Citizen
Issue of Passport
Registration of voters
New Land Registration
Land Mutation
Management of Land disputes
Consumer Grievance Redressal
Issue Citizen Certificate
G2G services / [Portlets]
Control & Management of Public Finances
Creation and Management of Employee Records
O & M Surveys for Gov Organizations & Agencies
Pension Process for Retd Gov Employees
Employee Promotion Management
Employee Grievance Management
Management Audit of Gov Orgs & Agencies
Collecting and Consolidating Manpower Requirements
Processing the Application & Analysis of Examination Result
G2B Portal Services / [Portlets]
Issue of PAN to an entity
License Award Process
Issue of Route Permits to Commercial Vehicles
Tender Management
Type Approval Process
Submission of Periodic Data from Banks & Financial Institutions
Registration for VAT & facilitation for filing VAT Returns
Enterprise Service Bus server / Integration Server
Service Delivery Gateway (Web Services Repository)
Application / Web Server [Individual Departments]
Vehicle Registration System
Driving License Registration System
NTA Office Automation Systems
Personnel Information System
Promotion Management Systems
eVAT/ePAN/e-self assesment(returns)
District Land Information Systems
Voters Registration System
Election result information
Citizenship Certificate Distribution Systems
Case Management System
IPS Lite
ePost
Vital registraton
PIS Systems
Enterprise Application Infrastructure Services [Individual Engines/servers]
Content and Document Management
Workflow & Rules
Payment services / Modules
Notifications
Audit Trial
Govt Data Management
Common utilities
Data repository services
Directory Schema
Government Data
Content Data
Application Data
Security Data
Portal Workflow data

6.2.4.2Logical Architecture

The solution architecture for the proposed GEA infrastructure and eService portal would be based on the layered architecture approach, allocated with a different set of service components like presentation, business, security, content, workflow, integration and data access service components. Each layer would be loosely coupled with the adjacent layers providing demarcation of functionalities. Components in each layer will interact with components of neighbouring layers only. The layered approach ensures a clean division of responsibility and makes the system more scalable, flexible, maintainable and extensible with a high level of cohesion between components.

The GEA and eService portal solution will be implemented making use of the powerful capability of commercial off-the-shelf software components as well as custom developed components.

The diagram below depicts the proposed logical solution architecture in layered approach.

The diagram is not intended to show source code filenames or specific executable elements. This diagram is meant to represent a lower level of detail, interpreting components more as sub-systems. Specifically state the framework (UI, service, data access, infrastructure, and security) and design patterns implemented

Instructions: *Use the following template to architecture diagram (in Archimate form) the major actors, the services offered, the key business domain application, the data stores for each major entity, and third party software packages. All of these high level components are shown from a logical view.*

There are 2 major approaches of application architecture is represented in the following architecture diagram. The first approach is to make all the services available to the end-users through the service delivery gateway making use of the national portal. The second approach is for the internal users, who use the applications directly without going through the portal.

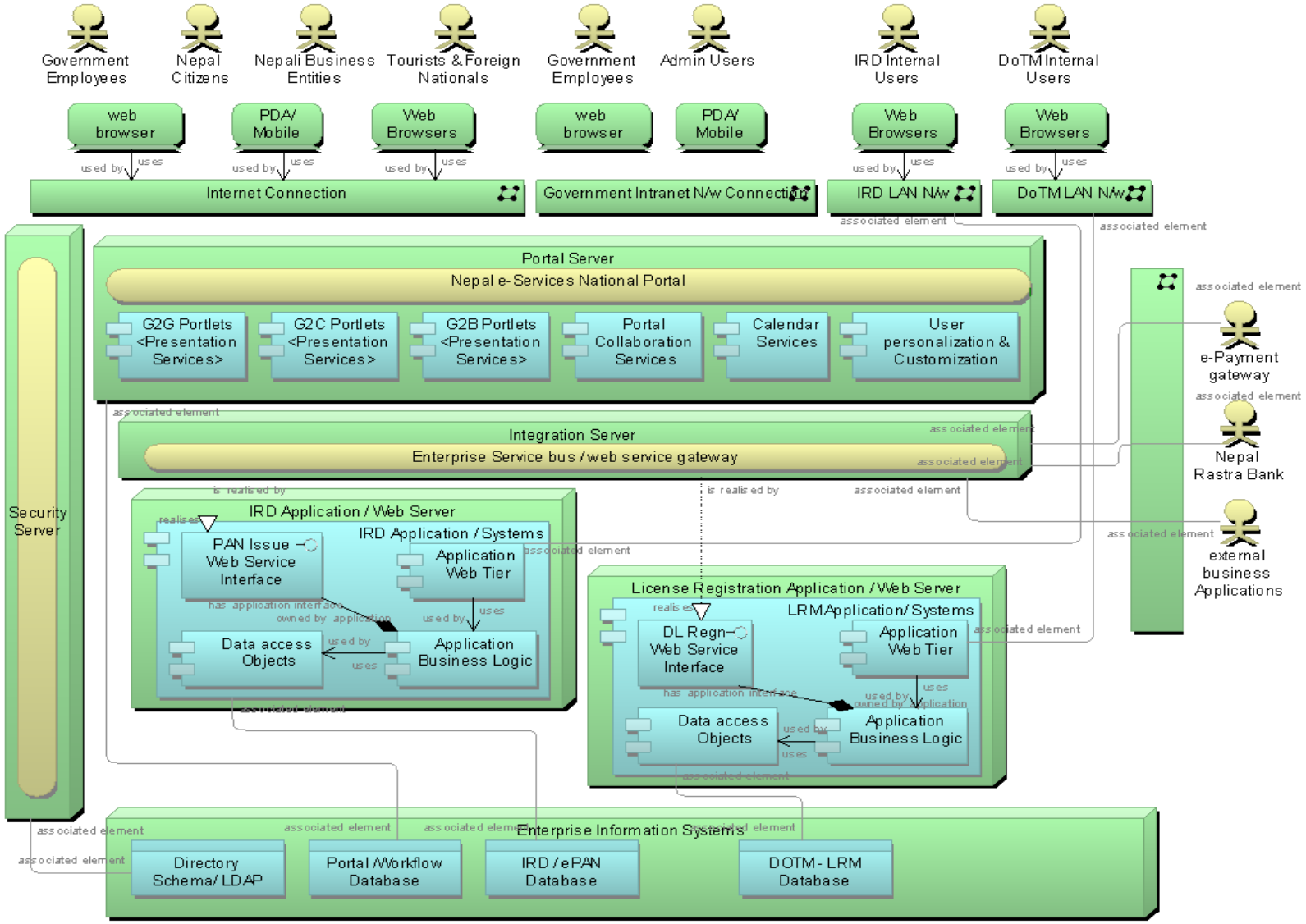
The step-wise approach for the existing applications to follow GEA Application Architecture include-

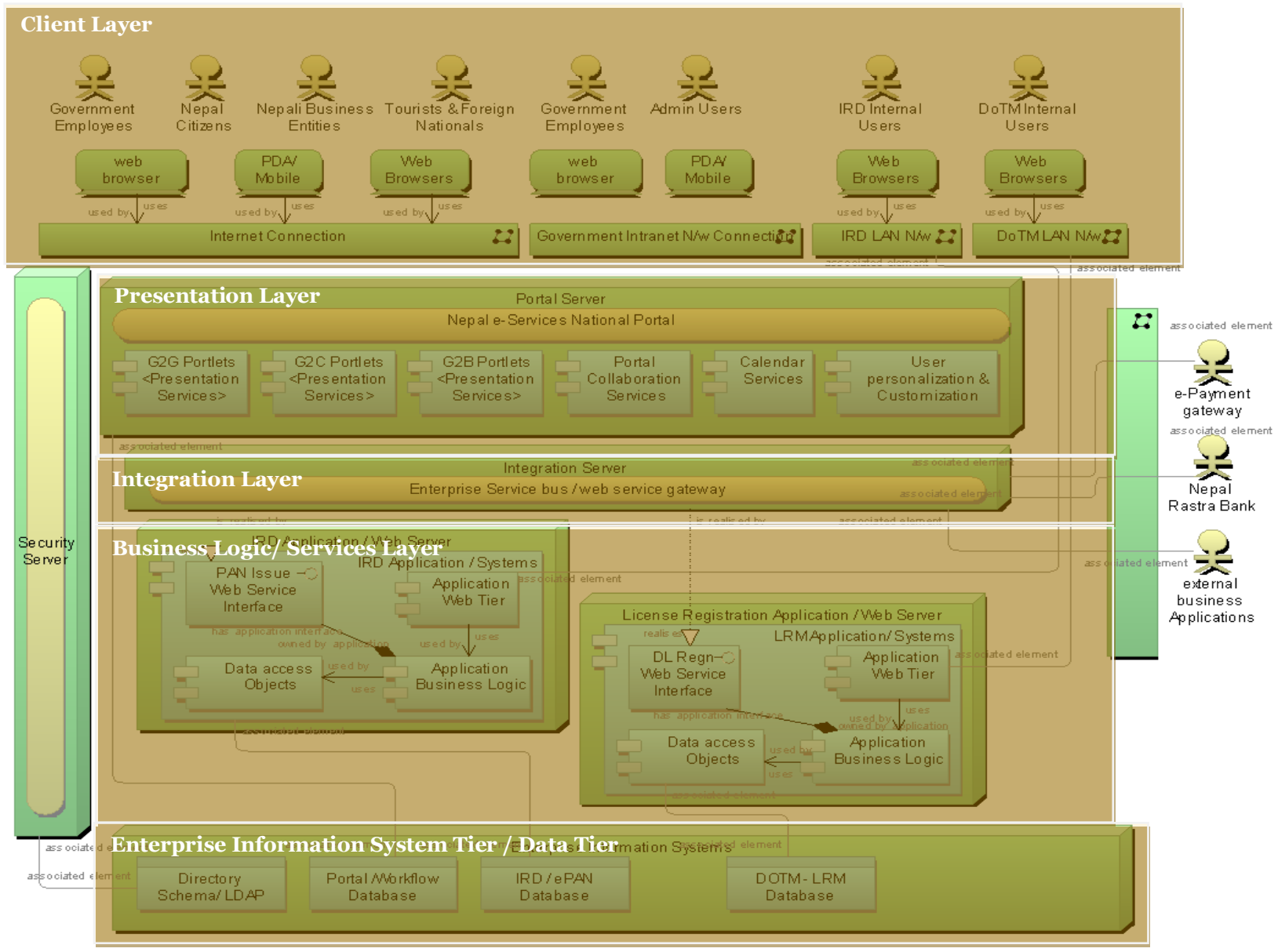
1. Identify the application type that your application represents.
2. If your type is above 2, enable the business logic as a web service.
3. Ensure the same web service that you build is used both the internal application as well as by the GEA portal through the web service.
4. The same web service would be invoked by the client tier of the internal application.

The step-wise approach for the new applications to follow GEA Application Architecture specification includes -

1. The application architecture while being architected and reviewed needs to have the clear abstracted Client tier, web tier / presentation tier, business logic layer, each business use case to be available as a web service in the business services layer and data store layer, which host the databases.
2. Once the web services for each business use case is ready, host register these web services on the ESB's registry.
3. Utilize this web service published in your internal applications, as well share it with the other consumers who are authorized to access this information.

The layers mentioned here is typically the standard approach to the future application under the e-Government initiative of Nepal. The first diagram represent the overall target application architecture without the layers, the subsequent one is represented with the layers.


Government Employees
Nepal Citizens
Nepali Business Entities
Tourists & Foreign Nationals
Government Employees
Admin Users
IRD Internal Users
DoTM Internal Users
web browser
PDA/ Mobile
Web Browsers
web browser
PDA/ Mobile
Web Browsers
Web Browsers
used by
uses
Internet Connection
Government Intranet N/w Connection
IRD LAN N/w
DoTM LAN N/w
associated element
Portal Server
Nepal e-Services National Portal
G2G Portlets <Presentation Services>
G2C Portlets <Presentation Services>
G2B Portlets <Presentation Services>
Portal Collaboration Services
Calendar Services
User personalization & Customization
Integration Server
Enterprise Service bus /web service gateway
Security Server
IRD Application / Web Server
IRD Application / Systems
PAN Issue Web Service Interface
Application Web Tier
Data access Objects
Application Business Logic
is realised by
realises
has application interface
owned by application
License Registration Application / Web Server
LRM Application/ Systems
DL Regn Web Service Interface
Application Web Tier
Data access Objects
Application Business Logic
e-Payment gateway
Nepal Rastra Bank
external business Applications
Enterprise Information Systems
Directory Schema/ LDAP
Portal /Workflow Database
IRD / ePAN Database
DOTM- LRM Database


Client Layer
Government Employees
Nepal Citizens
Nepali Business Entities
Tourists & Foreign Nationals
Government Employees
Admin Users
IRD Internal Users
DoTM Internal Users
web browser
PDA/ Mobile
Web Browsers
web browser
PDA/ Mobile
Web Browsers
Web Browsers
used by
uses
Internet Connection
Government Intranet N/w Connecti
IRD LAN N/w
DoTM LAN N/w
Presentation Layer
Portal Server
Nepal e-Services National Portal
G2G Portlets <Presentation Services>
G2C Portlets <Presentation Services>
G2B Portlets <Presentation Services>
Portal Collaboration Services
Calendar Services
User personalization & Customization
Integration Layer
Integration Server
Enterprise Service bus /web service gateway
Business Logic/ Services Layer
IRD Application /Web Server
IRD Application / Systems
PAN Issue Web Service Interface
Application Web Tier
Data access Objects
Application Business Logic
License Registration Application /Web Server
LRM Application/ Systems
DL Regn Web Service Interface
Application Web Tier
Data access Objects
Application Business Logic
Security Server
Enterprise Information System Tier / Data Tier
Directory Schema/ LDAP
Portal /Workflow Database
IRD / ePAN Database
DOTM - LRM Database
associated element
e-Payment gateway
Nepal Rastra Bank
external business Applications

The diagram above represents the following layers

1. Client Layer
2. Presentation Layer
3. Integration Layer
4. Business Logic Layer
5. Enterprise Information Systems Tier / Data Tier

6.2.4.3 National Portal Architecture

One of the key components of the Integrated Service Delivery framework is the National Portal of Nepal, which serves as the one-stop store for dissemination of relevant government information and services to all the stakeholders including citizens, business, government employee and other govt. agencies. It acts as the service delivery channel for all G2C, G2B & G2E services.

The following are the key benefits envisaged for Government of Nepal in establishment of National Level Portal Solution:

- Instantaneous access to Information related to Central Government, Its departments, Organization Structures, Contact information etc.
- Government to Business (G2B) & Government to Citizen (G2C) Informational and Transactional Services as listed in the tender document
- Interactive & Online Services (e-forms, e-payments)
- Reduction of administrative burden for Businesses & the National Government
- Increasing transparency & accountability
- Build the brand of Nepal among business community, citizens and global community

6.2.4.4 PwC eGovernance Portal Framework

PwC has developed a comprehensive eGovernance Portal Framework which takes in account most of the generic requirements of any Portal promoted by a Government Agency or Department. This framework will be leveraged for the Nepal National Portal.

PwC's eGovernance Portal Framework is based on open source Portal Framework leveraging an Enterprise Content Management System. Functionally the framework supports

- Creation and sustained maintenance of Web Content via a detailed role-based approval and authentication process
- Maintenance of Government Documents like Tenders, Notices, Forms etc.
- Customization and administration of Portlets to display information as determined by the client
- User Registration and Login
- Collaboration mechanisms like Discussion Forums and Feedback

The portal solution architecture considers the following aspects:

b. **Scalability, Reliability & Flexibility:** The technology is scalable with the emerging requirements and will continue to be reliable as the information handling needs of government increases.

c. **Ease of Development & Maintenance:** The complexity of the programming requirements for the Portal will be examined keeping in mind maintenance requirements.

d. **Total Cost of Ownership:** The framework ensures that the Total Cost of Ownership (TCO) is kept at optimal levels. This will take into account estimates for software acquisition, likely updates, initial development, training, and maintenance costs.

e. **Security:** Security is one of the prime consideration and the various technical issues to address include data integrity, confidentiality, authorization, authentication, control, compliance, prevention from unauthorized usage and audit monitoring.

f. **Open Standards:** Usage of Open standards protocols, languages and software components help protect the site and technology against redundancy, unlimited license usage and also having the advantage of inter-operability and less TCO.

g. **Ease of Integration:** The Portal may be linked to other sources (websites, contents and portals). The portal architecture has provision to integrate with evolving requirements in the future.

h. **Ease of Backup and Recovery:** The architecture considers backup/archival of static as well as transactional data which can be deployed in production as and when necessary.

i. **Rich User Experience:** The architecture considers the following related to Portal/Website GUI

- *Browser Compatibility:* Portal displays correctly in Internet Explorer and Firefox
- *Search Functionality:* Portal provides extensive search functionality which is also simple and effective to use
- *Multilingual:* The Portal framework supports contents to be available in multiple languages. However the national portal of Nepal will provide bi-lingual support in English & Nepali.

The proposed software stack is as follows:

Technology Area	Technology Platform
Operating System	Suse Linux Platform
Programming Language	Java, J2EE specification
Database	Oracle
Web Server	Apache
Application Server for Portal	JBOSS Enterprise Portal
Content Management	Alfresco Standard Edition
Workflow & BPM	JBOSS JBPM
User Management Directory Server	Red Hat Directory Server
Reporting	Jasper

6.2.5 Gap Analysis

Following are the list of gaps identified between the baseline and the target architectures.

1. Some of the applications, especially type1 applications need to be re-engineered to move it to online base applications.
2. Type 2 application those that are client server based applications also would need to be web enabled.
3. Except for few applications (like License registration Management Systems, PIS, ePAN etc) do have a clearly abstracted business logic layer. The requirement of a business logic / service is essential in order to web service enable a business logic.
4. Most of the department application would need re-engineering to integrate with the integration layer of the GEA.
5. The Network infrastructure connecting GIDC/NITC with many other departments does not exists. Since the integration layer would reside in the NITC, this would need to be connected with department applications the integration layer would connect. For ex: The Election commission is currently not network connected with NITC.
6. Application Monitoring currently does not exist.
7. Common Application Authentication and authorization does not exist.

6.2.6 Application Architecture Roadmap Components

Phase A

1. The Network infrastructure connecting GIDC/NITC with many other departments does not exists. Since the integration layer would reside in the NITC, this would need to be connected with department applications the integration layer would connect. For ex: The Election commission is currently not network connected with NITC.
2. Some of the applications, especially type1 applications need to be re-engineered to move it to online base applications.
3. Type 2 application those that are client server based applications also would need to be web enabled.

Phase B

1. Except for few applications (like License registration Management Systems, PIS, ePAN etc) do have a clearly abstracted business logic layer. The requirement of a business logic / service is essential in order to web service enable business logic.
2. Common Application Authentication and authorization needs to be deployed.
3. Most of the department application would need re-engineering to integrate with the integration layer of the GEA.

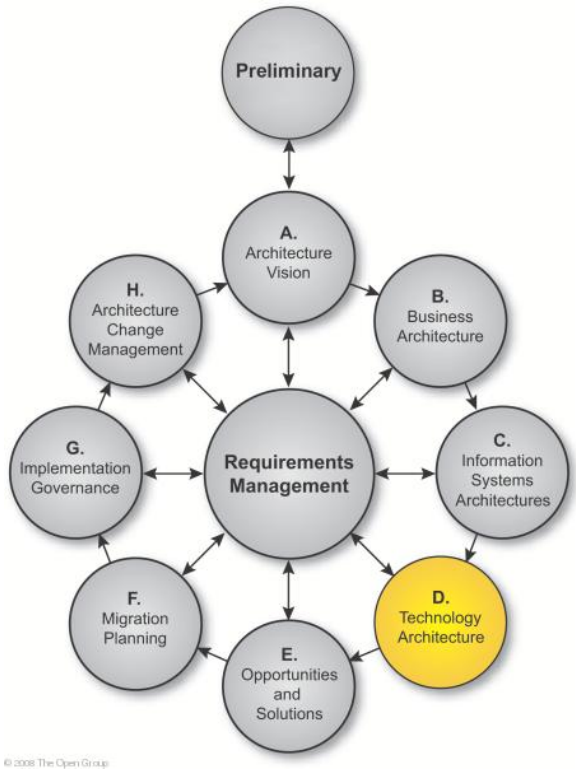
Phase C

1. Application monitoring currently capabilities can be introduced for mission critical applications to monitor the health of the systems.

Reference: For detailed description of each element in the Application Architecture refer to the GEA Enterprise Architecture continuum and Architecture repository.

7. TOGAF ADM Phase D - Technology Architecture

7. Phase D: Technology Architecture



Phase Overview

The Technology Architecture phase would aim to map data & application components defined in the Information Systems Architecture phase into a set of technology components, which represent software and hardware components, defines the physical realization of an architectural solution, which will have strong links to implementation and migration planning.

The Technology Architecture capture the following architectures

- Integration Architecture
- Security Architecture
- Infrastructure architecture

Each of the above sub categories of the technology architecture will define the technology principles, the baseline (i.e., current) and target views of the technology portfolio, identifying the gaps and detailing the roadmap components towards the Target Architecture

7.1 Technology Architecture Principles

Technical Architecture Principles *(Include integrations, infrastructure and security)*

- Interoperability
- Confidentiality
- Open standards based
- ESB based national service delivery gateway
- Web services for information exchange and granular service.
- Scalability, Availability, Backup & Archival
- Security Control Compliance, Selection & Standardization
- Levels of Security
- Security Measurement
- Use of common User Authentication Framework

7.2 Integration Architecture

7.2.1 Integration Architecture Principles

Principle # 1	
Name	Interoperability
Statement	Policies defined should reinforce & standards selected should facilitate interoperability Identify common components (including existing Government policies, standards, application, technology etc. wherever relevant) across the interoperability domain and define policies, standards, and procedures to ensure reusability of artefacts. For e.g. defining data structure, data sets at a national level etc. Choose standards that will enable more choice and reduce the administrative burden.
Rationale	• Eliminates patchwork of ICT solutions in different government offices those are unable to 'talk' or exchange data. Interoperability allows seamless exchange of information, reuse of data models and inter-changeability of data across systems • Brings in the ability to effectively interconnect, collaborate, access and facilitate data integration in order to communicate between different government organizations (G2G, G2C, and G2B etc.).

Principle # 2	
Name	Confidentiality
Statement	Guarantee the privacy of information with regard to citizens (e.g. health records), business (e.g. organization statistics) and government (e.g. confidentiality agreements) to help enforce the legally-defined restrictions on access & dissemination of information
Rationale	This will ensure that the confidential information and data are properly classified and adequately protected. Privacy cannot be guaranteed by technical standards alone, it has to have process, inter-organisational agreements, cyber laws etc. in place to enforce it. However fundamental tenet of this is to protect the integrity of government information and information held by various agencies.

Principle # 3	
Name	Open standards based
Statement	Adherence to open standards should be promoted
Rationale	• Adherence to standard that will provide for choice of vendor will promote competitiveness and opportunity to look at cross platforms. The attributes of open standards such as platform independence, vendor neutrality and ability to use across multiple implementations and the model for establishing open standards are what will allow for sustainable information exchange, interoperability, flexibility, data preservation & and greater freedom from technology and vendor lock-in

	• Adoption of open standards will facilitate storing of electronic national records and data using open data file formats.

Principle # 4	
Name	ESB based national service delivery gateway
Statement	The Enterprise Service Bus (ESB) should be the public API for the underlying implementation of the enterprise-wide Service Delivery Gateway. As a result it must be available as a resource for any service components in the enterprise. There should be loose coupling between the service and its underlying layers with the service layer acting as a façade the layer below it. Clients of the Service Delivery Gateway should have no knowledge of the various service domains below it.
Rationale	• The use of ESB promotes loose coupling, support integration of heterogeneous systems, support adherence to open standards • ESB enables rapid development, assembly & deployment of services, ease of maintenance and improved business visibility

Principle # 5	
Name	Web services for information exchange and granular service.
Statement	Web Services are to be used between the service layers. Granularity of the services composed in the ESB should not be too fine to promote a huge number of unmanageable services, where change in one results in a cascaded set of changes with the coherent others
Rationale	• By using web services to communicate between the service layers, the enterprise can create the ability to have a rationalized monitoring and security strategy for the Enterprise • Enable compliance with OASIS WS-* industry standard web service specifications of security, interoperability, reliability etc
Implications	• Governance committee working on the models of consensus, highest common factors and analysis driven frameworks should decide on the request and response payloads of the composed services

7.2.2 Baseline Integration Architecture

At iteration 1 of ADM cycle, there exists no integration between applications.

7.2.3 Target Integration Architecture

Nepal GEA Service Delivery Gateway Overview

To realize the e-Government vision of "Value Networking Nepal" to make all government services accessible to the common citizens and ensure efficiency, transparency & reliability of such services, the need to cooperate, collaborate and integrate information across different Government Departments is of utmost importance.

As part of consolidation & integration of the government services across ministry / departments a common integrated service delivery gateway was conceptualized. The proposed Nepal GEA Service Delivery Gateway (NGSDG) has been defined and designed that will act as open standard Enterprise Service Bus and provide seamless interoperability and exchange of data and events across the departments.

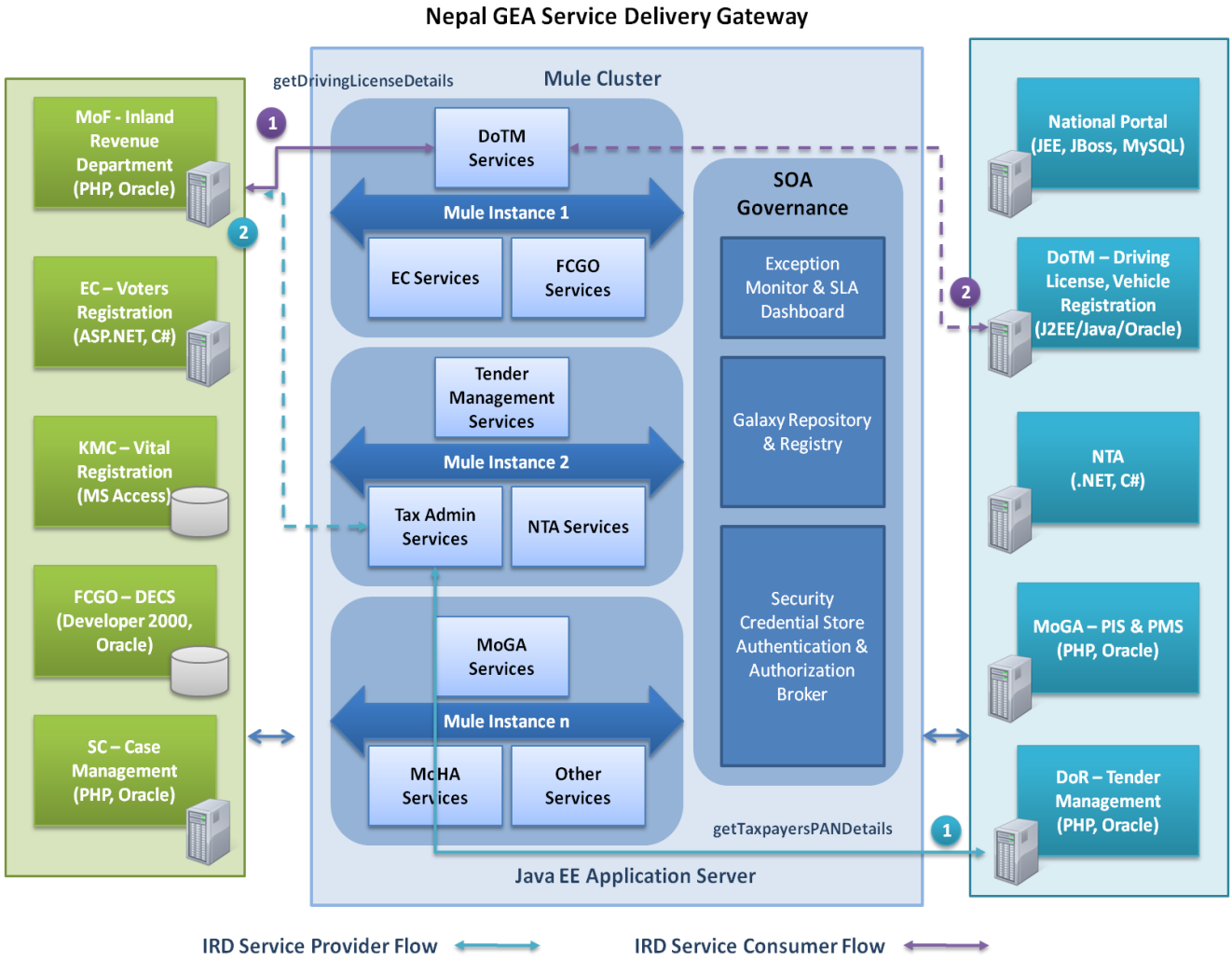
The highlights of the NGSDG is summarized below -

- NGSDG will enable a Service Oriented Architecture (SOA) and act as the Enterprise Service Bus for all the interactions between service consumers (the citizen and businesses) and various service providers (Government Departments) and even among Government Departments.
- Service enabling of Legacy Applications - With NGSDG, legacy applications can offer their services to various other consumers connected to the Enterprise Service Bus.
- Capable of handling large number of transactions across the entire network, provide a common set of specifications and a single point access.
- Security and Audit - Results in better tracking (auditing) and security of each service invocation and enforces government control through complete audit logs & time stamping of transactions
- Interoperability – The SDG Enterprise Service Bus as the middleware provides seamless interoperability and will facilitate easy exchange of data and events across the departments.
- Provide data and format transformation if any along with routing and filtering of data.
- Facilitate real time and near real time synchronization and co-ordination of inter departmental working, tracking all transactions of the Nepal Government.
- Shared Services - In future, SDG Enterprise Service Bus has the capability to add additional functionality to support shared common services like Authentication, payment gateway interface, short messaging services, instant messaging services etc.
- Provides necessary connectors to interface with the applications developed at the Department level.

The design and implementation of Government of Nepal's GEA Service Delivery Gateway is based on the open source open standard based ESB product "Mule"

ESB Topology

Nepal Government Enterprise Architecture's Service Delivery Gateway based on Mule is envisaged as a lightweight messaging framework and highly distributable object broker. In the following topology for Service Delivery Gateway, Mule services act as middlemen for the service consumer applications, taking care of invoking remote services for service provider applications. All the knowledge of the remote service is concentrated in a single place, the Mule Instance Clusters, which act as a proxy. This knowledge consists of not only connection details, but can also cover security configurations, specific data transformations, specific content based routing and filtering and service orchestrations.

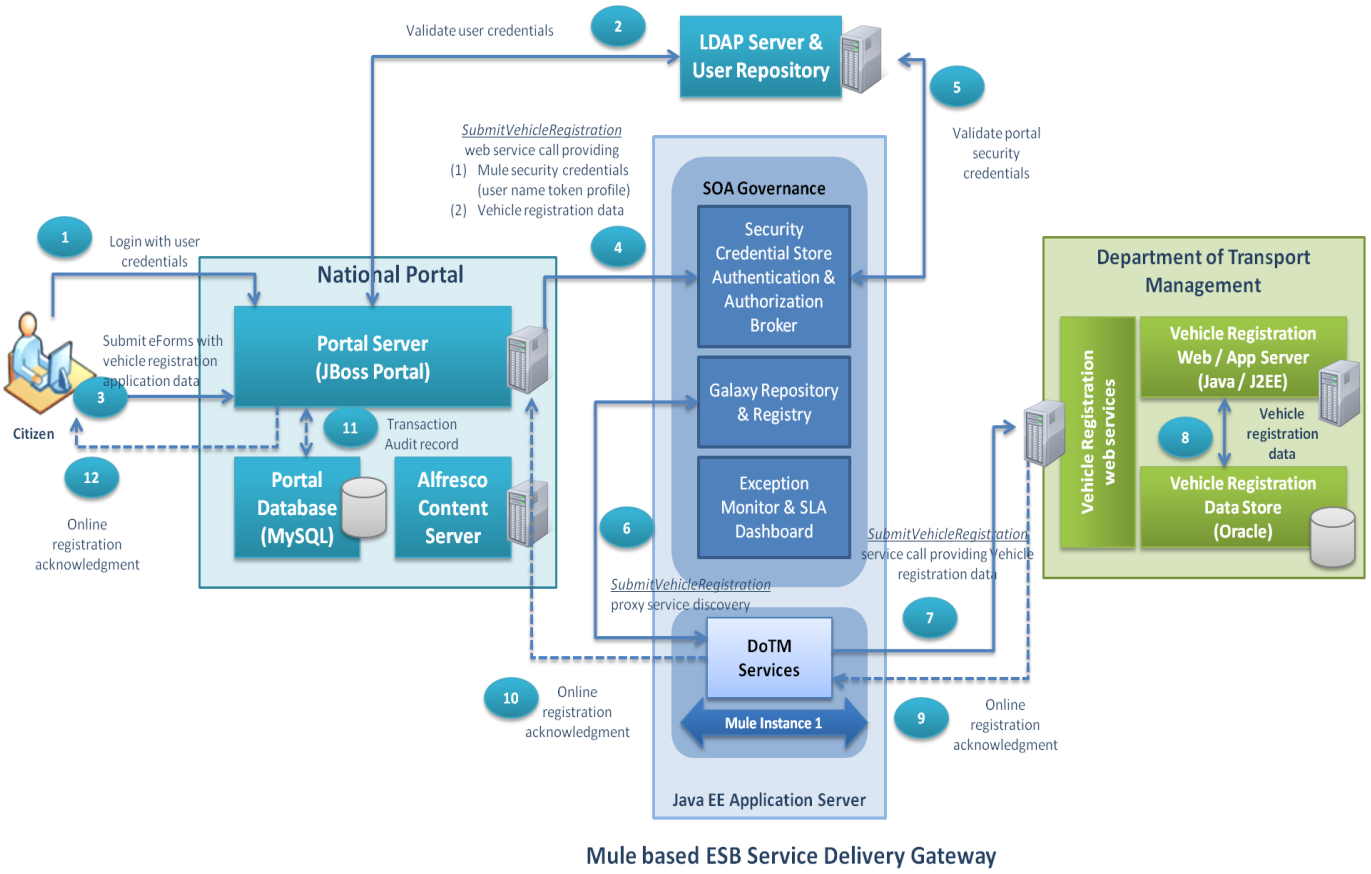


In the above topology several Mule instances will be deployed in Mule Instance Cluster to be hosted in a JEE Application Server. Each Mule instance will deploy the different set of government services. The exact government services to be deployed in each instance will be finalized during the implementation phase. However the services to be deployed in each Mule instance could be categorized based on departments or type of services e.g. citizen, business, employee etc.

To illustrate the information exchange across NGSDG, some end-to-end use case scenarios has been depicted below to demonstrate how the above ESB topology could be leveraged as the integration platform for information exchange across departments.

Use Case Scenario 1: Online Vehicle Registration Process

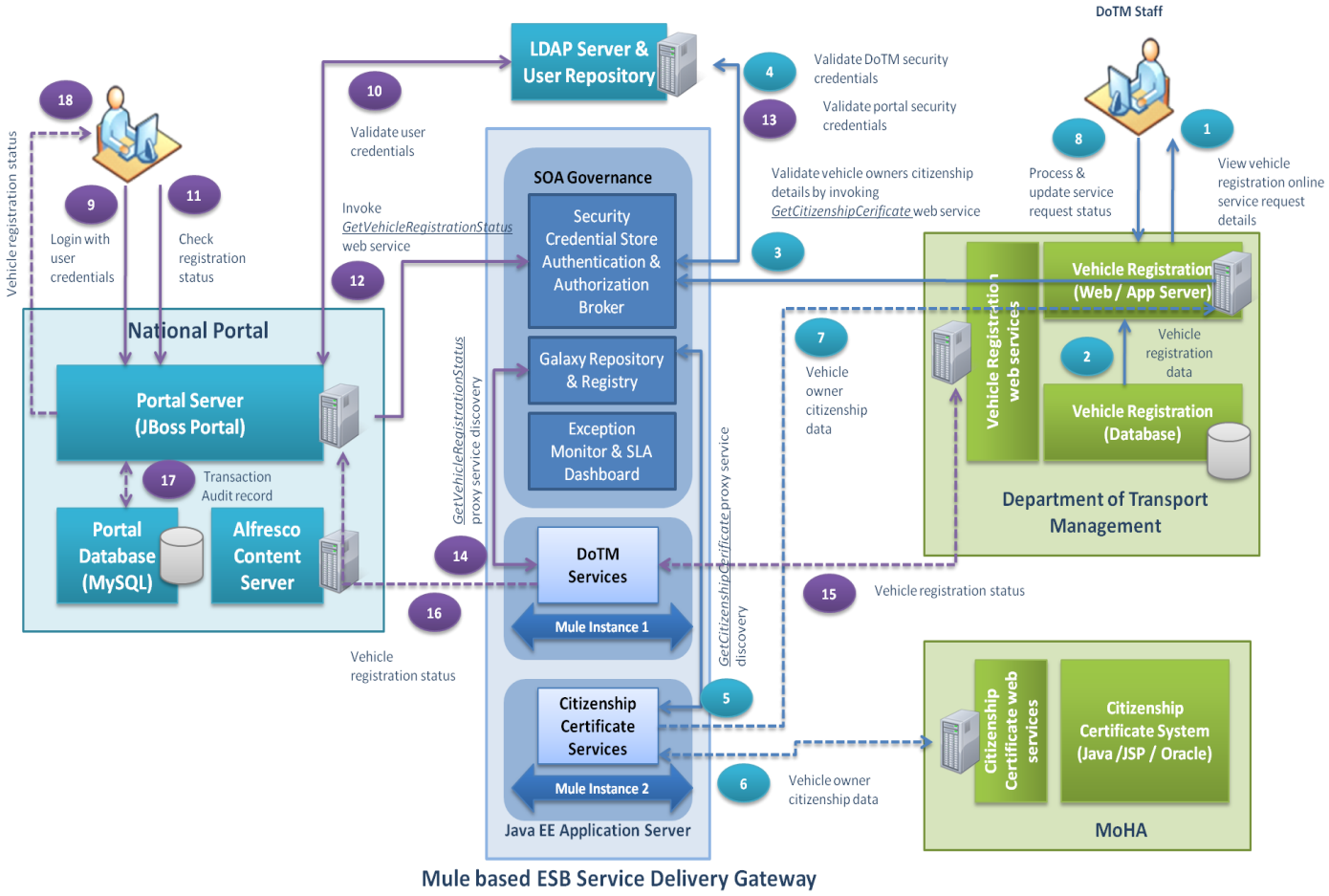
1: Citizen submits online service request for Vehicle Registration from National Portal



Step No	Step Description
1.	• Citizen logins to the National Portal with user credentials. The citizen would require to register online with the national portal prior to login through the "User Registration" option. The online user credentials provided as part of the User Registration process will be required by the citizen for login to the national portal.
2.	• The national portal authenticates the user credentials against the user repository in LDAP. • If authentication fails, the portal returns an error • If authentication is successful, the user is allowed to login to the national portal to avail the govt. e-Service
3.	• The user chooses the Department of Transport Management "Vehicle Registration" eService and opts for the online application for Vehicle Registration. • The user will be presented with the online vehicle registration form • The user fills the online form with the relevant information required and submits the online form

Step No	Step Description
4.	• After submission, the portal will convert the online form data captured into xml message format which is sent to a listening servlet running in the portal server. • The servlet will process the request and in turn invoke the "SubmitVehicleRegistration" web service to submit the information. The user name token for the portal proxy user defined will be appended as message header. • The form data and the citizen user credentials will be passed as the web service input requests and will be part of the message body. • The portal instance deployed in the GIDC will try to establish connection to the central Mule based ESB infrastructure with relevant authentication security credentials to invoke the "SubmitVehicleRegistration" web service
5.	• Mule will authenticate the user id and password provided in the user name token profile passed by the portal instance against the LDAP user repository. • If the user name token profile is not valid Mule will through an expcetion and return an error message back to the portal. • If the user name token is valid, Mule will check if the user profile is authorized to access the respective web service. If the user profile is not authorized to access the web service, Mule will return an error message back to the portal. • If the user name token profile is valid and is authorized to access the web service, Mule will continue further to process the request as mentioned in Step 6
6.	• The Mule "DoTM Services" which acts as the proxy for the underlying web service "SubmitVehicleRegistration" deployed in DoTM server will be deployed in Mule instance 1. This proxy service will be registered in the Galaxy Registry • Mule will invoke the "DoTM services" deployed in Mule instance 1 through service discovery of the already registered "SubmitVehicleRegistration" service in the Galaxy registry.
7.	• Mule proxy "DoTM Service" will establish connection with the department specific DoTM web server that hosts the vehicle registration system & the SubmitVehicleRegistration web service • The SubmitVehicleRegistration web service hosted in DoTM server will be invoked. The online request initiated from the national portal will reach the department server through the Mule based ESB service delivery gateway
8.	• The DoTM SubmitVehicleRegistration web service will process the form data provided by the citizen and store the data in the data store.
9.	• The online application acknowledgement with a reference number / application number will be returned as part of the reponse back to Mule "DoTM Service"
10.	• The Mule DoTM Service deployed in Mule instance 1 will return the response provided by the DoTM service back to the portal server
11.	• The audit details for the transaction is captured in the portal data store
12.	• The portal displays the response online to the citizen providing the reference number / application registration number for tracking the status of the online application

2: DoTM process service request for Vehicle Registration & citizen check registration status from National Portal



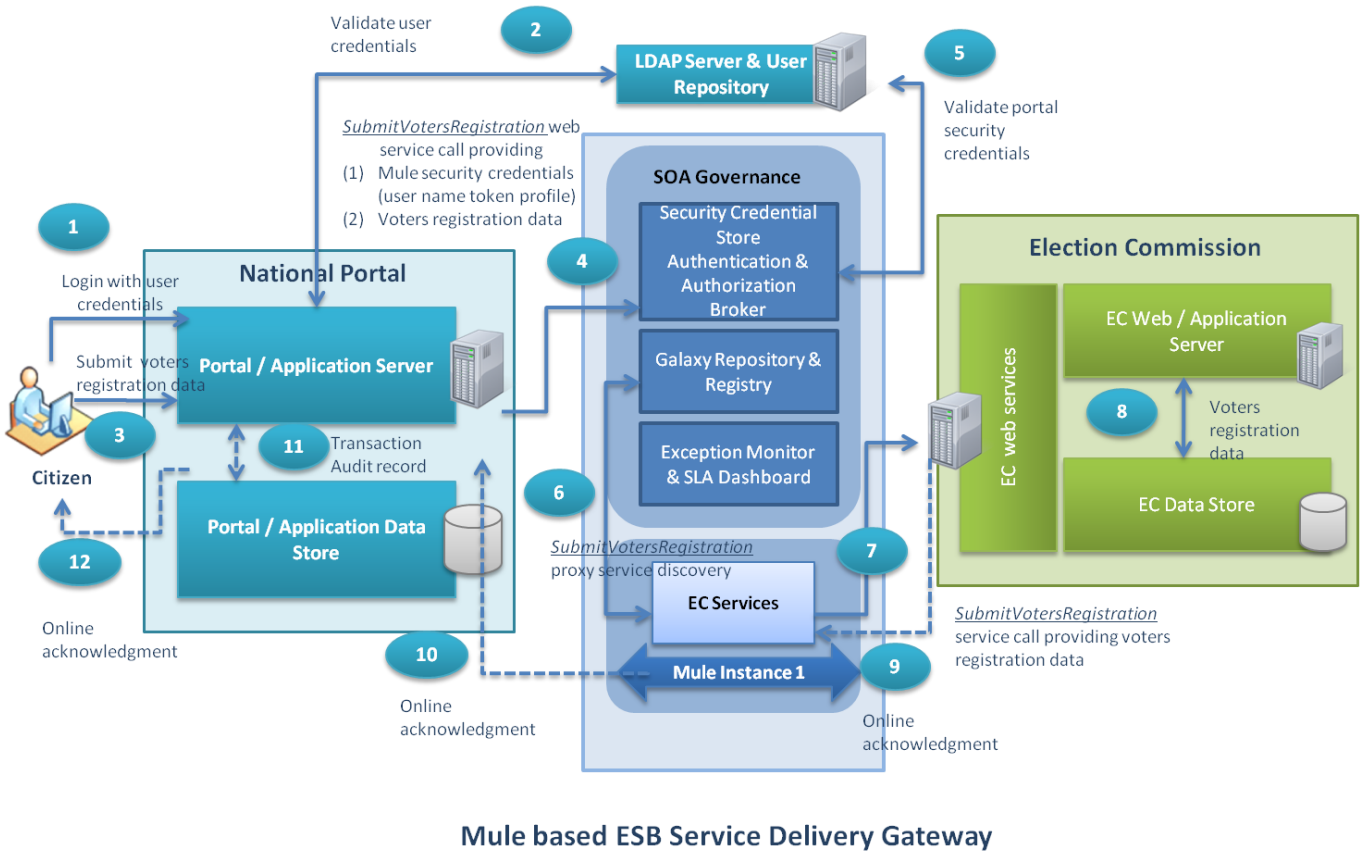
Step No	Step Description
1.	• The DoTM department staff logins in to the department specific application to view the online vehicle registration details provided by the citizen in the previous use case
2.	• The details of the service request for vehicle registration for the citizen captured in the DoTM database server is retrieved and displayed to the DoTM staff.
3.	• As part of validating the vehicle owner's citizenship data as provided by the vehicle owner, the department specific application will try to invoke the "GetCitizenshipCerificate" web service • The user name token for the DoTM proxy user defined will be appended as message header • The vehicle owner (citizen) name & citizenship number will be passed as web service input requests will be part of the message body. • The DoTM application instance deployed in the DoTM server will try to establish connection to the central Mule based ESB infrastructure with relevant authentication security credentials (user name token profile) to invoke the "GetCitizenshipCerificate" web service

Step No	Step Description
4.	• Mule will authenticate the user id and password provided in the user name token profile passed by the DoTM application instance against the LDAP user repository. • If the user name token profile is not valid Mule will through an exception and return an error message back to the DoTM application. • If the user name token is valid, Mule will check if the user profile is authorized to access the respective web service. If the user profile is not authorized to access the web service, Mule will return an error message back to the DoTM application. • If the user name token profile is valid and is authorized to access the web service, Mule will continue further to process the request
5.	• The Mule "Citizenship Certificate Services" which acts as the proxy for the underlying web service "GetCitizenshipCerificate" deployed in MoHA server will be deployed in Mule instance 2. This proxy service will be registered in the Galaxy Registry • Mule will invoke the "Citizenship Certificate Services" deployed in Mule instance 2 through service discovery of the already registered "GetCitizenshipCerificate" service in the Galaxy registry.
6.	• Mule proxy "Citizenship Certificate Services" will establish connection with the MoHA department specific server that hosts the GetCitizenshipCerificate web service • The GetCitizenshipCerificate web service hosted in MoHA server will be invoked. The online request initiated from the DoTM application will reach the MoHA department server through the Mule based ESB service delivery gateway • The web service will process the request accessing the department data store that captures the citizenship details. • If a matching record for the specific citizen name & citizenship number is found, the record is retrieved and returned as part of the output response back to Mule "Citizenship Certificate Services". • If no matching record is found, the web service will return appropriate error message.
7.	• The Mule "Citizenship Certificate Services"deployed in Mule instance 2 will return the response back to the invoking DoTM web / application server
8.	• The DoTM staff will check the response returned and will proceed further to process the vehicle registration request. • At various stages of the processing of the online service request for vehicle registration, the DoTM staff will update the status of the application.
9.	• The vehicle owner to check his online vehicle registration status will logins to the National Portal with the user credentials. The online user credentials provided as part of the User Registration process will be required by the citizen for login to the national portal.
10.	• The national portal authenticates the user credentials against the user repository in LDAP. • If authentication fails, the portal returns an error • If authentication is successful, the vehicle owner is allowed to login to the national portal to avail the govt. e-Service
11.	• The user chooses the Department of Transport Management "Vehicle Registration Status" eService option. • The user provides the online registration number & vehicle ownername and submits the request

Step No	Step Description
	to check the present status of the online registration initiated by him in the previous use case
12.	• After submission, the portal will convert the online data captured into xml message format which is sent to a listening servlet running in the portal server. • The servlet will process the request and in turn invoke the "GetVehicleRegistrationStatus" web service to submit the information. The user name token for the portal proxy user defined will be appended as message header. • The registration number and the citizen user credentials will be passed as the web service input requests and will be part of the message body. • The portal instance deployed in the GIDC will try to establish connection to the central Mule based ESB infrastructure with relevant authentication security credentials to invoke the "GetVehicleRegistrationStatus" web service
13.	• Mule will authenticate the user id and password provided in the user name token profile passed by the portal instance against the LDAP user repository. • If the user name token profile is not valid Mule will through an expcetion and return an error message back to the portal. • If the user name token is valid, Mule will check if the user profile is authorized to access the respective web service. If the user profile is not authorized to access the web service, Mule will return an error message back to the portal. • If the user name token profile is valid and is authorized to access the web service, Mule will continue further to process the request
14.	• The Mule "DoTM Services" which acts as the proxy for the underlying web service "GetVehicleRegistrationStatus" deployed in DoTM server will be deployed in Mule instance 1. This proxy service will be registered in the Galaxy Registry • Mule will invoke the "DoTM services" deployed in Mule instance 1 through service discovery of the already registered "GetVehicleRegistrationStatus" service in the Galaxy registry.
15.	• Mule proxy "DoTM Services" will establish connection with the DoTM department specific server that hosts the GetVehicleRegistrationStatus web service • The GetVehicleRegistrationStatus web service hosted in DoTM server will be invoked. The online request initiated from the national portal will reach the DoTM department server through the Mule based ESB service delivery gateway • The web service will process the request accessing the department data store that captures the vehicle registration details. • If a matching record for the specific vehicle owner name & registration number is found, the record is retrieved and returned as part of the output response back to Mule "DoTM Services". • If no matching record is found, the web service will return appropriate error message.
16.	• The Mule DoTM Service deployed in Mule instance 1 will return the response provided by the DoTM service back to the portal server
17.	• The audit details for the transaction is captured in the portal data store
18.	• The portal displays the response back to the citizen with the update of the status if any.

Use Case Scenario 2: Online Voter's Registration Process

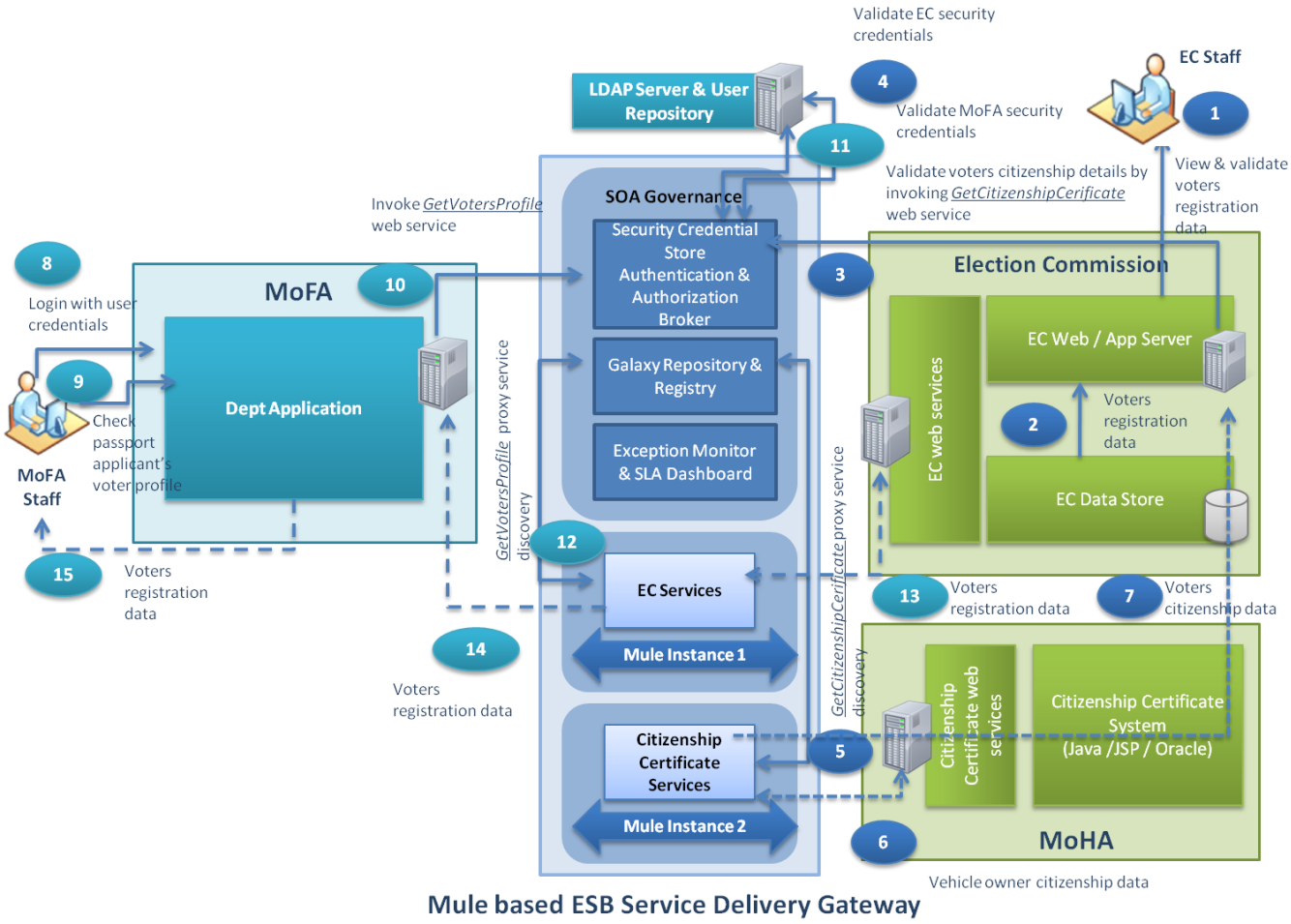
1: Citizen submits online service request for Voter's Registration from National Portal



Step No	Step Description
1.	• Citizen logins to the National Portal with user credentials. The citizen would require to register online with the national portal prior to login through the "User Registration" option. The online user credentials provided as part of the User Registration process will be required by the citizen for login to the national portal.
2.	• The national portal authenticates the user credentials against the user repository in LDAP. • If authentication fails, the portal returns an error • If authentication is successful, the user is allowed to login to the national portal to avail the govt. e-Service
3.	• The user chooses the Election Commission "Voters Registration" eService and opts for the online application for Voter's Registration. • The user will be presented with the online voters registration form • The user fills the online form with the relevant information required and submits the online form

Step No	Step Description
4.	• After submission, the portal will convert the online form data captured into xml message format which is sent to a listening servlet running in the portal server. • The servlet will process the request and in turn invoke the "SubmitVotersRegistration" web service to submit the information. The user name token for the portal proxy user defined will be appended as message header. • The form data and the citizen user credentials will be passed as the web service input requests and will be part of the message body. • The portal instance deployed in the GIDC will try to establish connection to the central Mule based ESB infrastructure with relevant authentication security credentials to invoke the "SubmitVotersRegistration" web service
5.	• Mule will authenticate the user id and password provided in the user name token profile passed by the portal instance against the LDAP user repository. • If the user name token profile is not valid Mule will through an exception and return an error message back to the portal. • If the user name token is valid, Mule will check if the user profile is authorized to access the respective web service. If the user profile is not authorized to access the web service, Mule will return an error message back to the portal. • If the user name token profile is valid and is authorized to access the web service, Mule will continue further to process the request as mentioned in Step 6
6.	• The Mule "EC Services" which acts as the proxy for the underlying web service "SubmitVotersRegistration" deployed in EC server will be deployed in Mule instance 1. This proxy service will be registered in the Galaxy Registry • Mule will invoke the "EC services" deployed in Mule instance 1 through service discovery of the already registered "SubmitVotersRegistration" service in the Galaxy registry.
7.	• Mule proxy "EC Service" will establish connection with the department specific EC web server that hosts the voters registration system & the SubmitVotersRegistration web service • The SubmitVotersRegistration web service hosted in EC server will be invoked. The online request initiated from the national portal will reach the department server through the Mule based ESB service delivery gateway
8.	• The EC SubmitVotersRegistration web service will process the form data provided by the citizen and store the data in the data store.
9.	• The online application acknowledgement with a reference number / application number will be returned as part of the reponse back to Mule "EC Service"
10.	• The Mule EC Service deployed in Mule instance 1 will return the response provided by the EC service back to the portal server
11.	• The audit details for the transaction is captured in the portal data store
12.	• The portal displays the response online to the citizen providing the reference number / application registration number for tracking the status of the online application

2: EC process service request for Voters Registration & MoFA staff checks voters profile



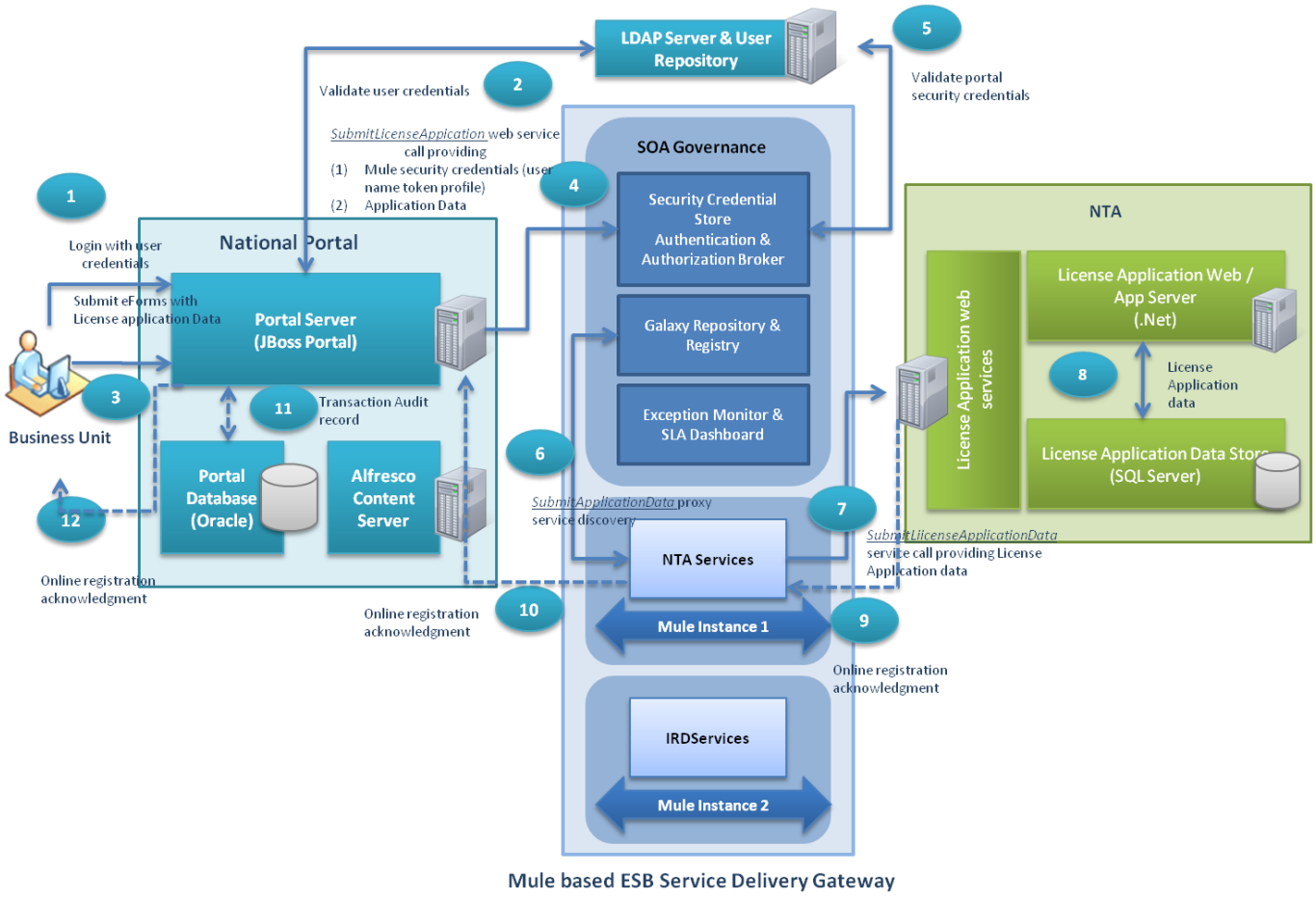
Step No	Step Description
1.	• The EC department staff logins in to the department specific application to view the online voters registration details provided by the citizen in the previous use case
2.	• The details of the service request for voters registration for the citizen captured in the EC database server is retrieved and displayed to the EC staff.
3.	• As part of validating the voters citizenship data as provided by the citizen, the department specific application will try to invoke the "GetCitizenshipCerificate" web service • The user name token for the EC proxy user defined will be appended as message header • The citizen name & citizenship number will be passed as web service input requests will be part of the message body. • The EC application instance deployed in the EC server will try to establish connection to the central Mule based ESB infrastructure with relevant authentication security credentials (user name token profile) to invoke the "GetCitizenshipCerificate" web service

Step No	Step Description
4.	• Mule will authenticate the user id and password provided in the user name token profile passed by the EC application instance against the LDAP user repository. • If the user name token profile is not valid Mule will through an exception and return an error message back to the EC application. • If the user name token is valid, Mule will check if the user profile is authorized to access the respective web service. If the user profile is not authorized to access the web service, Mule will return an error message back to the EC application. • If the user name token profile is valid and is authorized to access the web service, Mule will continue further to process the request
5.	• The Mule "Citizenship Certificate Services" which acts as the proxy for the underlying web service "GetCitizenshipCerificate" deployed in MoHA server will be deployed in Mule instance 2. This proxy service will be registered in the Galaxy Registry • Mule will invoke the "Citizenship Certificate Services" deployed in Mule instance 2 through service discovery of the already registered "GetCitizenshipCerificate" service in the Galaxy registry.
6.	• Mule proxy "Citizenship Certificate Services" will establish connection with the MoHA department specific server that hosts the GetCitizenshipCerificate web service • The GetCitizenshipCerificate web service hosted in MoHA server will be invoked. The online request initiated from the EC application will reach the MoHA department server through the Mule based ESB service delivery gateway • The web service will process the request accessing the department data store that captures the citizenship details. • If a matching record for the specific citizen name & citizenship number is found, the record is retrieved and returned as part of the output response back to Mule "Citizenship Certificate Services". • If no matching record is found, the web service will return appropriate error message.
7.	• The Mule "Citizenship Certificate Services"deployed in Mule instance 2 will return the response back to the invoking EC web / application server
8.	• A MoFA Staff logins in to the MoFA department specific application with the user credentials to check the voters profile of the passport application.
9.	• The MoFA staff chooses the option to check the voters profile of the passport applicant & submits the request
10.	• As part of getting the voters profile data, the department specific application will try to invoke the "GetVotersProfile" web service • The user name token for the MoFA proxy user defined will be appended as message header • The MoFA application instance deployed in the MoFA server will try to establish connection to the central Mule based ESB infrastructure with relevant authentication security credentials (user name token profile) to invoke the "GetVotersProfile" web service
11.	• Mule will authenticate the user id and password provided in the user name token profile passed by the MoFA application instance against the LDAP user repository. • If the user name token profile is not valid Mule will through an exception and return an error message back to the MoFA application.

Step No	Step Description
	• If the user name token is valid, Mule will check if the user profile is authorized to access the respective web service. If the user profile is not authorized to access the web service, Mule will return an error message back to the MoFA application. • If the user name token profile is valid and is authorized to access the web service, Mule will continue further to process the request
12.	• The Mule "EC Services" which acts as the proxy for the underlying web service "GetVotersProfile" deployed in EC server will be deployed in Mule instance 1. This proxy service will be registered in the Galaxy Registry • Mule will invoke the "EC Services" deployed in Mule instance 1 through service discovery of the already registered "GetVotersProfile" service in the Galaxy registry.
13.	• Mule proxy "EC Services" will establish connection with the EC department specific server that hosts the GetVotersProfile web service • The GetVotersProfile web service hosted in EC server will be invoked. The online request initiated from the MoFA application will reach the EC department server through the Mule based ESB service delivery gateway • The web service will process the request accessing the department data store that captures the voters profile details
14.	• The Mule "EC Services"deployed in Mule instance 1 will return the response back to the invoking MoFA web / application server
15.	• The voters registration data is displayed to the MoFA staff

Use Case Scenario 3: Online VAS License Registration Process

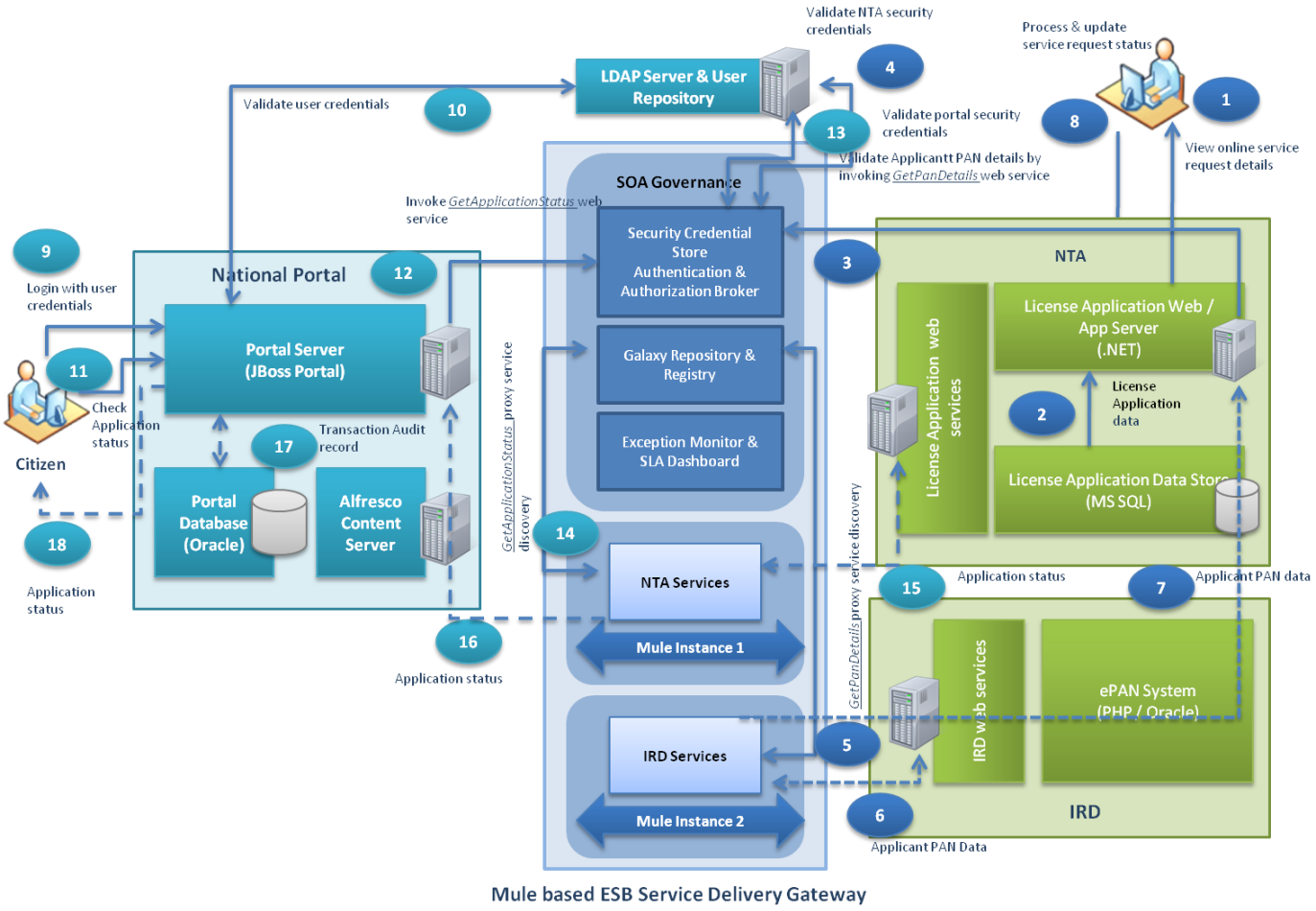
1: Business submits online service request for VAS License Registration from National Portal



Step No	Step Description
1.	• Business logins to the National Portal with user credentials. The business would require to register online with the national portal prior to login through the "User Registration" option. The online user credentials provided as part of the User Registration process will be required by the citizen for login to the national portal.
2.	• The national portal authenticates the user credentials against the user repository in LDAP. • If authentication fails, the portal returns an error • If authentication is successful, the user is allowed to login to the national portal to avail the govt. e-Service
3.	• The user chooses the NTA "VAS License Registration" eService and opts for the online application for VAS License Registration. • The user will be presented with the online license registration form • The user fills the online form with the relevant information required and submits the online form
4.	• After submission, the portal will convert the online form data captured into xml message format which is sent to a listening servlet running in the portal server. • The servlet will process the request and in turn invoke the "SubmitLicenseApplication" web service to submit the information. The user name token for the portal proxy user defined will be appended as message header.

Step No	Step Description
	• The form data and the business user credentials will be passed as the web service input requests and will be part of the message body. • The portal instance deployed in the GIDC will try to establish connection to the central Mule based ESB infrastructure with relevant authentication security credentials to invoke the "SubmitLicenseApplication" web service
5.	• Mule will authenticate the user id and password provided in the user name token profile passed by the portal instance against the LDAP user repository. • If the user name token profile is not valid Mule will through an expcetion and return an error message back to the portal. • If the user name token is valid, Mule will check if the user profile is authorized to access the respective web service. If the user profile is not authorized to access the web service, Mule will return an error message back to the portal. • If the user name token profile is valid and is authorized to access the web service, Mule will continue further to process the request as mentioned in Step 6
6.	• The Mule "NTA Services" which acts as the proxy for the underlying web service "SubmitLicenseApplication" deployed in NTA server will be deployed in Mule instance 1. This proxy service will be registered in the Galaxy Registry • Mule will invoke the "NTA services" deployed in Mule instance 1 through service discovery of the already registered "SubmitLicenseApplication" service in the Galaxy registry.
7.	• Mule proxy "NTA Service" will establish connection with the department specific NTA web server that hosts the VAS license registration system & the SubmitLicenseApplication web service • The SubmitLicenseApplication web service hosted in NTA server will be invoked. The online request initiated from the national portal will reach the department server through the Mule based ESB service delivery gateway
8.	• The NTA SubmitLicenseApplication web service will process the form data provided by the business and store the data in the data store.
9.	• The online application acknowledgement with a reference number / application number will be returned as part of the reponse back to Mule "NTA Service"
10.	• The Mule NTA Service deployed in Mule instance 1 will return the response provided by the DoTM service back to the portal server
11.	• The audit details for the transaction is captured in the portal data store
12.	• The portal displays the response online to the business providing the reference number / application registration number for tracking the status of the online application

2: NTA process service request for VAS License Registration & citizen check registration status from National Portal



Step No	Step Description
1.	• The NTA department staff logins in to the department specific application to view the online VAS license registration details provided by the business in the previous use case
2.	• The details of the service request for license registration for the business captured in the NTA database server is retrieved and displayed to the NTA staff.
3.	• As part of validating the business's PAN data as provided by the business, the department specific application will try to invoke the "GetPANDetails" web service • The user name token for the NTA proxy user defined will be appended as message header • The NTA application instance deployed in the NTA server will try to establish connection to the central Mule based ESB infrastructure with relevant authentication security credentials (user name token profile) to invoke the "GetPANDetails" web service

Step No	Step Description
4.	• Mule will authenticate the user id and password provided in the user name token profile passed by the NTA application instance against the LDAP user repository. • If the user name token profile is not valid Mule will through an exception and return an error message back to the NTA application. • If the user name token is valid, Mule will check if the user profile is authorized to access the respective web service. If the user profile is not authorized to access the web service, Mule will return an error message back to the NTA application. • If the user name token profile is valid and is authorized to access the web service, Mule will continue further to process the request
5.	• The Mule "IRD Services" which acts as the proxy for the underlying web service "GetPANDetails" deployed in IRD server will be deployed in Mule instance 2. This proxy service will be registered in the Galaxy Registry • Mule will invoke the "IRD Services" deployed in Mule instance 2 through service discovery of the already registered "GetPANDetails" service in the Galaxy registry.
6.	• Mule proxy "IRD Services" will establish connection with the IRD department specific server that hosts the GetPANDetails web service • The GetPANDetails web service hosted in IRD server will be invoked. The online request initiated from the NTA application will reach the IRD department server through the Mule based ESB service delivery gateway • The web service will process the request accessing the department data store that captures the business PAN details.
7.	• The Mule "IRD Services"deployed in Mule instance 2 will return the response back to the invoking NTA web / application server
8.	• The NTA staff will check the response returned and will proceed further to process the VAS license registration request. • At various stages of the processing of the online service request for license registration, the NTA staff will update the status of the application.
9.	• The business to check their online license registration status will logins to the National Portal with the user credentials. The online user credentials provided as part of the User Registration process will be required by the business for login to the national portal.
10.	• The national portal authenticates the user credentials against the user repository in LDAP. • If authentication fails, the portal returns an error • If authentication is successful, thebusiness user is allowed to login to the national portal to avail the govt. e-Service
11.	• The user chooses the NTA "VAS License Registration Status" eService option. • The user provides the online registration number & business name/registration number and submits the request to check the present status of the online registration initiated in the previous use case
12.	• After submission, the portal will convert the online data captured into xml message format which is sent to a listening servlet running in the portal server. • The servlet will process the request and in turn invoke the "GetVASApplicationStatus" web service

Step No	Step Description
	to submit the information. The user name token for the portal proxy user defined will be appended as message header. • The search criteria and the citizen user credentials will be passed as the web service input requests and will be part of the message body. • The portal instance deployed in the GIDC will try to establish connection to the central Mule based ESB infrastructure with relevant authentication security credentials to invoke the "GetVASApplicationStatus" web service
13.	• Mule will authenticate the user id and password provided in the user name token profile passed by the portal instance against the LDAP user repository. • If the user name token profile is not valid Mule will through an expcetion and return an error message back to the portal. • If the user name token is valid, Mule will check if the user profile is authorized to access the respective web service. If the user profile is not authorized to access the web service, Mule will return an error message back to the portal. • If the user name token profile is valid and is authorized to access the web service, Mule will continue further to process the request
14.	• The Mule "NTA Services" which acts as the proxy for the underlying web service "GetVASApplicationStatus" deployed in NTA server will be deployed in Mule instance 1. This proxy service will be registered in the Galaxy Registry • Mule will invoke the "NTA services" deployed in Mule instance 1 through service discovery of the already registered "GetVASApplicationStatus" service in the Galaxy registry.
15.	• Mule proxy "NTA Services" will establish connection with the NTA department specific server that hosts the GetVASApplicationStatus web service • The GetVASApplicationStatus web service hosted in NTA server will be invoked. The online request initiated from the national portal will reach the NTA department server through the Mule based ESB service delivery gateway • The web service will process the request accessing the department data store that captures the license registration details
16.	• The Mule NTA Service deployed in Mule instance 1 will return the response provided by the NTA service back to the portal server
17.	• The audit details for the transaction is captured in the portal data store
18.	• The portal displays the response back to the business with the update of the status if any.

7.2.4 Gap Analysis

The Gap is the target itself with the absence of any integration between departments and platforms.

7.2.5 Integration Architecture Roadmap

The High level roadmap represents the sequence in it's priority of implementing the design consideration. The phases mentioned here are subjected different timelines as per the client's strategic plans. These are jus a sequential phases of implementation.

Phase A

1. NGSDG will enable a Service Oriented Architecture (SOA) and act as the Enterprise Service Bus for all the interactions between service consumers (the citizen and businesses) and various service providers (Government Departments) and even among Government Departments. The SDG Enterprise Service Bus as the middleware provides seamless interoperability and will facilitate easy exchange of data and events across the departments
2. Service enabling of Legacy Applications - With NGSDG, legacy applications can offer their services to various other consumers connected to the Enterprise Service Bus.
3. Provide a common set of integration specifications and a single point access.
4. Security and Audit - Results in better tracking (auditing) and security of each service invocation and enforces government control through complete audit logs & time stamping of transactions

Phase B

1. Provides necessary connectors to interface with the applications developed at the Department level.
2. Capable of handling large number of transactions across the entire network,
3. Provide data and format transformation if any along with routing and filtering of data.
4. Facilitate real time and near real time synchronization and co-ordination of inter departmental working, tracking all transactions of the Nepal Government.

Phase C

1. Shared Services - In future, SDG Enterprise Service Bus has the capability to add additional functionality to support shared common services like Authentication, payment gateway interface, short messaging services, instant messaging services etc.

Reference: For detailed description of each element in the Integration Architecture refer to the GEA Enterprise Architecture continuum and Architecture repository.

Refer to the "Nepal GEA - SOA ESB Design Guidelines" & "Nepal GEA - SOA Development Guidelines" for detailed information pertaining to Integration Architecture

7.3 Security Architecture

7.3.1 Security Architecture Principles

Principle # 1	
Name	Security Control Compliance, Selection & Standardization

Statement	Security controls should be compliant with the pre-defined security policies. The selection of security controls should be based on a risk analysis and risk management decision. The process for selecting new controls will consider both the degree of risk mitigation provided by the control and the total cost to acquire, implement and maintain the control. Selection of controls should be driven by the ability of the control to be applied uniformly across the enterprise and to minimize exceptions.
Rationale	• Achieving a standards-based environment will reduce operational costs, improve interoperability and improve supportability • Ensures security solutions are fit-for-purpose • Avoids breaches of confidentiality
Implications	IT security policy, data security policy and application security should be developed for all phase

Principle # 2	
Name	Levels of Security
Statement	Information systems (including applications, computing platforms, data and networks) will maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure or modification of information.
Rationale	In practical sense perfect security cannot be achieved in any information system. Therefore, security controls will be applied to reduce risk to an acceptable level.
Implications	Separate centralized teams need to be formed for Application, data and IT Security. A repository needs to be maintained for this.

Principle # 3	
Name	Security Measurement
Statement	Security controls will be able to be reviewed or audited through some qualitative or quantitative means for traceability and to ensure that risk is being maintained at acceptable levels.
Rationale	Allows errors to be corrected and system misuse to be minimised
Implications	A reporting structure needs to be defined and management should be able to see a consolidated report

Principle # 4	
Name	Use of common User Authentication
Statement	Use of a common User Authentication framework at all levels of the GEA must be supported. This includes reuse of the same authentication framework for national portal

	login and registering services on the bus, for both consumers and producers.
Rationale	• Allows easy access to authorised users • This approach avoids duplication of effort and achieves economies of scale
Implications	Centralized authentication mechanism needs to be developed. Existing application needs to be changed so that they can use the centralized model.

7.3.2 Baseline Security Architecture

The purpose of Security Architecture Framework is to support organizations and administrators to provide electronic services to businesses and citizens, by appropriate selection mechanisms for authentication and registration of users. The adoption of directives and guidelines of the Security Framework will improve the level of safety of services provided by public administration bodies, allowing improve the overall functioning of the Government. The Security Framework is an important aspect of the strategy of the Government of Nepal for transition and adaptation of services to meet the requirements of the current industry standards. In the current scenario in Nepal the there is no uniform security policy that is being followed across the departments.

7.3.3 Target Security Architecture

Government of Nepal is being driven to change business approaches by many factors both internally and externally. To support this growth and change, security must be integrated into business processes. Based upon security trends, as well as analysis and observations of Government of Nepal current state, Government of Nepal must formulate a consistent approach to build information security within the environment.

To meet the needs of enterprise security, the Government of Nepal security architecture provides the basic framework for approaching security while maintaining consistency across the enterprise. The main objectives of the ESA are to:

- Define the security dimensions
- Focus security efforts to ensure the proper controls are implemented to adequately protect information assets based on business drivers;
- Create a security community within the organization with a common vernacular and approach;
- Create a structure around security to integrate it into the overall business context; and
- Provide a prioritized road map for business units to progress towards this overall model.

Enterprise Security Architecture transforms business objectives into the people, processes and technology components necessary to secure information protect assets and provide Government of Nepal with a structured, business focused security program.

The ESA provides a common point of reference as business units address the issues within their operations. The ESA is comprised of specific criteria for each business unit to identify areas of focus, roles and responsibilities to support the overall security function and a strategic migration approach. Additionally, the ESA showcases the fact information security is not solely a technology issue. There is no silver bullet technical solution to implement security architecture in an enterprise as large as Government of Nepal. To reach full maturity, technology must be combined with effective processes and skilled people.

Broadly the security dimensions can be broken into five different sections

- Security Policy: Information Technology Security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction,

modification, or disruption. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

- Data Security: In simple terms, data security is the practice of keeping data protected from corruption and unauthorized access. The focus behind data security is to ensure privacy while protecting data. Data is considered a primary asset and as such must be protected in a manner commensurate to its value. Security and privacy must focus on controlling unauthorized access to data. Security compromises or privacy violations could jeopardize our ability to provide service; lose revenue through fraud or destruction of proprietary or confidential data.
- Application Security: Application security is the use of software, hardware, and procedural methods to protect applications from external threats. Security measures built into applications and a sound application security routine minimize the likelihood that hackers will be able to manipulate applications and access, steal, modify, or delete sensitive data. Application security principles are collections of desirable application properties, behaviours, designs and implementation practices that attempt to reduce the likelihood of threat realization and impact should that threat be realized. Security principles are language-independent, architecturally-neutral primitives that can be leveraged within most software development methodologies to design and construct applications.
- Infrastructure Security
- Security Governance: Information security Governance provides the governance processes and assurance to allow business units to ensure business transactions can be trusted; ensure IT services are usable and can resist and recover from failures due to error, attacks or disaster; and ensure critical confidential information is withheld from those who should not have access to it

7.3.3.1 Security Policy

Information Security adds value to the organization only when taken in the context of the business. Business objectives drive the requirements for security; security can enable business objectives by efficiently and effectively managing risk. Balance must be maintained between the drive to accomplish aggressive business objectives and ability to manage risks influencing the business. The approach for information security for Government of Nepal must be flexible, remain conscious of the market and the business and result in an effective, efficient, economical security infrastructure.

The Information technology is broken down into nine different security components -

- Organization;
- Regulatory Compliance;
- Policy Management;
- Security Awareness;
- Measurement & Reporting;
- Information & Technology Asset Management;
- Incident Response;
- Threat & Vulnerability Management; and
- Identity Management.

7.3.3.2 Data Security

Logical Data security refers generally to the management of people, processes and procedures required to create a consistent enterprise view of an organization's data in order to improve data security. More specifically, according to The Data Governance Institute, this is "a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods."

A logical data security helps in organizing how the data should be communicated in a simple and productive way. The main objective of this activity is to archive at least the following

- Enable better decision-making
- Reduce operational friction
- Protect the needs of data stakeholders
- Train management and staff to adopt common approaches to data issues
- Build standard, repeatable processes
- Reduce costs and increase effectiveness through coordination of efforts
- Ensure transparency of processes

To archive this there should be a well defined access control policy. When a user tries to access one business service, the access control process should check that the user has been authorized to use that resource. Service authorization matrix can define this access control and form a rule base for the system to decide whether access request from the user shall be granted or rejected. Following is a sample from the service authorization matrix spreadsheet.

Nepal GEA - Service Authorization								
Service Provider	Business Service ID	Business Service Name	Web Service ID	Web Service Name	Web Service Description	Type of Service	Actor	Class of Roles(Job Process)
IRD (e-PAN)	BA_BS_01	Issue of PAN to a person	BA_WS_01	Apply for PAN	This web service will allow citizens to apply for PAN online. This web service is already available via Website	G2C	Citizen	Applicant
			BA_WS_02	Know Registration Status	This web service will allow citizens to know the PAN registration status. This service is already available via SMS	G2C	Citizen	Applicant
			BA_WS_03	Get Taxpayer's Details	This web service to be used by citizens will provide the taxpayer's PAN details namely the PAN, taxpayer's name, address etc.	G2C	Citizen	Tax Payer
			BA_WS_03	Get Taxpayer's Details	This web service will be used by the govt. unit / agency who would like to validate the taxpayer's PAN details	G2G	Govt Agency(non IRD)	Section Officer(Sakha Adhikrit) or Above

7.3.3.3 Application Security

Authentication Framework

The purpose of e-Authentication Framework is to support organizations and administrators to provide electronic services to businesses and citizens, by appropriate selection mechanisms for authentication and registration of users. The adoption of directives and guidelines of the e-Authentication Framework will improve the level of safety of services provided by public administration bodies, allowing improve the overall functioning of the Government. The e-Authentication Framework is an important aspect of the strategy of the Government of Nepal for transition and adaptation of services to meet the requirements of the current industry standards.

The e-Authentication Framework requires compliance by all entities involved in e-government services to achieve a secure and trusted environment for the proper handling of these through internet.

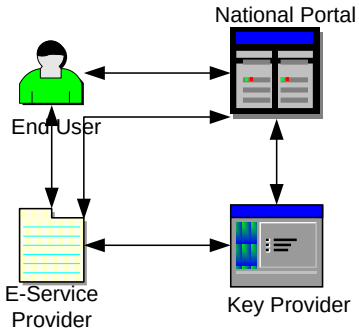


Figure GEA – e-Authentication Framework General Architecture

In summary, the agencies offer their services through National Portal or directly, level of trust, authentication and registration has been established. End-users use the online services offered after being tested and verify the accuracy of their electronic identity.

Basic principles and content of e-Authentication Framework

The main contribution of the e-Authentication Framework is to provide specific rules and guidelines for:

- The classification of data processed by electronic services
- The identification of "confidence levels" for electronic services, based on category of data use, but also taking into account possible effects that may be caused by incorrect operation or management them.
- The relationship of trust between levels, where each level of authentication is defined specific authentication mechanisms.
- The relationship of each level of trust with the appropriate “registration procedures”. The public administration bodies that design and develop electronic services should follow the following basic steps, as provided in this e-Authentication Framework:
  - ✓ Determine the level of confidence in which that service after first identify precisely the types of data used.
  - ✓ Depending on the level of trust and following the recommendations of this PPSA, choose the appropriate authentication mechanism.
  - ✓ Depending on the level of trust and following the recommendations of this PPSA, to adopt the necessary registration procedures for users.

Authentication Model

In the context of eService access users usually are enrolled with multiple unrelated services with different user interface and different credential. Thus user has an inconsistent user interface and works with different copies of the identity. e Authentication Framework will try to address these issues by comparing different authentication model and analyzing which works best in this scenario.

Broadly we can define three types of identity management system and they are Silo, Centralized and Federated Model. The Federated Model that best suites NGEA’s security requirements has been depicted below -

Federated Model

While silo model requires multiple passwords for a single user centralized model is difficult to implement. The balance between two is the federated model. A federated model provides a single logon service across multiple applications with a single identifier. In this model the credentials are issued by the federated Central Logon Service after a registration process. Credentials issued by this central logon service can be consumed by the other applications. Different application has its own user registration process to determine the authorization level. Once the authentication procedure is done by the Central Logon Service it communicates the outcome to the application. One advantage of this model is user can retain distinct application identifier for each participating application. While user registers with the Central Logon Service a new identifier will be assigned to user for subsequent use. It is the duty of the logon service to keep the mapping between Central Logon Service identifier and each application identifier. This model can be implemented to support two authentication flows:

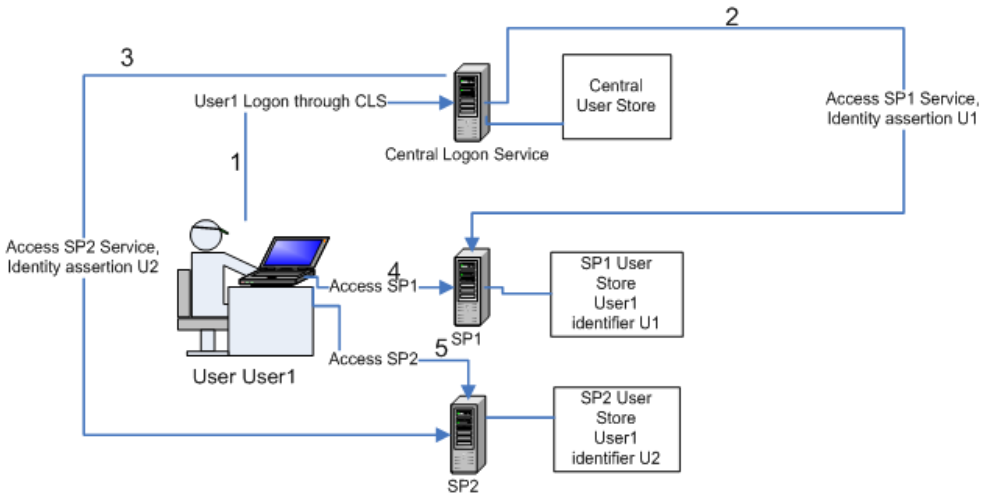
- ✓ Logon thorough Central Logon Service
- ✓ Logon thorough application

Logon through Portal

In this flow user would log on to the portal first and then user would be presented with a list of services which he/she can access. Upon selection user would be taken to the respective application as an authenticated user.

Logon through application

In this flow user first access the application. Then it is the duty of the application to authenticate the user using the application specific credential. Portal authentication will not play any role over here.



7.3.3.4 Web Service Security

Web Services can be considered as an interface that can be accessed via Hypertext Transfer Protocol (HTTP) and executed on remote system hosting the requested service. The main advantage of web service is interoperable machine to machine interaction over the network. So whether it is a stand alone or composed it must provide a strong security guarantees. Web services security can be described along the well known security dimensions, that is:

- Integrity: A message must remain unaltered during transmission across all the intermediary services of different nature.
- Confidentiality: Contents of a message cannot be viewed while in transit, except by authorized services that need to see message contents in order to route.
- Availability: Message should be promptly delivered to the intended recipient who ensures legitimate users receive the services they are entitled to.

In addition each web service must protect its resource from unauthorized access. Addressing such requirements requires suitable means of identification and authorization. In a web service environment it is also important to protect the parties requiring the service in order to ensure that all information used by the parties is authentic and correct.

The core security aspects for web services can be broken into following sub parts:

- SSL/TSL
- XML Data Security
- Security Assertion Markup Language
- SOAP Message Security

7.3.4 Gap Analysis

1. Registration: It should be simple and all the interfacing applications and components (Database, Web server, application server and users) of the system should register, be identified and validated and all activity securely logged and authorized in a uniform centralized way.
2. Single Access point: There should be a single point of entry for the application for each user. Identification and authentication components will be required to authenticate and authorize users.
3. Identification: The Identification process is required to assign a unique identifier to all users and components that interact with the system. The system is required to recognise an individual user / component instance and distinguishes it from other users / components. Username is to be assigned to all the users of the application. An application ID is to be assigned to all the components and interface applications
4. Authentication: Authentication is the process of verifying an identity claimed by or for a system user / component. The system is required to authenticate the user / component and in the process determine the legitimacy and role of a user / component who requests access and interaction with the system. Authentication logs must be available and exception reports generated where applicable. Authentication process should be centralized
5. Authorisation (Access Control): Once the user has been validated as legitimate, the application will be able to verify what resources the user will be given access to. An authorization is a right or a permission that is granted to an authorized entity to access a system resource. The system will allow for Roles Based Access Control (RBAC). Roles are defined as a collection of permissions. Permissions will be grouped based on functional roles. The system will provide access controls based on different criteria like user profile, location and departments. The system will enforce data level security where users will only have access to data for which they have been authorized. The system should be able to enforce policy based on the resources (data, URL, webpage etc) and the profile/role of the user. The system should have a provision for system administrator to customize the security policy based on the business requirements.
6. Integrity: Data Integrity ensures that the data has not been changed, destroyed or lost in an unauthorized or accidental manner. It also informs of any unauthorized data modification by unauthorized users during transmittal or storage. The system will cater to session level security and integrity. Both internal and external users need to have session level integrity to ensure that the contents of the information cannot be modified in transit. For example users should be issued with a unique session identification number when

they make their first request on logging onto the system. The client IP address should also be captured and linked to the session ID and used for checking the integrity of any requests.

7. End to End Integrity: Users (internal and external) will be able to exchange documents / data in such a manner that in the event of the documents / data being modified during transit, this will be evident to the users. Confidentiality requires that information is not made available or disclosed to any unauthorized individuals, entities or processes. Secure connections are required to be established between the all of the components of the application and the any interface application components. Data passing between components will be sensitive and confidential. Therefore, any data in transit is required to be protected by establishing secure connections which ensure data integrity and confidentiality. Communication between the various components that make up the application must be secure. All communication between components is required to be authenticated, authorized and utilizes encryption. All communication activity is required to be audited and monitored via a set of management reports. Communication between administrators and the system components must be secure. Again all communication activity by administrators is required to be audited and monitored via a set of reports.
8. Auditing: The auditing feature will provide an audit trail of which user / component did what and when at any given point in time (this is described in more details in the functional requirements). Security auditing involves recognizing, recording, storing, and analyzing information related to security relevant activities. The resulting audit records can be examined to determine which security relevant activities took place and who (which user/application) is responsible for them. Security Audit Requirements specifies functional aspects of log generation, such as viewing, archival and storage which ensures audit integrity. Functional requirements are defined in three major categories,
    - ✓ Security Audit Data Generation
    - ✓ Audit Review
    - ✓ Audit Event Storage
9. Non-repudiation: Non-repudiation with proof of origin provides the recipient of data with evidence that proves the origin of data and thus protects the recipient against an attempt by the originator to falsely deny sending the data. The system will allow for:
    - ✓ Non-repudiation of the Origin: A particular department may want a long-term binding proof that a request originated with the user, in case the user later denies sending the information.
    - ✓ Non-repudiation of Receipt: This allows for the department to prove that the user received the response.
10. Administration: Easy to use administration functionality will be provided to the application administrators to maintain user identification attributes authentication and authorization information. The administration functionality will be accessible to the administrators through a single point of entry and proper authorisation.
11. Alerting and Notification: Alerting and notification mechanism shall be responsible for raising security alerts for events impacting the security of the application based upon the event notifications from the system. The alerts shall be raised for predefined as well as custom defined events. The alerting and notification system shall be able to classify the events by severity and notify the relevant person by suitable means like email, SMS or console along with the relevant data facilitating further action. The requirements for alerting and notification are:
    - ✓ Shall have the ability to detect events, inform the interested applications when a specific event occurs and notify interested parties. Events are violation of security policies, denial of services, system malfunction and failure of the security framework/requirements.
    - ✓ Setup and management of alerts and notification policies and configurations should be undertaken via the Security Management Interface.

12. Security Policy: IT security policy should be developed for Information security, Data Security and Application Security.
13. Application Scan: All the application should go through code scanning process and penetration testing before deploying in the production environment.
14. Configuration Hardening: All software and hardware are installed with default configuration. This might not be secured enough for a production environment. By tweaking some properties or features can greatly reduce networks or applications vulnerability to an attacker.

7.3.5 Security Architecture Roadmap Components

Phase A

1. Registration: Uniform centralized registration for all the application
2. Authentication Federated: System should be able to use the centralized authentication scheme as well as application based authentication
3. Single Access point: Single point of entry for the all the application
4. Identification: There should be a unique ID for all the users and application
5. Application Scan: All application should be scanned to check if there is any vulnerability.
6. Configuration Hardening: All the application and hardware should be tweaked to ensure that a default property does not create any risk to the environment.

Phase B

1. Authentication Centralized: Application should use the centralized authentication mechanism. No local user repository should be used to authenticate
2. Integrity: All application should have session level security
3. Policy based Authorization: Authorization should be controlled from the central user repository.
4. End to End Integrity: All application should use transport level security while interacting with other application.
5. Auditing: All application should have auditing feature to track who performed a specific activity and when.
6. Non Repudiation: Application should be capable to provide the prove the origin of data and recipient of the data
7. Security Policy: Need to develop information , data and application security policy

Phase C

1. Administration: Centralized administration utility for all application in the organization
2. Alerting and Notification: Systems to raise security related events with severity defined and forward that

Reference: For detailed description of each element in the Security Architecture refer to the GEA Enterprise Architecture continuum and Architecture repository.

Refer to the "Nepal GEA – Security Architecture report for detailed information pertaining to Security Architecture

7.4 Infrastructure Architecture

7.4.1 Infrastructure Architecture Principles

Principle # 1	
Name	Scalability, Availability, Backup & Archival
Statement	Scalability: Technology standards chosen should meet the changing and growing ministry needs and requirements and the applications and technologies should essentially scale up, to adapt and respond to such requirement changes and demand fluctuations. Server, storage and network capacities must handle user, application and data loads. Availability / Failover: The technology infrastructure should exhibit no single point of failure Archival & Backup: The system would have data and source spanning across multi years. The archival& backup polices and mechanism should address the archival& backup requirement of the system.
Rationale	• Needed to support the overall SLA requirements around scalability, availability & performance
Implications	• The system infrastructure should be architected considering failover requirements and ensure, a single server or network link failure does not bring down the entire system (although e.g. performance may degrade). • The system should handle every request and yield a response. It should handle error and exception conditions effectively. • In the event of failures or crashes the transactions and data would need to be recovered. • The platform solution should support effective disaster recovery • Need to monitor the systems health at regular intervals. Use of central system, monitoring tool would be required to gauge the health of the system all time and monitor against the pre-defined SLA.

7.4.2 Baseline Infrastructure Architecture

PwC conducted a survey by visiting the IT heads and head of relevant departments to get an understanding of the current state of the IT infrastructure within the government bodies. The following table gives a broad summary of the survey –

	Survey Parameters	Nepal Police	KMC	SC	EC	FCGO	DoR	NTA	MoGA	DoLRM
1	Application server node	Yes	No	Yes	Yes	3rd Party	Yes	Yes	Yes	No
2	Content creation & management server node	3rd Party	No	No	No	No	No	No	No	No

	Survey Parameters	Nepal Police	KMC	SC	EC	FCGO	DoR	NTA	MoGA	DoLRM
3	Directory server node	No	No	No	No	No	No	No	No	No
4	Database server node	Yes	No	Yes	Yes	3rd Party	Yes	Yes	Yes	No
5	File server node	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6	Domain name server node	3rd Party	No	No	No	3rd Party	No	No	No	No
7	Firewall server node	Yes	No	Yes	Yes	No	Yes	No	Yes	No
8	General purpose workstation node	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
9	Middleware/ integration server node	No	No	No	No	No	No	No	No	No
10	Kiosk node	No	No	No	Yes	No	No	No	No	No
11	Main relay node	3rd Party	No	Yes	3rd Party	3rd Party	3rd Party	3rd Party	3rd Party	No
12	Public key infrastructure services	No	No	No	No	No	No	No	No	No
13	Security server node	No	No	Yes	No	Yes	No	No	Yes	No
14	Systems management node	No	No	No	Yes	No	No	No	No	No
15	Voice over IP gateway	No	No	No	No	No	No	No	No	No
16	Web server node - Informational	3rd Party	No	No	3rd Party	No	No	No	No	No
17	Web server node – Transactional	No	No	No	Yes	No	No	No	No	No
18	Workflow server node	No	No	No	No	No	No	No	No	No
19	Load balancer node	MP	No	No	No	No	No	Yes	No	No
20	Infrastructure management server node	No	No	No	Yes	No	No	No	No	No
21	High-level infrastructure / network diagram	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

The survey revealed that while the FCGO, the MoGA and the Supreme Court of Nepal have relatively secure environments, in comparison to the other departments, there is a lack of resource management and resource optimisation tools. The current scenario is diverse, with practically minimalist infrastructure in departments like the Municipalities and at the same time departments like the department of Post and MoGA are significantly IT enabled and have a progressive IT adoption road-map.

This diverse spectrum of IT maturity requires that a significant capacity building exercise in terms of IT awareness and IT enablement be conducted to bring the departments at a minimum shared infrastructure level.

To broadly outline the relevant current state IT infrastructure, the present infrastructure landscape of the following 3 departments with relatively secured environment has been considered

1. Nepal Police
2. The Department of Posts
3. Ministry of General Administration

Nepal Police transacts in extremely confidential and secured data, however, the current resource management, network security, user management and physical security infrastructure are insufficient to provide even basic levels of security. We also recommend that the SWAN which is currently being leased from the NTC be an owned resource to transact on such important and critical data relevant to national security.

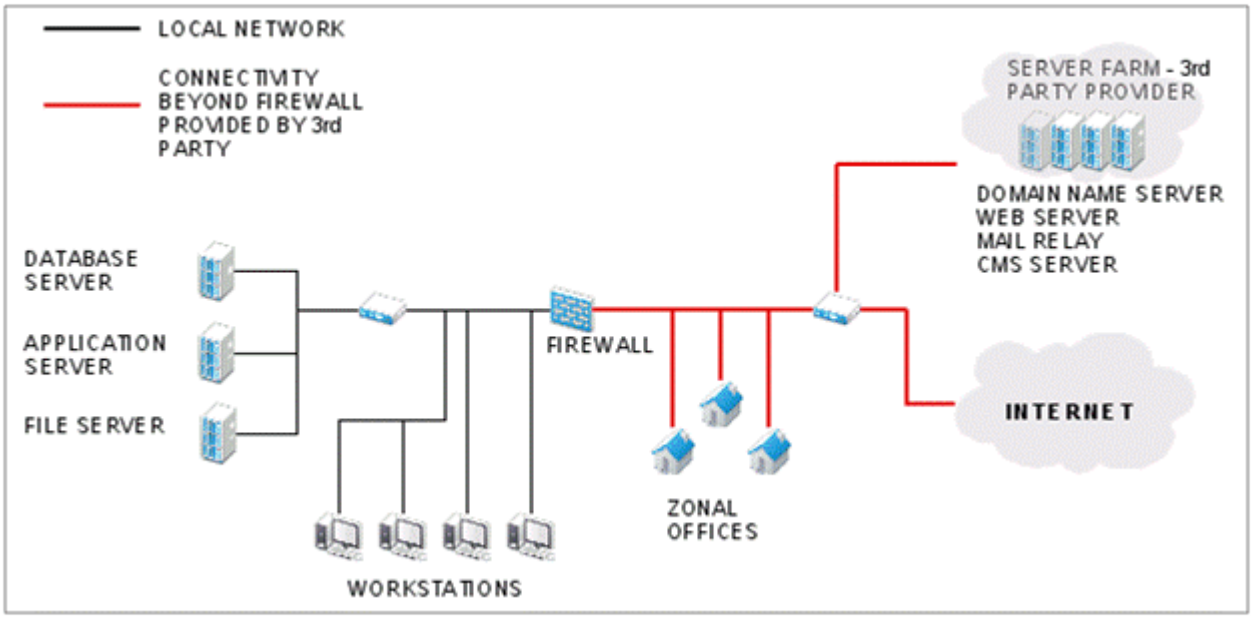
The Department of Posts is limited from the perspective of resource management, user management, and physical security. However, they have succeeded in implementing a variety of technologies relevant to various operations and have capacity and maturity to expand / integrate into a shared resource infrastructure.

The Ministry of General Administration is strongly and securely connected to other ministries and departments within the Singh Durbar complex. There is infrastructure replication with Ministry of Finance to provide redundancy also. These are again relevant capacities that can be migrated into a shared resource infrastructure.

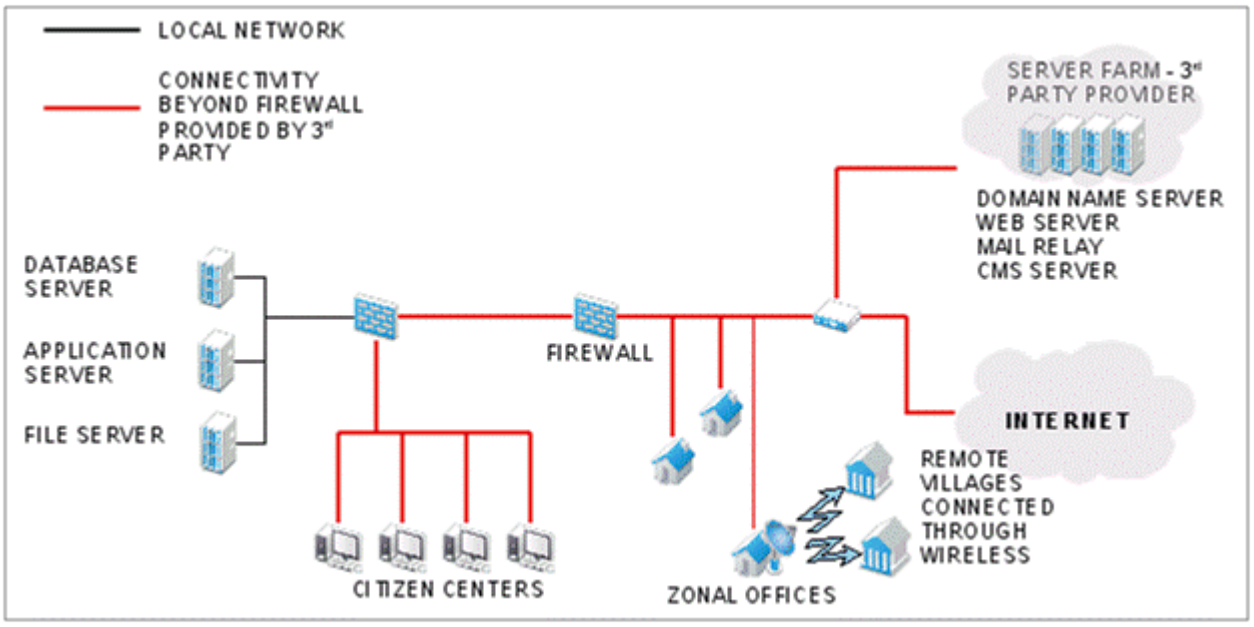
The other departments like Department of Roads and Department of Land Reforms and Management have operational infrastructure with a variety of components however, a significant number of these components are "end-of-life" and require up-gradation. Their IT capacity also needs to be enhanced in-terms of management tools and skill sets. These, thus become ideally suited to use the shared infrastructure instead of creating individual capacities for each of these departments.

A very high level infrastructure diagram for the above three typical departments is given below for reference

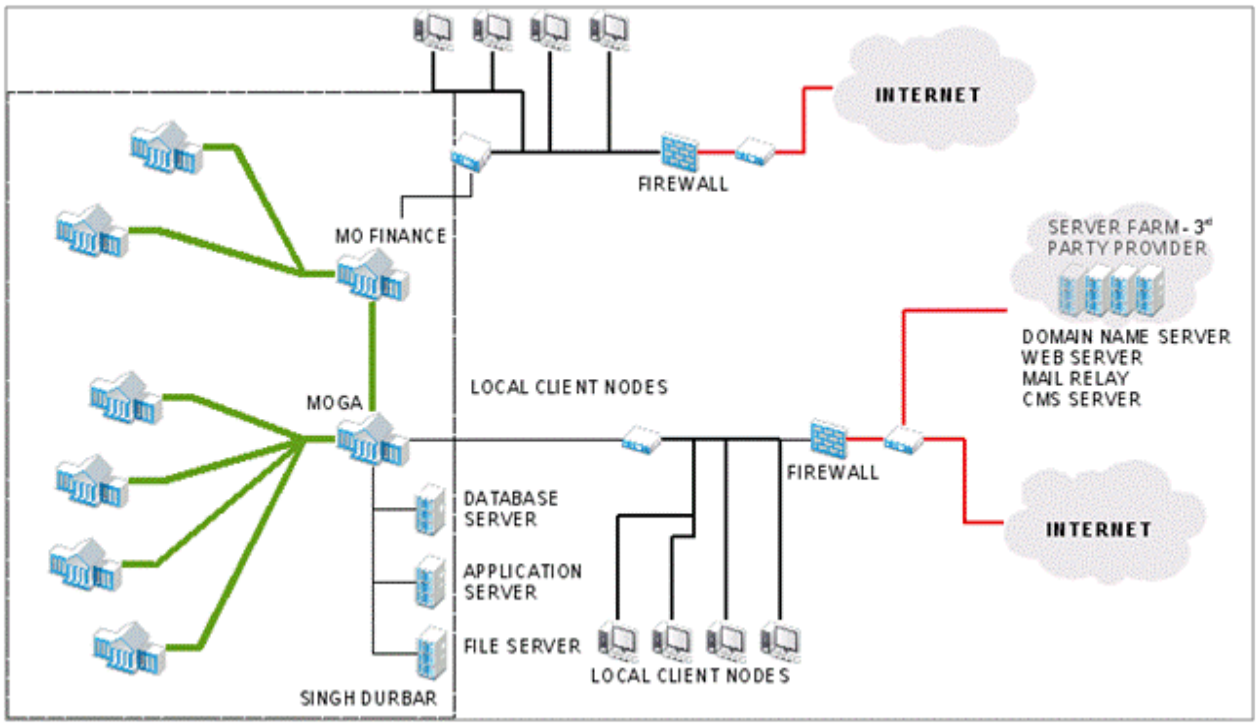
Nepal Police



Department of Post



MOGA



7.4.3 Target Infrastructure Architecture

Information Technology is a key enabler to the process of smart e-governance, offering access and delivery of services to the expectations of people:

- Horizontal and Vertical integration within the organization is essential for effective and efficient information exchange.
- This should be followed by authorizing public access to administration at various points in this Horizontal and Vertical information corridor.

- Standardizing, and transforming all citizens' centric Government's applications into electronic form for interactive public use is the last step in e-governances process.

To operationalize the goal for e-governance, a countrywide IT infrastructure deployment should be planned from two perspectives:

- **Shared and secured network**, and
- **Shared data centre services**

To assist the Nepal government with the objective of improving inter-department IT infrastructure sharing, the technology / infrastructure architecture proposes a set of best practices and design considerations that address:

- Shared Infrastructure
- Shared Data Centre Services
- Shared Security Services
- Shared Infrastructure Management Services (Network and Data enter)

Shared and Secured Network

Today governments are increasingly turning to the flexibility of IP networks to deliver converged voice, video, and data services. Converged network, with a focal emphasis on "open standards" (for intra inter and extra organization exchanges). This offers the dual advantage of reduced cost and increased efficiency.

Costs are reduced because multiple agencies can leverage a common investment. Additionally, the provider of services can maximize utilization of the shared network and data centre assets by turning dedicated resources assigned to each application within each group into a shared pool of resources that can be dynamically allocated based on application and business needs.

Efficiency is improved because the single shared infrastructure is easier to manage and re-configure to conform to the changing needs of the government and the constituents it serves. By leveraging a common shared infrastructure, agencies can easily share applications and information based on policy and application demand, allowing new applications to be built based on constituent needs instead of government hierarchy.

Looking at the current and future trends, the main technical requirements for complete shared infrastructure architecture are:

- Remote access from branch or home locations and the capability to establish a VPN connection to the network when travelling
- Logical isolation of traffic from the appropriate users
- Authentication and logging capabilities
- Accounting, filtering, content checking, and security
- Seamless support for both wired and wireless access

Shared Datacenter Services

Data centers are evolving and government agencies that focus on shared infrastructure architectures can benefit from this evolution. Data centers house many critical assets for government agencies, including data storage systems, applications, and servers that support day-to-day operations. Traditionally, these data centers housed mainframe computers, then client and server systems. Today data centers have became overly complex, at times underused and exhausting physical resources such as heat, space, and power. However these expansions

also provided for scalability, reliability, and availability. As the shared infrastructure architecture for data centers is designed, these shortcomings must be mitigated while preserving the positive critical attributes.

Cost is the most critical factor driving data center consolidation because as data centers expanded to meet agency requirements, with more and more servers, applications, and storage devices, they became increasingly expensive to support and maintain. Costs include the real estate required to store the equipment, some of which may only be operating at a fraction of its capacity, the power to run the equipment, and the maintenance of the devices. Hence while capital expenditures present the initial financial impact, recurring operating expenses place a huge financial strain on government agencies, particularly when many government agencies maintain their own low-capacity, and inefficient, data centers.

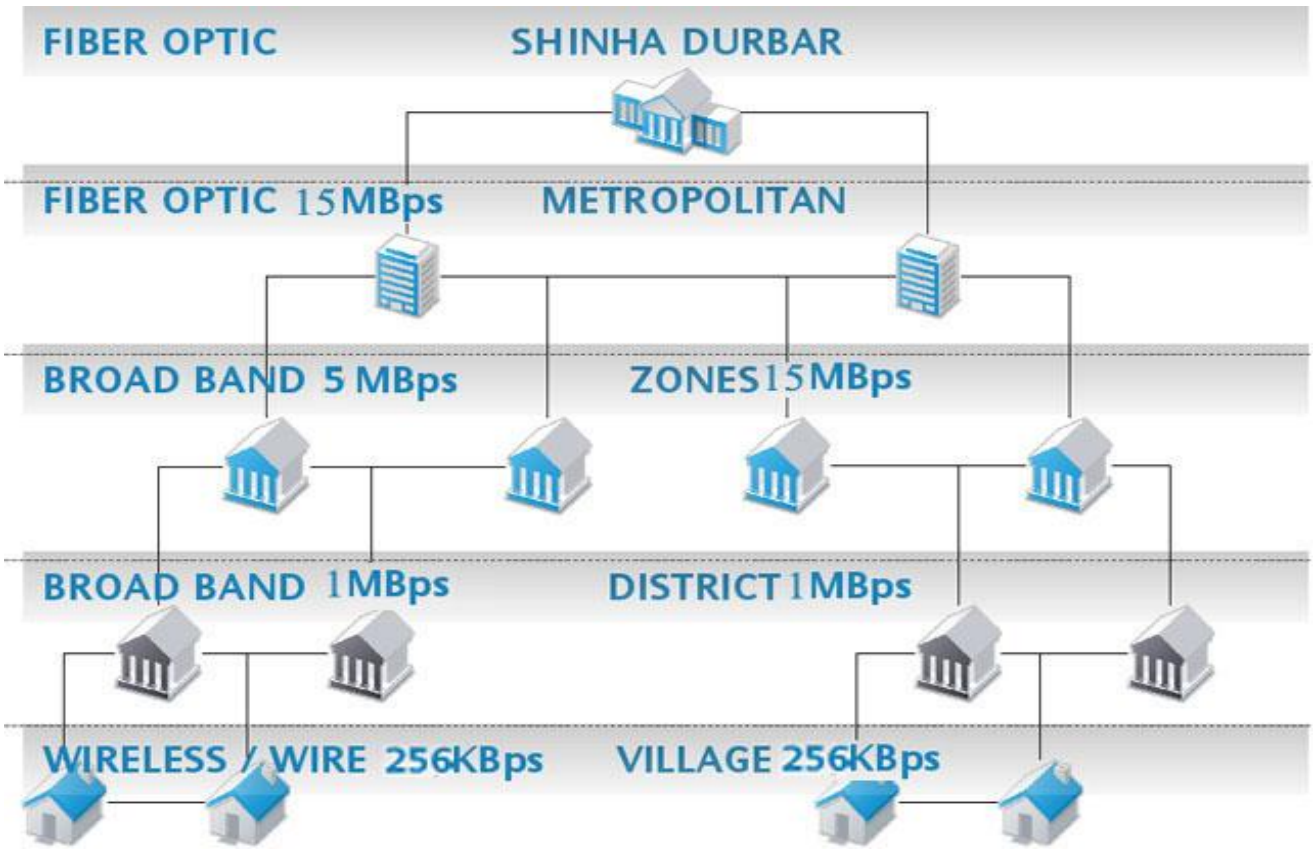
Shared Infrastructure – Broad Design Considerations

The government of Nepal should create a state – of – the – art network infrastructure under Nepal Wide Area Network Project (NWAN) with the following goals:

1. establish a reliable horizontal and vertical communication corridor for within the state administration to make government more productive and compatible for electronic transactions;
2. achieve e-governance commitment and bring governance closer to public;
3. strengthen disaster management response capacity;

We recommend that this state owned ICT network infrastructure (Nepal Wide Area Network – NWAN) be setup to provide:

1. Voice, Video and Data – all services on IP,
2. connect the 14 zones and 75 district offices in the network capable of handling high volume, high speed data and video conference
3. connect subsequently, strategically selected villages numbering more than 1000
4. One robust campus area network at Singh Durbar (SDAN) connected with NWAN enabling connectivity up to the District level access for all officers at secretariat and vice versa,
5. Satellite interconnect with NWAN Hub to make all services of the network Omni present in the state/country at the village level, through VSAT or Local Wireless as infrastructure permits terminal.



At a very high level we recommend the following connectivity:

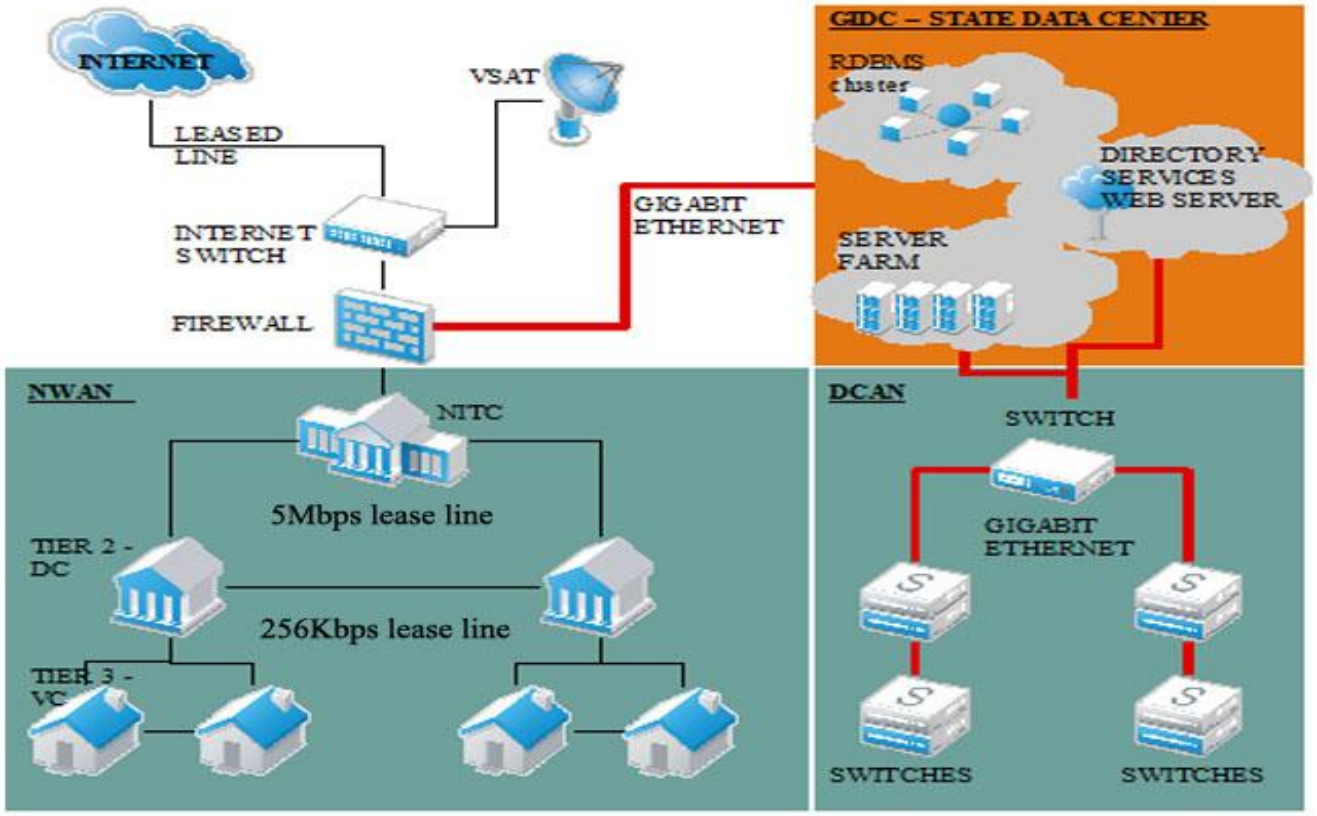
- Singh Durbar – Secure Fibre Optic connectivity between all ministries within the Singh Durbar having 15 MBps bandwidth network with redundancy .
- Kathmandu – All departments within Kathmandu should connect to the Singh Durbar on Fiber Optic connectivity having 5 MBps bandwidth network with redundancy
- Zones – Zonal offices should be connected with 5 Mbps broadband to Kathmandu and Singh Durbar offices having 15 MBps bandwidth network with redundancy
- Districts – The district offices should be connected to the zonal and Singh Durbar offices with at least 1 MBps bandwidth network with redundancy .
- Villages – The villages can be connected to the district offices using wireless or other connectivity on at least 256 KBps bandwidth network with redundancy.

NWAN Network Architecture and Topology:

We recommend that the NWAN be based on a "hub-and-spoke" design, with 3 tiers:

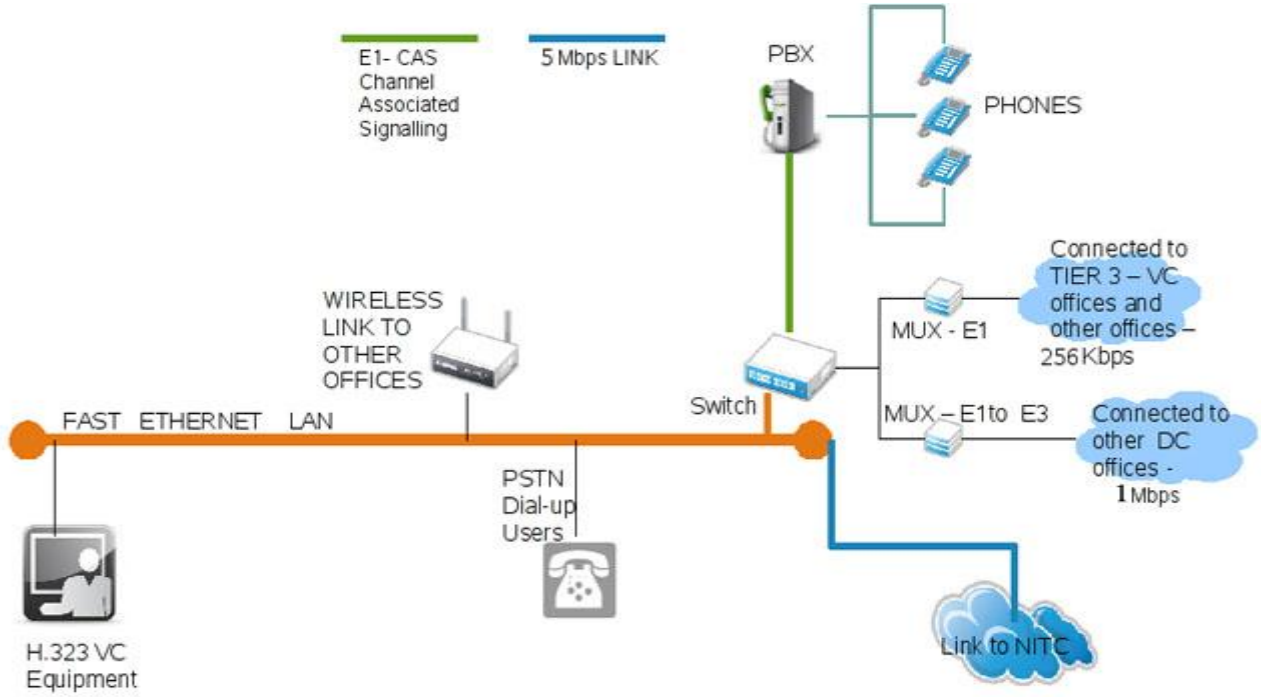
1. Tier 1 – NITC at Singha Durbar, Secretariat offices within Singha Durbar and the Metropolitan and Secretariat offices within Kathmandu where the highest offices of the government functions should be connected horizontally through a Durbar Campus Area Network (DCAN). The district centers (DCs) would be connected vertically with this Campus Area Network.
2. Tier 2 – The District and Zonal Offices for the various Secretariats would be connected horizontally to a District Center (DC).
3. Tier 3 – The local village offices where applicable would be connected horizontally to a Village Center (VC) which in turn would be vertically connected to the district center (DC).

The NITC is the network HUB. The Durbar Campus Area Network (DCAN) integrates with NWAN at NITC (as shown in the figure below)



The recommended design for NWAN is that of a total IP network. In such a scenario, Data, Voice and video travels as IP packets in the network, with a total convergence.

Tier – 1: NITC NWAN Center Network



As shown in the above diagram, the network in the NITC NWAN center comprises all the components of a central hub site.

Existing data connections (5000 – 10000 estimated) on the DCAN should be interconnected to NWAN. All Government offices and each of the (5000 – 10000 estimated) users at Secretariat, in the capital city, should be capable of doing video conferencing (VC) to any one or all Master Control Units (MCU) in the network any where in the state.

Mobility feature introduced into GSWAN:

An extended c-band VSAT station (need to get some second opinion on this recommendation) should be interfaced on to the LAN at NITC, to enable NWAN connection with the portable VSAT mobile working at a distant remote location. This will enable wide area network services to locations where there is a total telecom black out. The events taking place at remote locations are covered and connected to NWAN through portable VSAT terminal. This will give tremendous flexibility to the state administration in reaching to the public in remote areas during any emergency.

WLAN for important other offices beyond reach of cable:

A Wireless LAN can be commissioned, to connect to the DCAN in case they are not on the Ethernet backbone of the campus network.

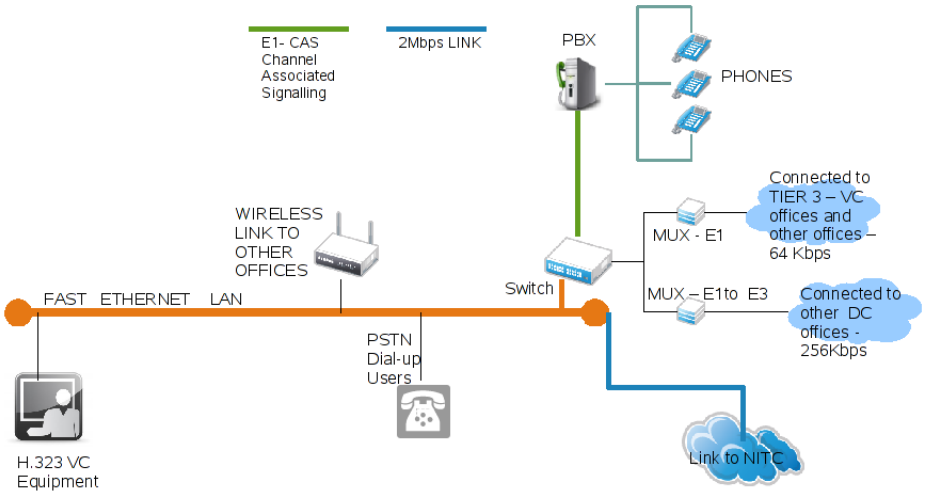
Server farm:

Multiple Servers can be commissioned in server farm at the State Datacenter in GIDC. All common IT services, viz. internet, web hosting and maintenance, data base storage and maintain, mail services, etc... , can be managed from the server farm facility centre, interfaced with NWAN and DCAN.

Tier 2 – District Centre – Generic Architecture

The District Centre NWAN node should have all – voice, video and data communication faculties available.

The districts in each zone should have a District NWAN Centre (DC) and be connected horizontally at the zone office in addition to all Village NWAN Nodes (VC) stations falling under its jurisdiction. Offices authorized by



the Government should be able to enter into the Network through dialup access. Remote Access Server (RAS) at each DC should have 10 dialup PSTN lines enabling access to those who are not directly connected with NWAN.

Shared Datacenter Services – Broad Design Considerations

In the shared data centre approach of the shared infrastructure architecture, a centre of excellence delivers to each agency a uniform set of data centre services that are technologically current and much more cost-effective. To accomplish this, the next-generation shared data centre must meet these requirements:

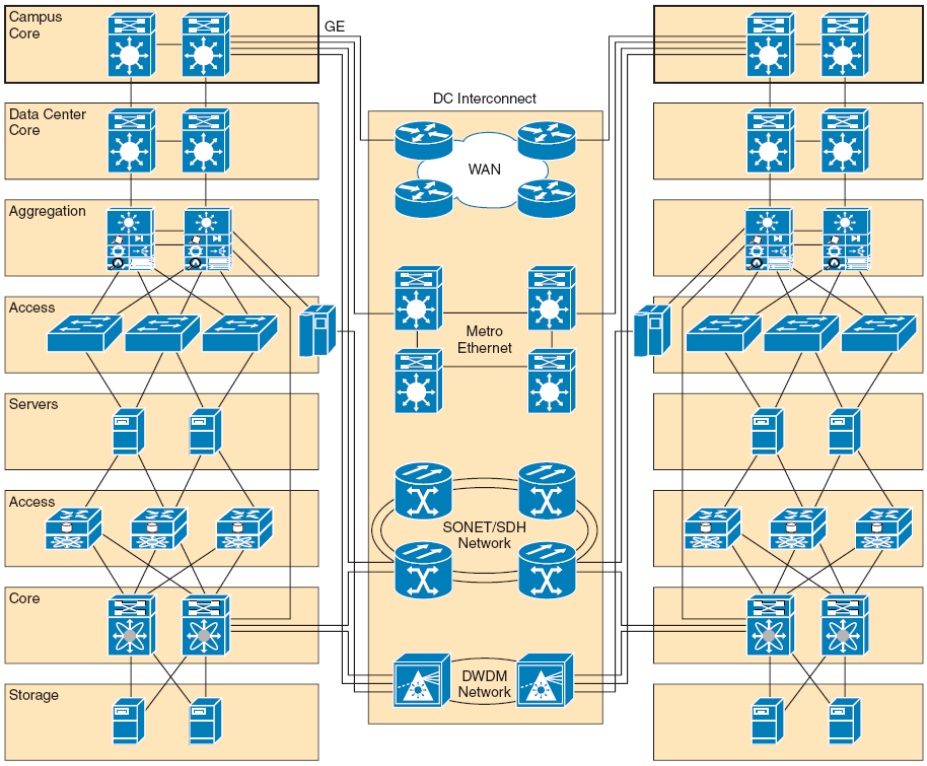
- **Scalability, availability, and reliability**—The consolidation of infrastructure into a shared LAN/WAN environment leads to higher-bandwidth 10 Gigabit Ethernet links in the access and aggregation network, while maintaining a high-availability design to ensure that the data centres are always accessible.
- **Security**—an ever-increasing factor in network design is security, requiring both products and a suite of security best practice designs to ensure that the critical assets of data centres can withstand known and day-zero threats.
- **Segmentation**—Consolidation of data centres translates to secure resource allocation and full utilization of the assets, thereby maximizing the capabilities of the equipment. In a shared environment, segmentation allows multiple agencies to share assets that are partitioned to meet the requirements of each agency.
- **Virtualization**—with the capacity of the WAN, multiple sites for data centres and agencies can now virtualize more assets into the data center and offload the management of onsite gear. These assets can be located in multiple data centres to provide greater survivability in the event of unforeseen circumstances that might bring down a particular site.
- **Intelligence**—Different departments have different application requirements that can strain the data centre. Intelligent service blades enable application acceleration, increased application security, and methods to simplify the application infrastructure to permit the faster deployment of new application servers.
- **Manageability**—this centre of excellence approach simplifies the management of the data centre. With infrastructure segmentation and virtualization bundled with management tools from Cisco and

partners, the shared data centre architecture drastically reduces agency overhead and streamlines operations.

A shared infrastructure architecture that meets these requirements helps drive down the total cost of ownership while enabling the data centre to effectively meet the demands of multiple agencies. This can help address any regulatory or political roadblocks that a consolidation effort might face. Finally, the efficiencies gained not only reduce cost, but enable government agencies to more effectively develop tools to serve their constituents.

Data Centre Architecture – Approach

The shared data centre architecture of the shared infrastructure approach can be highly sophisticated. The components of the data centre are simplified here to explore the specific requirements of a well-designed shared data centre for multiple agencies.



- Building blocks:
  - Network areas—Core, aggregation, access, and DC interconnect
  - Network DNA—Layer 2 and Layer 3 designs, high availability, and clustering
  - Network virtualization and segmentation
  - Network intelligence
  - Network security
- Server fabric
- SAN fabric

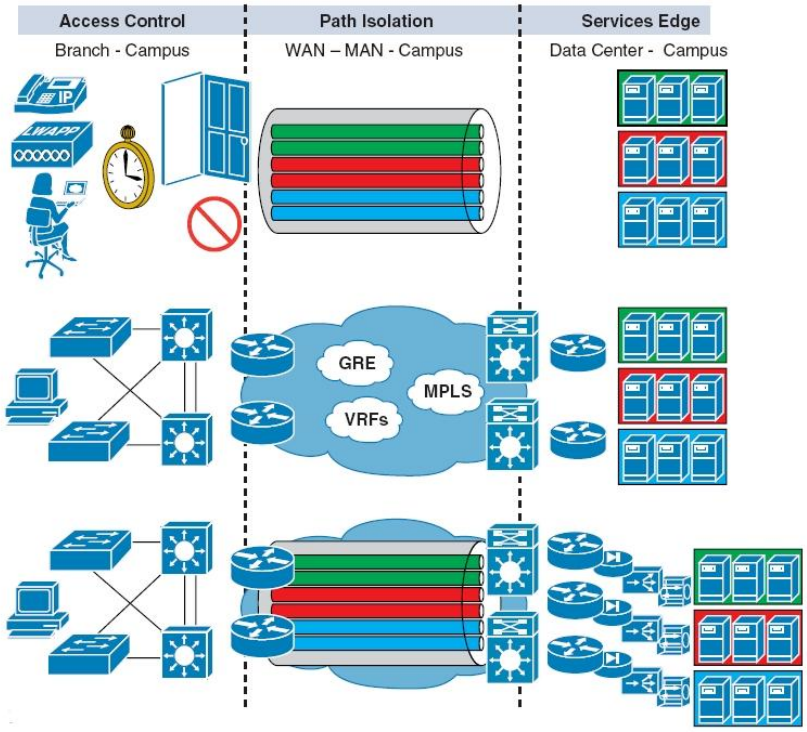
The architectural framework is divided into three functional areas, each of which maps to one of the objectives:

- Access control
- Path isolation
- Services edge

1. Identify & authenticate client (user, device, app) attempting to gain network access
2. Isolate into a Segment
3. Grant _controlled_access or prevent access

4. Map client VLAN to transport technology
5. Transport client traffic through isolated path
6. Terminate isolated path @ destination edge

7. Map isolated path to destination VLAN
8. Apply policy at VLAN entry point
9. Isolate Application environments



7.4.4 Gap Analysis

Following are the gaps identified between the baseline and the target architectures. The list of identified opportunities is

1. Security
   - Shared Security Services
   - Shared Security Infrastructure
   - Network Security in a Secure Segment
2. State Wide Area Network
3. State Data Center
   - Data Centre Operations and System Management – ITIL
   - Security Considerations for the Data Centre
   - Data Centre Security Framework
   - Data-centre Automation

4. Configuration Management Database
5. Infrastructure Governance

Reference: For detailed description of each element in the Infrastructure Architecture refer to the GEA Enterprise Architecture continuum and Architecture repository.

Refer to the "Nepal GEA –Infrastructure Architecture" report for detailed information pertaining to Infrastructure Architecture

7.4.5 Infrastructure Architecture Roadmap Components

7.4.5.1 Roadmap – Shared Network Adoption

The architecture for a shared infrastructure can translate to many benefits for government agencies looking to address many of today's IT and collaboration requirements.

Based on the SONA framework, PWC government programs and technical architectures integrate networked infrastructure services, constituent services, and business applications within and among agencies.

Having a phased roadmap allows a successful migration from the current infrastructure to an architecture supported by a center of excellence that enables shared infrastructure and services between multiple agencies.

Each phase of the roadmap introduces new technologies to reach a shared infrastructure, which enables agencies to share services through a center of excellence. Each agency may have different needs, requiring some tasks to be performed sooner, but the below table shows a transformation to a shared infrastructure model broken down into logical steps.

	Technology	Shared / Dedicated across Agencies	Description
1.	Time-Division Multiplexing (TDM)	Dedicated	Current state of the network which is typically characterized by siloed TDM technologies such as PBX for voice and Frame Relay/ATM for data connectivity.
2.	IP Network	Dedicated	The first step in migration from TDM technologies to an IP-enabled infrastructure that builds the foundations for the transformation to occur. The IP network needs to be built with network characteristics to support QoS, high availability, etc.
3.	IP Communications	Dedicated	Enable "Unified Communications", voicemail, conferencing, rich-media communication, and extension mobility.
4.	IP Contact Center	Dedicated	Enable a centralized contact center to deliver intelligent call routing and call treatment to support an IP-enabled customer contact center.
5.	Self-Defending Network Security	Dedicated	Enable each site with the security needed to maintain the business through capabilities including stateful firewalls, intrusion protection and prevention, URL filtering, and trust

	Technology	Shared / Dedicated across Agencies	Description
			and identity.
6.	Intelligent Routing	Dedicated	• Site-to-site VPN with IPSec for encryption when required. • DCN for out-of-band management. • QoS to ensure the site-to-site experience is equal to the experience of a single location, which is a key foundation to support differentiated services. • Hierarchical, end-to-end network.
7.	Mobility	Dedicated	Enable mobile IP to support the mobile workforce.
8.	Data Center	Dedicated	Consolidate data center into a centralized environment enabled through an IP network fabric that supports the network DNA to transform the data center architecture.
9.	Intelligent Routing	Shared	Enable virtualization and segmentation of the intelligent routing layer to support shared infrastructure resources across multiple agencies.
10.	Self-Defending Network Security	Shared	Virtualize security features such as firewall into the network to support multiple agencies.
11.	Data Center	Dedicated	Enable data center consolidation with the server and storage fabric.
12.	IP Communications	Shared	Virtualize IP Communications through the centralized environment supporting voicemail, conferencing, and other rich-media communication for multiple agencies.
13.	IP Contact Center	Shared	Virtualize the IP contact center for multiple agencies.
14.	Data Center	Shared	Consolidate data center functions across multiple agencies and introduce application acceleration and load balancing.
15.	Data Center	Shared	Virtualize data center functions across multiple agencies and introduce application protocol optimization/translation.

7.4.5.2 Roadmap – Data Center Consolidation

Phase 1 – IT Asset Inventory Baseline (Including Preliminary Assessment & Quick Wins)

Assessment will include details such as facility location, how the data center is utilized, and by whom, whether a facility is stand-alone or co-located with other activities, square footage of the facility, legal ownership details,

measurement of energy consumption, and ongoing costs. Those who conduct the assessment will be required to:

- Create an inventory of HW.SW assets by data center
- Capture baseline metrics for utilization & energy for each data center
- Identify quick wins, including specific deliverables
- Provide an IT Asset inventory for the baseline and the quick wins.

Phase 2 – Application Mapping

Efforts must be made to extend the ongoing inventory to the level where administrators can map applications:

- To servers
- To specific databases and platforms
- To specific application dependencies
- With specific details on application security
- With details on application usage and service level agreements (SLAs)
- With information on segment architecture

Phase 3 – Analysis & Strategic Decisions

- Perform energy and cost evaluation for possible different approaches
- Identify the risks, alternatives, cost assumptions and business benefits
- Make strategic technology & consolidation investment decisions

Specific deliverables:

Consolidation analysis and strategic investment decisions on standard platforms and services

Phase 4 – Consolidation Design & Transition Plan

- Design and test consolidation alternative
- Develop transition plan for energy use optimization and data center consolidation
- Create a project plan and full Work Breakdown Structure for the transition plan

Specific deliverables:

Consolidation design and transition plan

Phase 5 – Consolidation & Optimization Execution

- Execute virtualization, consolidation and migration plans
- Execute energy use optimization plans
- measure and report on utilization and cost saving metrics

Specific deliverables:

Consolidation and execution plus progress reports

Phase 6 – Ongoing Optimization Support

Based on lessons *learned from previous work, continue energy use optimization and consolidation*

Specific deliverables:

- Ongoing semi-annual metrics reports
- Continue ongoing monitoring and reporting of utilization and cost saving metrics.

End Goal

One likely end-goal if the extensive assessments are too slow the expansion of government data centers by instead focusing on enterprise architectures that will support more cloud-based IT services

7.5 NeGIF - Overview

NeGIF provides a framework to share, collaborate and integrate information and organisation processes by defining the minimum set of collection of ICT standards and technical specifications governing the communication of systems, flow of information, as well as the exchange of data and business processes that relates to Government Ministries, agencies and departments. Increasingly the use of open standards to enable such interoperability is the key for success of any NeGIF framework and choosing the right set of technical standards and policies that are suitable to the environment.

The key driving factors for NeGIF is the following

- Interoperability
- Service Maturity
- Availability of support
- Openness

This NeGIF would serve the following objectives of Govt. of Nepal's government implementations:

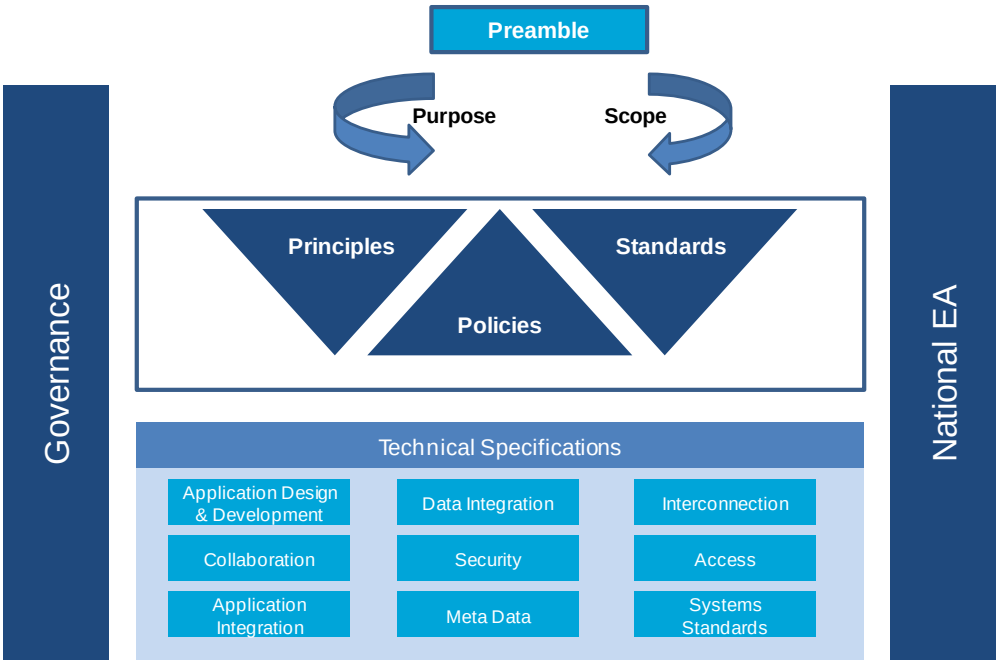
- Enable proprietary and open source systems in different Government information systems, both within Government and external to Government, to communicate and inter-operate efficiently and effectively;
- Promote and foster the adoption of open standards that enables the exchange of data between applications;
- Promote vendor-neutral and technology-neutral implementations, with the adoption of open standards, for all Government information systems; and
- Reduce the total cost of ownership of Government information systems, with the adoption of open standards.

To achieve this level of interoperability it requires a holistic approach covering different dimensions of interoperability standards at various levels such as, business process or organizational interoperability, information or semantic interoperability, and technical interoperability.

Key Features of NeGIF -

- XML as the primary standard of data interoperability
- All standards selected support a secure computing environment
- Selected standards have the capacity to be scaled to changed demands
- Promote the use of metadata
- Use of open standards that are widely supported
-

The core of NeGIF is the Preamble (covering purpose and scope), Principles, Policies and Standards. Governance and Architecture are aspects that will aid NeGIF implementation, interrelationship, management and success.



Preamble

Preamble covers the purpose and scope of Nepal eGIF.

The overarching purpose of NeGIF in Nepal should be to improve economic growth and equity by enhancing access to information and its effective use, thereby improving delivery of services to benefit stakeholders – citizens, businesses and also Government (intra and inter).

The scope of the NeGIF is to facilitate the exchange of data and information between:

1. Government-to-Government (G2G) - Within Nepal Government i.e. between Government agencies and departments.
2. Government-to-Citizens (G2C) - Between Nepal Government and its citizens.
3. Government-to-Businesses (G2B) - Between Nepal Government and businesses in the private sector, i.e. suppliers and contractors to the Government.

Principle

Refer to the key architectural principles for interoperability.

Policies

Some of the key policies covering various aspects of NeGIF which are to be followed –

- Overall Policies
  - All selected standards should be based on the objective, scope and principles of NeGIF.
  - The use of open standards should be given preference over proprietary standards wherever appropriate. In the event of choosing proprietary standards the NeGIF principles should be considered as the basic requirement
  - The institution-based approach should be replaced by a service-centre one closely aligned with e-Governance strategy and adherence to the NeGIF should be mandated throughout all government ministries, agencies and authorities.
- Application & Technology Policies

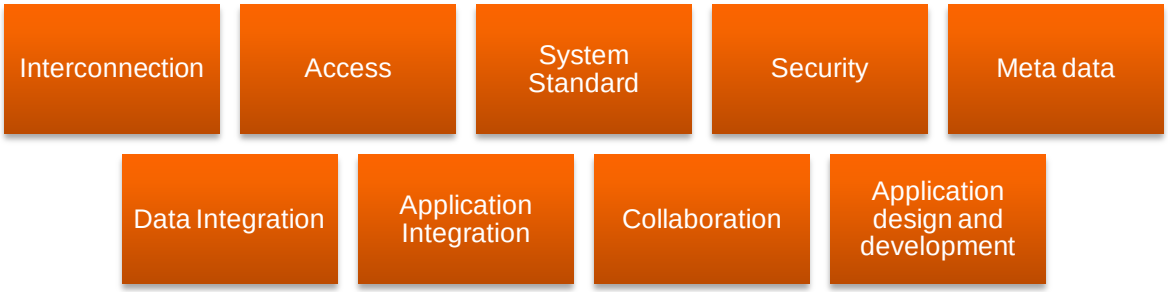
- The standards should as far as possible be aligned with the World Wide Web for all public sector information systems.
- The development of applications or e-Services should provide services to the users who do not have the access to latest technologies and to those who may not be aware of using such technologies.
- All future application and migration of legacy application should be web based (browser based interface).
- While developing applications, special accessibility needs have to be considered including the provision of more sophisticated and user-specific resources.
- Current applications may not need to comply immediately with NeGIF; however, any new information system/change/upgrade must be compliant. A given version of NeGIF should apply over the lifecycle of a specific, discrete system.

- Data & Metadata Policies
  - XML should be the primary standard for data integration and data management for all application in every ministry, agency and authority in Nepal. The Nepal Meta data standards should be primarily based on the international Dublin Core model (ISO 15836)
  - Development of national level data set and centralization of Metadata of the country should be done in compliance with the interoperability standards on metadata
- Security Policies
  - Nepal should have process, principles, policies, technology and control mechanism to achieve fair maturity in Trusted Computing and Digital Rights Management (DRM) to ensure:
    - Confidentiality/privacy of Nepal government held information
    - to continue to exercise control of Nepal government data and computing environments
    - Protect confidentiality rights accorded to personnel's who use government systems
    - Ensure privacy of personal information.
  - The security requirements for the information, the services, and the infrastructure should be identified and treated in accordance to the type of information, SLA's, and the outcome of the risk analysis
  - Security is a process that should be present at all stages of application development, the security working group should document systems, security controls, and the environment topologies, educate every ministry/agency IT department on their responsibilities for the security and the correct use of the access means and update policy and procedures

7.5.1 NeGIF – Technical Standards

The NeGIF comprises the technical principles, policies and standards required to achieve interoperability. These are the minimum set necessary to support the range of transactions and services provided by Government and to integrate information systems within Government.

The technical policies cover the following major areas which are essential for interoperability:



The brief overview of the nine technical areas and the respective components are given below.

Technical Areas	Components
Interconnection	- Interconnection –Telecom • Access Transmission Network • Fixed Line Next Generation Network • Next Generation Mobile Network Standards - Interconnection- Enterprise • Physical Layer Infrastructure • Application Layer Protocols • Transport Layer Protocols • Internet Layer Protocols • Link Layer Protocols - Interconnection- Integrated (Telecom + Enterprise) • Internet Service Provider Standards • Financial Interconnectivity System Standards
Data Integration	• Character and encoding for information interchange • Data description • Data exchange & Transformation • Data exchange Formats • Ontology-based information exchange • Data modelling language • Data integration meta language • Minimum interoperable character set • Digitization • Data Definition for Smart Cards
Security	• Access management • Anti Spam • Anti Virus/Anti Spyware • Desktop Firewall • Digital Signature • Email Security • Encryption Algorithm • Enterprise Firewall • Identity , Authentication , authorization and privacy • Identity management • Intrusion detection and prevention • IP Encapsulation security • IP security • Layer 2 Security • Proxy server

Technical Areas	Components
	• Public key infrastructure • Remote Security • Secure transport • VPN • XML security standards • Physical Security
Access	• Access Token • Animation • Compression • Kiosk • Mobile devices • Scripting • Smart Card • Directory Access • Web Access standard • Web browser • Work stations
Collaboration	• Email System • Enterprise Content Management • IP Telephony • Video Conferencing
Application Design & Development	• Application Development For Handheld Devices • Application development framework • Business Rules, Logic and Objects • Commercial, off-the-shelf applications(COTS) • Geographic information system • Modelling design and development • Programming language for Application Development • Reporting tools • Software configurations Management (SCM) • Service Oriented Architecture • Smart Card Applications
Application Integration	• Message oriented Middleware • Object request brokers • Remote procedure calls
System Standards	• Application Servers • Backup Recovery • Business Intelligence • DB Connectivity and access technology • DBMS • Desktop O/S • Directory Services • Hardware Platforms • IT Operations Management • Mobile O/S • Portal servers • Server O/S • Storage Devices • Web Server

Technical Areas	Components
Specification for specific business areas	• Finance • Workflow and Web Services • e-Health • e-Learning • Legal • HR • E-News

7.5.2 NeGIF – Data Standards

The e-Government Interoperability Framework (e-GIF) mandates the adoption of XML and the development of XML schemas as the cornerstone of the government interoperability and integration strategy. A key element in the development of XML schemas is an agreed set of Government Data Standards (GDS). The data standards provide the detailed description of the data entity structure and its data elements.

The adoption of data standards for use across government will enable easier, more efficient exchanging and processing of data. It will also remove ambiguities and inconsistencies in the use of data across the government ministries, departments & govt. agencies. These standards apply to all systems that are mandated in the NeGIF and are for use in all other public sector interfaces.

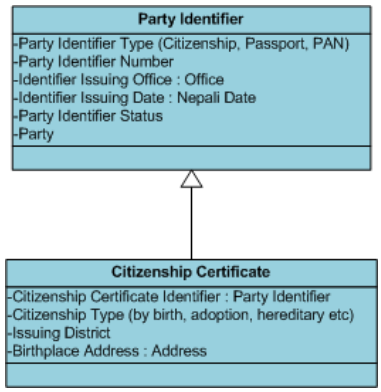
Data Standard Catalogue

The Data Standard Catalogue sets out the rationale, approach and rules for setting and agreeing at the set of Government Data Standards (GDS) to be used in the Govt. Data Schemas and other electronic interchanges of data involving the public sector, developed to support the e-GIF. These standards are defined at a logical (business) level and not at a physical database storage level. However it is recommended that they be used for specifying data storage at the business level.

The following structure/template is recommendatory to define data standards:

- Name
- Description
- Type
- Is Part Of
- Has Parts
- Data Format & Size
- Version
- UML Diagram
- XML Schema ID
- Validations
- Values
- Owner
- Based on
- Status
- Verification
- Comments
- Date Agreed

An example of the data standard for the Citizenship Certificate data entity is listed below as per the data standard template identified. The Nepal GEA Data Standard Catalogue document will provide the comprehensive list of the data standards for the identified common & segment specific data entities.

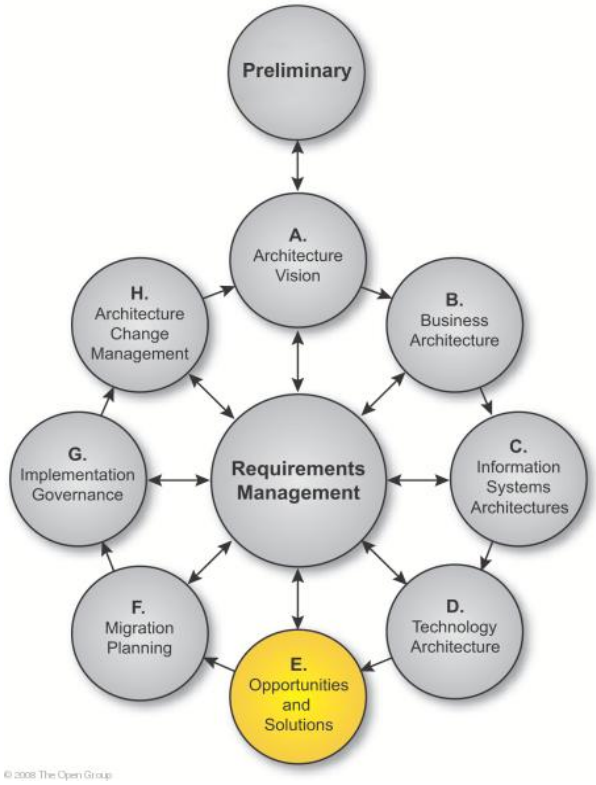
Metadata	Value
Name	**Citizenship Certificate**
Description	This is a specialized form of Party Identifier data element that captures citizenship certificate details of a citizen of Nepal.
Type	Generic Data Element
Is Part of	Party Identifier (SuperType)
Has Part	• Citizenship Certificate Identifier (extended from Party Identifier) • Citizenship Type (by birth, adoption, hereditary etc) • Citizenship Certificate Issuing District • Birthplace Address
Data Format & Size	*Refer to the format & size of the individual child elements in the Data Standard Catalogue*
Version	1.0
UML Diagram	
XML Schema ID	Refer to XML Schema (xsd) **PartyIdentifierDescriptiveType** Refer to XML Definition **CitizenshipCertificate** Structure
Validations	*Refer to the validation of the individual child elements in the Data Standard Catalogue*
Values	*Refer to the values of the individual child elements in the Data Standard Catalogue*
Owner	Ministry of Home Affairs, Nepal
Based on	
Verification	***If Descendent*** • Birth Certificate / Educational Certificate • Citizenship Certificates of Parents • Documents showing ownership of property in the District in family's name OR Migration Certificate issued by relevant CDO Office ***If married to a Nepali man*** • Citizenship Certificate of Husband • Marriage Certificate • NOC from Country of Origin • Documents showing ownership of property in the District in Husband's family name OR Migration Certificate issued by relevant CDO Office to Husband's family

Metadata	Value
	• Recommendation Letter from VDC Chairperson / Mayor / Municipality Secretary
Comments	
Status	Drafted
Date Agreed	

The detailed description for the recommended NeGIF standards, specifications & protocols has been covered in the "NeGIF Main Report".

8. TOGAF ADM Phase E – Opportunities & Solutions

8. Phase E: Opportunities and Solutions

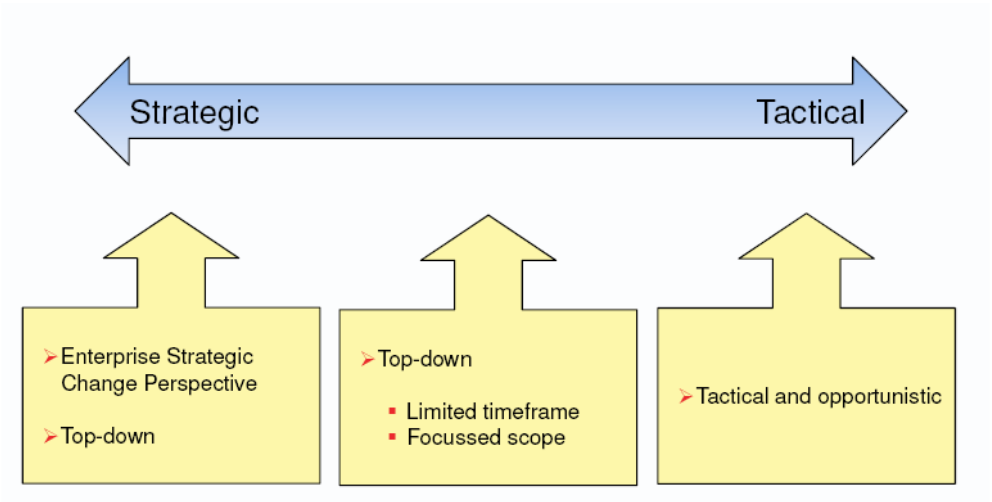


Phase Overview

The objective of this phase is to review, rationalize and consolidate the gaps & roadmap components identified for each architectural segment from Phase B to D and formulate a high-level Implementation and Migration Strategy (that will be part of the Implementation and Migration Plan) to illustrate the overall implementation approach required to move to the target architecture based upon the outline critical path resulting from the gap analysis.

Based on the consolidated architecture roadmap components identified from Phase B to D, a series of Transition Architectures is derived that show incremental progress from the Baseline Architecture to the Target to delivers continuous business value (e.g., capability increments) through the exploitation of opportunities to realize the roadmap components.

8.1 Opportunities & Solutions for Target Architectures



First phase directly concerned with how the Target Architecture will be implemented

- Corporate business and technical perspective
- Rationalize IT activities
- Group into project work packages

Consolidate, integrate and analyze extensive inputs, including

- Existing building blocks
- Case studies
- Consolidated gap analysis results

Simplify by ruthlessly reducing

- Number of building blocks to be created
- Overhead of Portfolio and Project Management

Create high-level Implementation and Migration strategy

- Organize work packages on critical path
- Recognize dependencies
- Co-existence and interoperability
- Recognize and manage risks

Conduct Impact Analysis

- Especially on existing IT systems

8.2 Rationalized & Consolidated Phase B to D Roadmap

The gap analysis results and the roadmap components from each one of the architecture phases, Business, Information Systems, and Technology Architectures (created in Phases B to D) were reviewed, their implications assessed with respect to potential solutions/opportunities and inter-dependencies, rationalized and consolidated in one long list that become the basis for the work breakdown structure and subsequent identifying of the transition architecture.

Phase A	Phase B	Phase C
Business Architecture		
• Uniform Connectivity: Secure, 24x7 Connectivity across all levels of Government across all Ministries / Departments	• National Data Repository: for secure and shared storage of all the Govt. Data from various Ministries / Departments	• e-Payment Gateway: for electronic transfer of Service Charges into Govt. Accounts and for receiving monies from the Government

• Simplification of Application Forms: with limited data inputs and auto-extracting of the data from relevant databases	• Auto-generation of Transaction ID: for each & every online transaction for Application tracking and future reference •	• Digital Copy of Certificates: for instant verification of various Documents / Instruments (e.g. Passport, Driving License, Land Certificate, etc.)
• Facility for Online submission of Service Requests: through Tele-Centres, National Portal and Mobile Devices	• Shared Service Delivery Infrastructure: utilizing Tele-Centres by: Encouraging various Ministries / Departments to route their G2C, B2C and B2B Services via the Tele-Centres a. Devising suitable Business Models (e.g. PPP) to meet CAPEX & OPEX of Tele-Centres and to generate employment opportunities b. Ensuring optimum spread & reaches (e.g. areas with high density of population to have more Tele-Centres, etc.) c. Standardizing Infrastructure & Connectivity Specifications for the Tele-Centres after taking suitable inputs from those Ministries / Departments whose services would be on offer via Tele-Centres d. Implementing suitable Communication Strategy to ensure that all are aware of the benefits on offer via Tele-Centres	
• Smart Verification of Applicants' Data: by electronic-interfacing between various Ministries / Departments for cross-verification and sharing of citizens' data		
• Government-wide Training Strategy: for Government Personnel across various levels to ensure effective usage of computerized systems		

Phase A	Phase B	Phase C
Data Architecture		
• Establishing the data architecture principles that will serve as the key architectural input or drivers to the government organizations for the design of the future state data architecture. • Defining enterprise core common data entities & data model which represents the core generic data entities to be	• Defining segment specific data entities & data model required for data sharing & exchange across the interoperability framework for the 16 short listed departments in scope.	• Definition of a centralized Master Data Management Hub solution that attempts to centralize and standardize the national master data set by accurately consolidating, cleansing, de-duplicating and reconciling the master data residing across disparate data silos. This will help maintain a single, trusted, accurate, complete and consistent

used across the various govt. units / departments of the Govt. of Nepal for data sharing & exchange across the interoperability framework • Establishing the government NeGIF data & metadata standards for the core common data entities		view of the citizens & business records across government units which could be the single point of reference for other departments thus allowing quick & easy identification of citizens at any touch point.
• Finalize the target data model for the IRD segment incorporating any additional data entities that would be required over and above the baseline data entities to support the to-be process re-engineering consideration as suggested by PwC team	• Supporting & guiding the data governance team in defining new segment specific data entities, updating the common data entities, govt. data schema & data standards as and when new departments will be ready to integration with the Nepal GEA infrastructure to expose new eServices	
• Definition of Govt. data schema in XML format for data sharing & exchange across the interoperability framework which will be based on the above ***common data specification.*** All departments that would expose its govt. services as eServices would have to adhere to the recommended common data exchange specification as defined in the Govt. Data XML Schema & the exchange package (or web service contract definition) to enable seamless information flow across eGIF	• Definition of Govt. data schema in XML format for ***segment specific data specification*** for data sharing & exchange across the interoperability framework. Specific departments that would expose its govt. services as eServices would have to adhere to the recommended segment specific data exchange specification as defined in the Govt. Data XML Schema & the exchange package (or web service contract definition) to enable seamless information flow across eGIF	
• Formalizing a data governance model & structure		
Phase A	**Phase B**	**Phase C**
Application Architecture		
• The Network infrastructure connecting GIDC/NITC with many other departments does not exists. Since the integration layer would reside in the NITC, this would need to be connected with department applications the integration layer would connect.	• Except for few applications (like License registration Management Systems, PIS, ePAN etc) do have a clearly abstracted business logic layer. The requirement of a business logic / service is essential in order to web service	• Application monitoring currently capabilities can be introduced for mission critical applications to monitor the health of the systems.

For ex: The Election commission is currently not network connected with NITC.	enable business logic.	
• Some of the applications, especially type1 applications need to be re-engineered to move it to online base applications.	• Common Application Authentication and authorization needs to be deployed.	
• Type 2 application those that are client server based applications also would need to be web enabled.	• Most of the department application would need re-engineering to integrate with the integration layer of the GEA.	
Phase A	**Phase B**	**Phase C**
Integration Architecture		
• NGSDG will enable a Service Oriented Architecture (SOA) and act as the Enterprise Service Bus for all the interactions between service consumers (the citizen and businesses) and various service providers (Government Departments) and even among Government Departments.	• Provides necessary connectors to interface with the applications developed at the Department level. • Capable of handling large number of transactions across the entire network, • Provide data and format transformation if any along with routing and filtering of data.	• Shared Services - In future, SDG Enterprise Service Bus has the capability to add additional functionality to support shared common services like Authentication, payment gateway interface, short messaging services, instant messaging services etc.
• Service enabling of department applications with NGSDG, department new & legacy applications can offer their services to various other consumers connected to the Enterprise Service Bus.	• Facilitate real time and near real time synchronization and co-ordination of inter departmental working, tracking all transactions of the Nepal Government.	
• Provide a common set of integration specifications and a single point access. • Security and Audit - Results in better tracking (auditing) and security of each service invocation and enforces government control through complete audit logs & time stamping of transactions		
Phase A	**Phase B**	**Phase C**
Security Architecture		
• Registration: Uniform centralized registration for all the application	• Authentication Centralized: Application should use the	• Administration: Centralized administration utility for all

	centralized authentication mechanism. No local user repository should be used to authenticate	application in the organization
• Authentication Federated: System should be able to use the centralized authentication scheme as well as application based authentication	• Integrity: All application should have session level security	• Alerting and Notification: Systems to raise security related events with severity defined and forward that
• Single Access point: Single point of entry for the all the application	• Policy based Authorization: Authorization should be controlled from the central user repository.	
• Identification: There should be a unique ID for all the users and application	• End to End Integrity: All application should use transport level security while interacting with other application.	
• Application Scan: All application should be scanned to check if there is any vulnerability.	• Auditing: All application should have auditing feature to track who performed a specific activity and when.	
• Configuration Hardening: All the application and hardware should be tweaked to ensure that a default property does not create any risk to the environment.	• Non Repudiation: Application should be capable to provide the prove the origin of data and recipient of the data	
	• Security Policy: Need to develop information , data and application security policy	
Phase A	Phase B	Phase C
Infrastructure Architecture		
• Data Center Consolidation	• Shared Network Adoption	• Configuration Management Database
• Security a. Shared Security Services b. Shared Security Infrastructure c. Network Security in a Secure Segment	• State Wide Area Network	• Infrastructure Governance
	• State Data Center a. Data Centre Operations and System Management – ITIL b. Security Considerations for the Data Centre c. Data Centre Security	

	Framework d. Data-centre Automation	

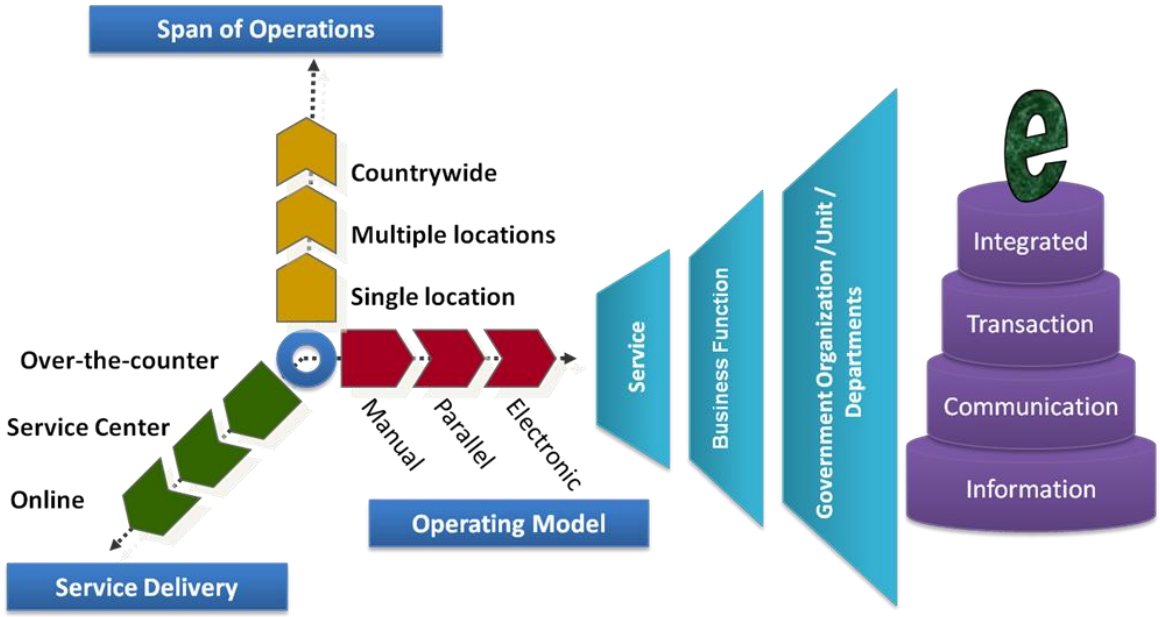
8.3 High level Implementation & Migration Strategy

Based on the above consolidated & rationalized individual architecture roadmaps, an overall implementation / solutions strategy and approach is derived that will guide the Target Architecture implementation and structure of the Transition Architectures.

As per the proposed implementation strategy, the service delivery of the government services to citizens as e-Services will typically be achieved in a phased manner depending on the existing application systems & network infrastructure maturity of each department in leveraging the proposed service delivery infrastructure for delivering its services. The aim is to provide the immediate facility for citizens to submit the online service request forms for the service identified by the departments from the national portal. Based on the mode of operation the submission, processing and status tracking of the services will be done either –

- In the national portal if the departments cannot connect to the service delivery gateway
- In the departmental systems if the departments can connect to the service delivery gateway

The transition from manual to electronic mode of operation the future state service delivery model is illustrated below -



Service Delivery Operating Model

The operating model for the delivery of e-Services from the national portal through electronic forms typically transitions from Manual to Electronic –

- Manual
    - The national portal will host the government service e-Forms. Citizens can login to the national portal, fill and submit the form.

- The national portal will store and capture the service request in the portal infrastructure which will serve as the central application for capturing the service request.
- Departments do not have any application system & network infrastructure to connect to the eService delivery gateway. A designated person will download the service request from the national portal and start processing it manually as per the current process of the department.

- Parallel
  - The national portal will host the government service e-Forms. Citizens can login to the national portal, fill and submit the form.
  - The national portal will store and capture the service request in the portal infrastructure which will serve as the central application for capturing the service request.
  - Departmental application system exists but is not integrated with the eService delivery gateway. A designated person will download the service request from the national portal and start processing it through the departmental system.
- Electronic
  - The national portal will host the government service e-Forms. Citizens can login to the national portal, fill and submit the form
  - The national portal will publish the service request directly in the eService delivery gateway.
  - Departmental system is integrated with the eService delivery gateway and capable of picking up the service request and processes it.

Service Delivery Channels

The service delivery channels typically transitions from –

- Manual – Over the Counter
  - This is the typical manual process where the service request form will be collected, filled and submitted manually over the counter by the citizens
- Semi Manual – Service Centers
  - This is a semi manual approach where citizens in remote location can avail the service request facility provided by local service centers (similar to tele-centers) who will facilitate in online submission of the forms on behalf of the citizen. All supporting documents will be handed over the service center staff for verification.
- Electronic – Online through National Portal
  - Citizens can directly avail online service facility from the national portal, fill and submit the form, uploading supporting documents.

8.4 Identity Transition Architecture

Based on the rationalized and consolidated architecture roadmap components identified from Phase B to D in section 8.2, a series of Transition Architectures is derived that show incremental progress from the Baseline Architecture to the Target to delivers continuous business value (e.g., capability increments) through the exploitation of opportunities to realize the roadmap components.

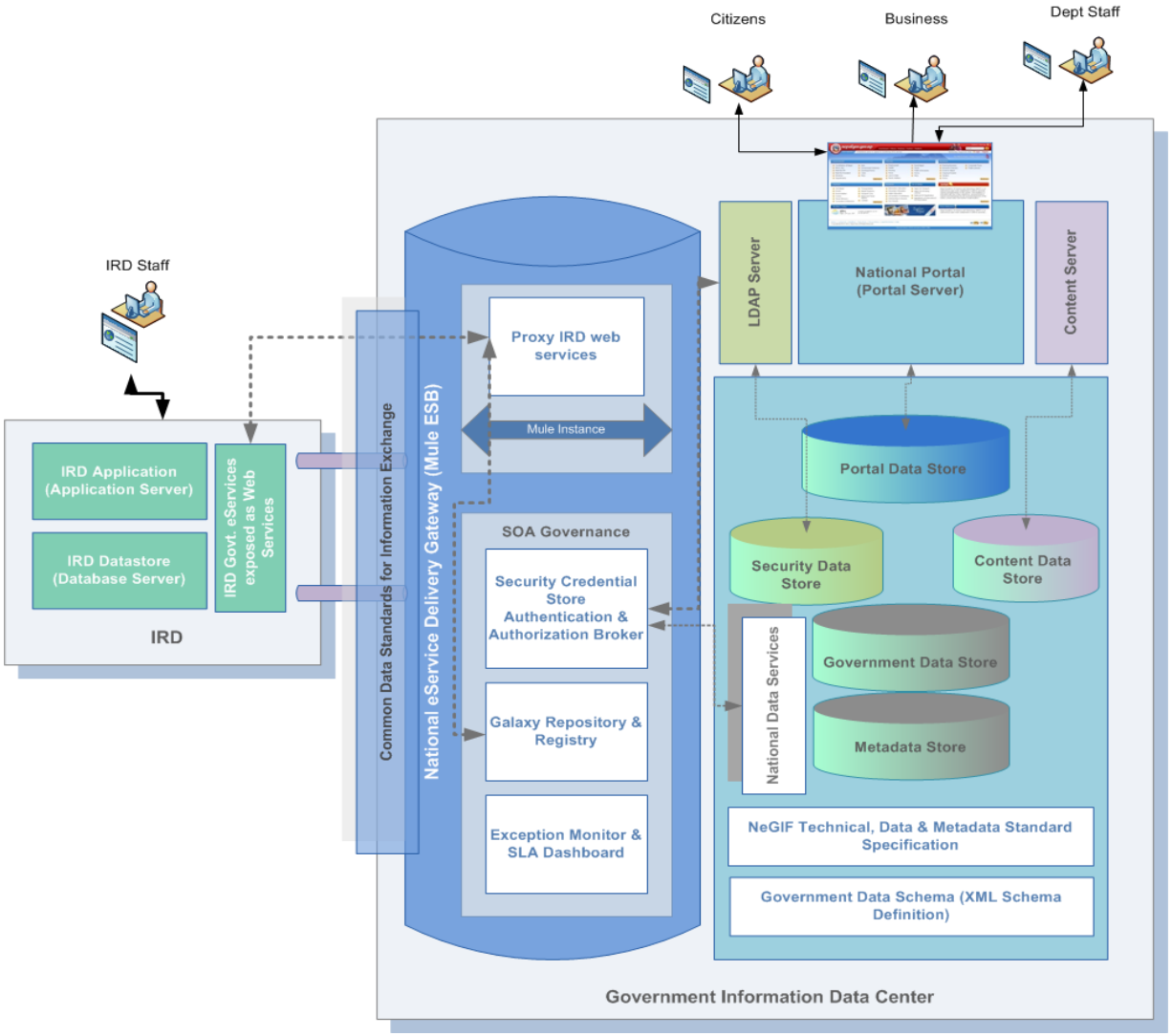
For the complete transformation of the proposed Nepal GEA from baseline to target, a phased approach will be followed from transitioning from the baseline to the target architecture for the Govt of Nepal. An advantage of using the phased Transition Architecture approach is that government/organizations find that a change of architecture has too much impact on the organization to be undertaken in a single phase.

The following are the indicative phases / transition state identified. The timelines of the transition state / phases mentioned here would depend on the GEA Steering committee and the readiness of the individual departments ICT projects/programs. This section of phase wise approach reflects the indicative sequence of the projects to be undertaken to avoid conflicts of dependency of the projects and solutions.

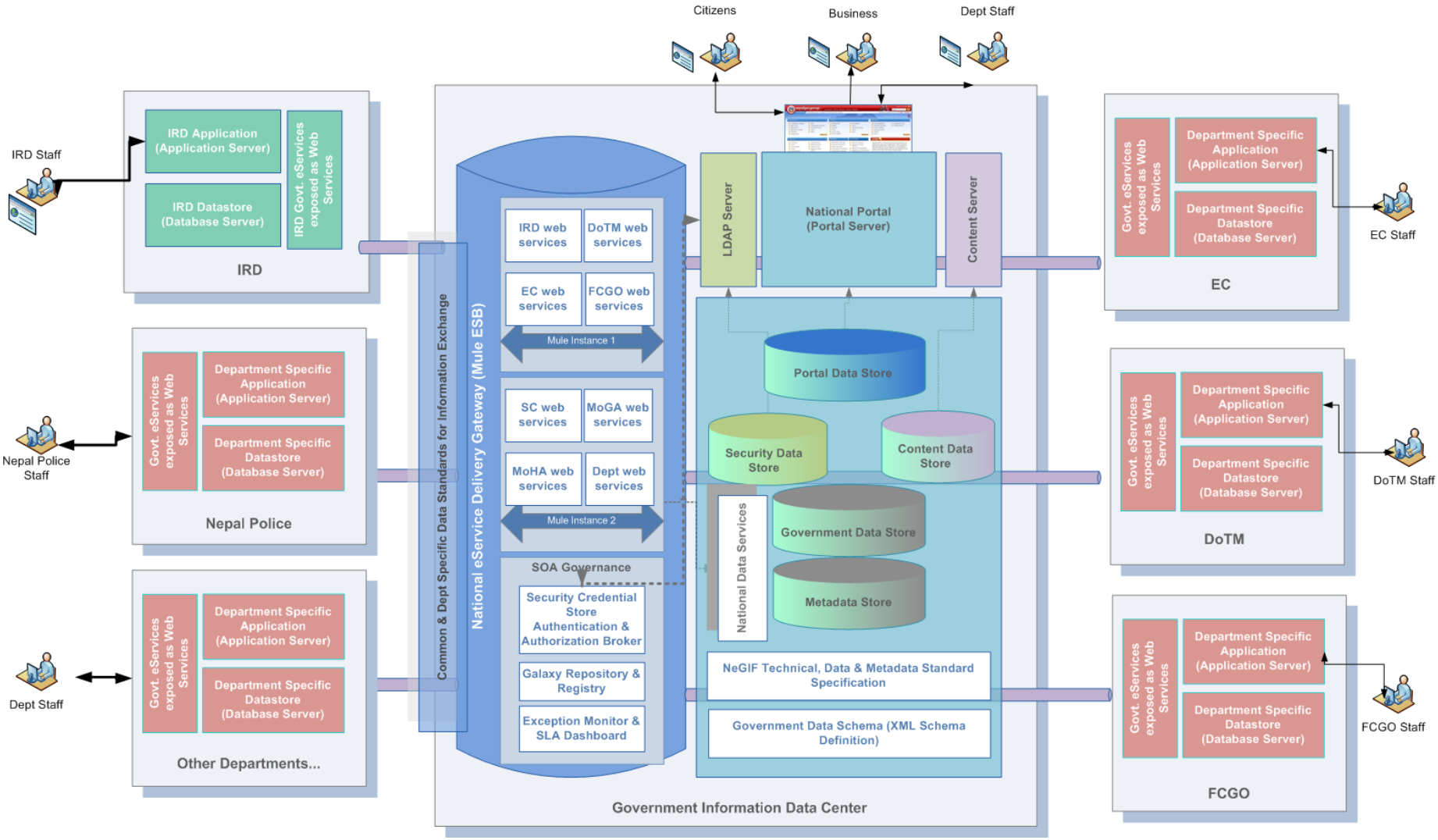
Transition State 1 (Phase A)	Transition State 2 (Phase B)	Transition State 3 (Phase C)
1. Establish Nepal eService Delivery Gateway middleware platform based on SOA for all interactions between service consumers & providers 2. Deployment of Mule ESB with security / audit	1. Mule to provide necessary connectors to interface with department applications	1. Add common shared services like payment gateway interface etc 2. Integration with ePayment gateway
3. National portal deployed with static content	2. National portal to incrementally host eServices in phased manner	3. National portal to incrementally host eServices in phased manner
4. Setup of centralized user registration (LDAP based) for national portal users 5. Federated authentication approach adopted	3. Centralized user registration (LDAP based) for all applications with unique ID for all users & applications 4. Gradually move towards centralized authentication 5. Enforce policy based authorization to be controlled from central user repository 6. Enforce session level security 7. Support non-repudiation	4. Enforce Digital signature & PKI infrastructure 5. Alerts & notification features
6. Establish common data standard for information exchange 7. Define & publish Govt. data XML schema	8. Establish segment specific data standard for information exchange 9. Define & publish segment specific Govt. data XML schema	6. Setup of National Data Repository 7. Establish Master data management solution
8. GIDC infrastructure setup to host ESB & national portal	10. GIDC to host other ICT project departments applications	
9. Establish 24*7 uniform network connectivity with GIDC & IRD department application	11. Setup of Nepal wide area network 12. Establish 24*7 uniform network connectivity with GIDC & other department applications	8. Establish connectivity with Tele-centers

Transition State 1 (Phase A)	Transition State 2 (Phase B)	Transition State 3 (Phase C)
10. Pilot Implementation with IRD with national portal to host IRD eServices 11. Segment specific data standards for IRD to be defined 12. Web services for IRD eServices to be defined 13. ESB service enabling of IRD web services 14. National portal to provide interface to citizen, business & departments to avail IRD eServices	13. Departments with completion/near completion of ICT project (e.g. EC, Nepal Police, NTA, FCGO etc) to connect to service delivery gateway 14. Web services for the department specific eServices to be defined 15. ESB service enabling of department specific web services 16. National portal to provide interface to citizen & business to avail department specific eServices 17. National portal to provide interface to other departments with no department specific applications to avail department specific eServices 18. Service consumers (other departments) for G2G services to connect to ESB infrastructure to avail department specific eServices	
15. Formalize EA Governance Model		
16. Departments with ICT projects at various stage of maturity to comply with the Nepal GEA & eGIF specification 17. Design / re-design based on GEA specifications 18. GEA governance committee to review design & ensure compliance with GEA specs		

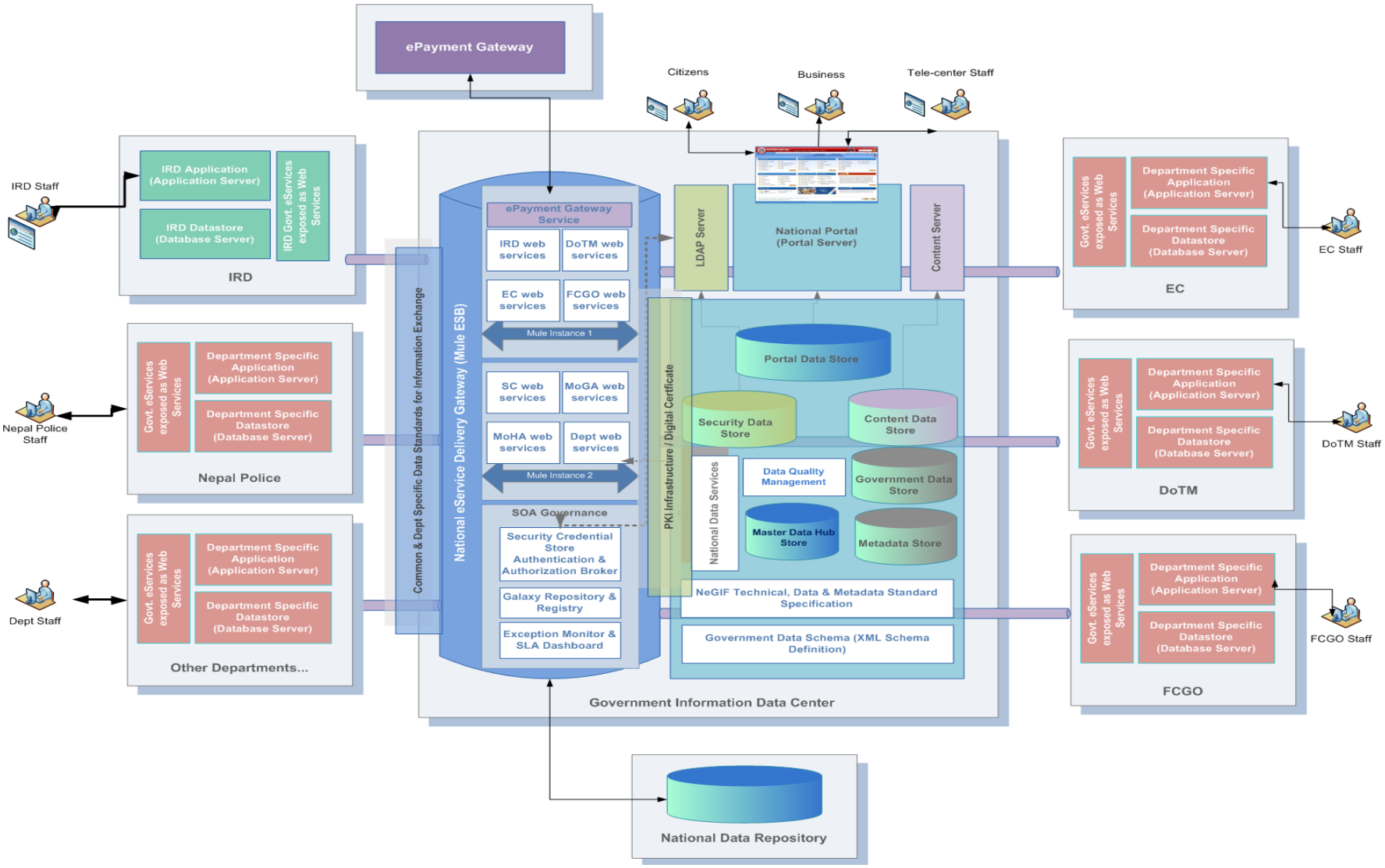
Transition Architecture – Transition State 1



Transition Architecture – Transition State 2



Transition Architecture – Transition State 3



8.5 Create Portfolio & Project Charters

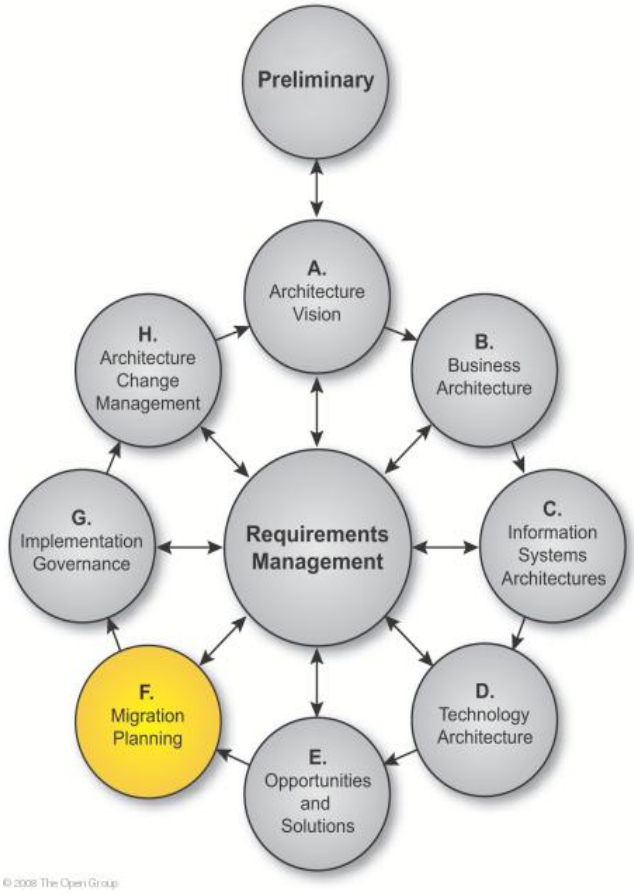
Based on the transition architectures derived to incrementally progress from the baseline to the target, the approach in this stage is to complete the portfolio and major project charters with their deliverables being grouped into increments and scheduled for release within Transition Architecture increments. These architectures provide the enterprise context allowing projects to start their system development methodology initiation, planning, and requirements assessment phases.

The major activity in this stage is to review and consolidate the portfolio and potentially major project charters and ensure that their architectural outcomes are clearly defined. These architectural outcomes will give the portfolios enterprise context and determine the "fit" and "value" of the deliverables for governance.

The list of strategic portfolios/projects to be grouped into each transition increments will depend on the GEA steering committee and the readiness of each department specific ICT programs/projects.

9. TOGAF ADM Phase F – Migration Planning

9. Phase F: Migration Planning



Phase Overview

The main focus of Phase F is the creation of a viable Implementation and Migration Plan in co-operation with the portfolio and project managers.

Phase F activities include assessing the dependencies, costs, and benefits of the various migration projects. The prioritized list of projects will form the basis of the detailed Implementation and Migration Plan that will supplement the architectures with portfolio and project-level detail assigning tasks to specific resources.

The Implementation and Migration Plan is part of a family of plans issued by enterprise management frameworks that have to be closely co-ordinated to ensure that business value is delivered and that the resources are made available to complete the necessary work. This phase ensures that all concerned agencies outside of the enterprise architecture world are aware of the scope and import of the Implementation and Migration Plan and its implications with respect to their activities.

Finally, the architecture evolution cycle should be established to ensure that the architecture stays relevant, and lessons learned should be documented to enable continuous process improvement.

Definition of the **Implementation & Migration Roadmap** for Nepal GEA initiative would require major inputs, participation, collaboration and co-ordination across the government departments and GEA Governing Council and depends on the maturity & readiness of the department specific ICT programs/projects with GEA. This phase will be more applicable & complete at a later stage once the various building blocks (ICT projects / programs) of the transition architecture have been finalized.

However the brief approach typically followed during this phase has been outlined below to provide a guideline for departments initiating new ICT projects / programs.

9.1 Business value for each Project

The approach in this step is to establish and assign business values to all of the ICT projects and project increments. The intent is to first establish what constitutes business value within the organization, how it can be measured, and then apply it to each one of the projects and project increments.

9.2 Estimates for resource requirement & project timing.

The approach in this step is to determine the required resources and times for each project and project increment and provide the initial cost estimates for the projects. The costs should be broken down into capital (to create the capability) and operations and maintenance (to run and sustain the capability). Note that operations and maintenance funding will have to commence as soon as the first increment is delivered to the operations management organization, so it has to be clear from the outset where both types of funding are coming from (and whether they are affordable). Excellent examples of the challenges are the cost of software maintenance and the costs associated with upgrading (including some of the custom software modifications that were made).

9.3 Prioritization of Migration Projects

The objective of this step is to prioritize the projects by ascertaining the business value of the artifacts delivered by the projects against the cost of delivering them. The approach is to first determine, as clearly as possible, the net benefit of all of the solutions delivered by the projects, and then verify that the risks have been effectively mitigated and factored in. Afterwards, the intent is to gain the requisite consensus (often at the enterprise level) to create a prioritized list of projects that will provide the basis for resource allocation

Prioritization criteria will include the key business drivers identified in Phase E as well as those relating to individual stakeholders' agendas.

Some of the key prioritization criteria that could be considered include:

- Would have high-visibility when implemented
- Would enhance the efficiency (by providing more Lead-time, by easing the flows, etc.) of process participants
- Ability of stakeholders to handle change, whether stakeholders would be ready to accept & adopt to the changed process and services
- Would reduce overall cost for recipients to avail the service
- Impacts a large number of stakeholders
- Consolidation of services
- A goal to have a minimum of "interim" solutions (they often become long-term/strategic!), Would be a Long-term solution and can be persisted with for a feasible period of time
- Would have suitable IT Systems to support reengineered flows
- Would give rise to suitable Web Service(s)

9.4 High level Implementation Roadmap and Migration Plan

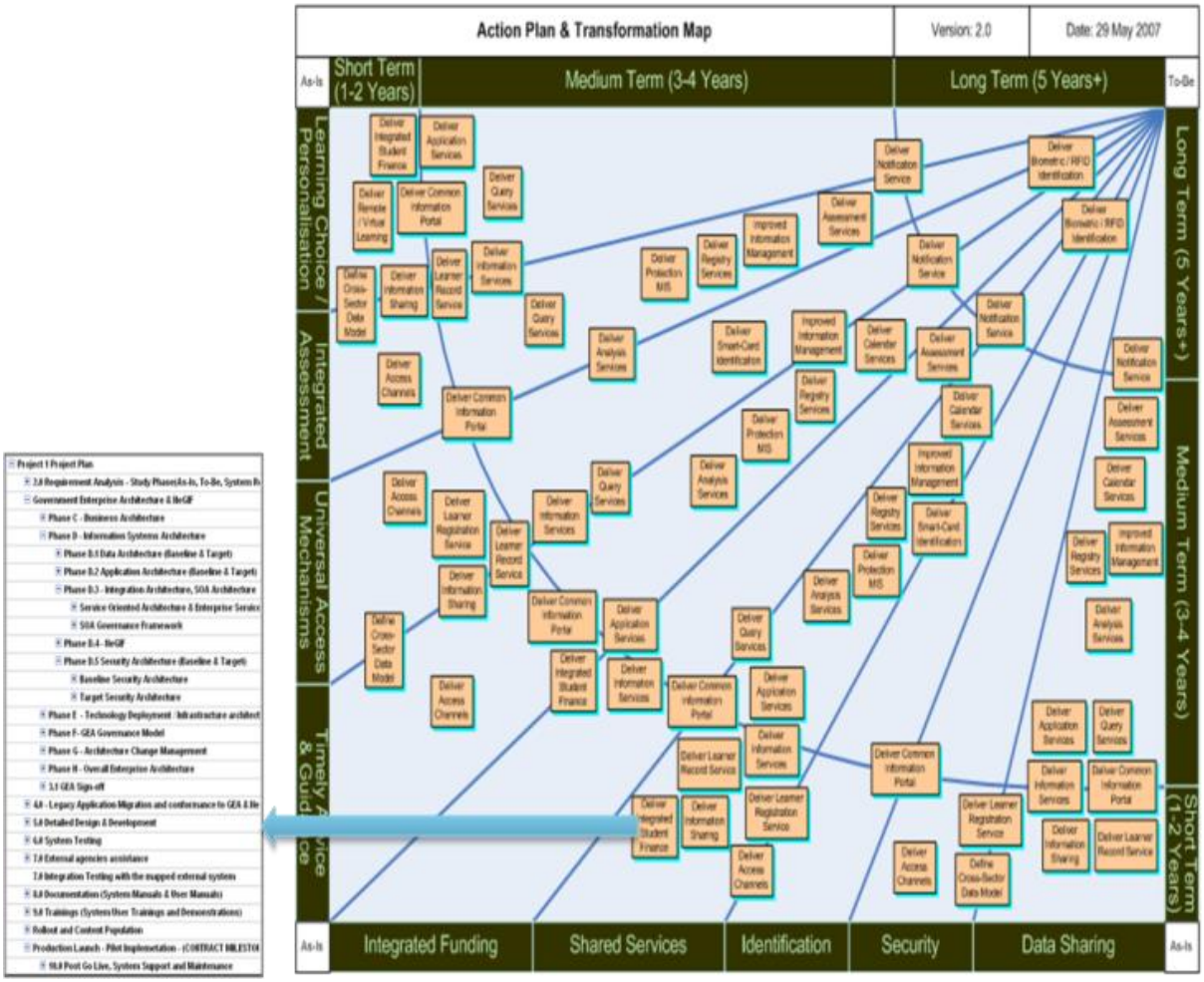
The objective of this step is to generate the Implementation and Migration Plan sequence and details. The main feature of architecture planning is that there will be a great deal of concurrent ICT projects / program activities and the Implementation and Migration Plan will be the binding all of these artifacts together. In Phase E and in previous steps within Phase F, most of the project /portfolio planning actions will have been completed and this step brings all the detail together into an overall plan.

In this step, the major task is to formally integrate all of the projects, project increments, and activities as well as dependencies into a project plan, preferably using a project scheduling and management tool that use a standard methodology such as Critical Path Method or the like. The Transition Architecture states, with their

defined business value, will act as portfolio milestones. Also it is ensure that all external dependencies are captured and included. For example, a delay in completing & formalizing the NID legal framework and subsequent implementation of NID project might prioritizing the EC ICT project in early transition architecture state to consider the EC voters profile as the trusted source of citizen data.

Additionally project schedule also needs to be incorporated in the plan. Projects should take their assigned roles and ensure that their deliverables are thoroughly planned. Their project plans should be in part rolled up (in part or in their entirety) into the Implementation and Migration Plan. It is advisable for the enterprise architect to ensure that the plan is adjusted with the overall implementation & migration plan to accommodate the project concerns if any so that it has the best chance for success. This activity results in the finalized Implementation and Migration Plan.

A typical example of an implementation roadmap and migration plan is shown below -



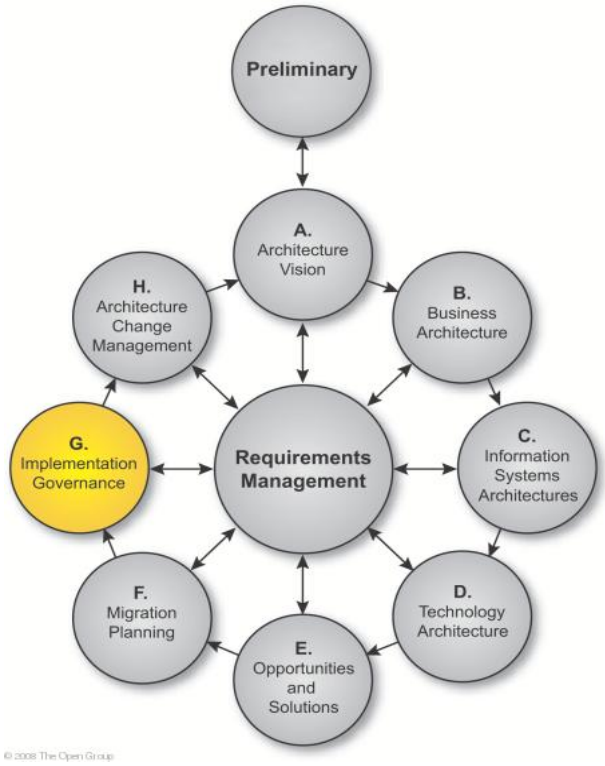
9.5 Architecture evolution cycle

Enterprise architectures must be kept up-to-date or they will slowly become irrelevant, superseded by portfolio and/or project architectures. The time required to translate a change from the strategic to the project architecture is significant and must be understood and catered for within the organization.

Furthermore, lessons learned are crucial within a learning organization and should be documented and assessed as part of the enterprise evolution process. The architecture evolution cycle will both impact and be governed by the enterprise's Architecture Change Management (Phase H).

10. TOGAF ADM Phase G - Architecture Governance

10. Phase G: Architecture Governance



Phase Overview

Enterprise architecture is a practice that needs to be sustained for a successfully governed enterprise. Without Governance the departments could be following its own strategy, policy, guidelines and standards without any alignment to the overall e-GMP. In order to ensure EA is a living and breathing practice, it needs to be governed.

This will involve a lifecycle that captures the IT lifecycle of any ICT project due to be developed by the departments. This lifecycle will address various facets of Governance such as addressing the IT Operations, IT Program Management, Risk Compliances, IT Strategy and Service Orientation of Applications.

The following figure illustrates the different dimensions on overall EA Governance of a country. For each of the dimension the methodology is also noted.

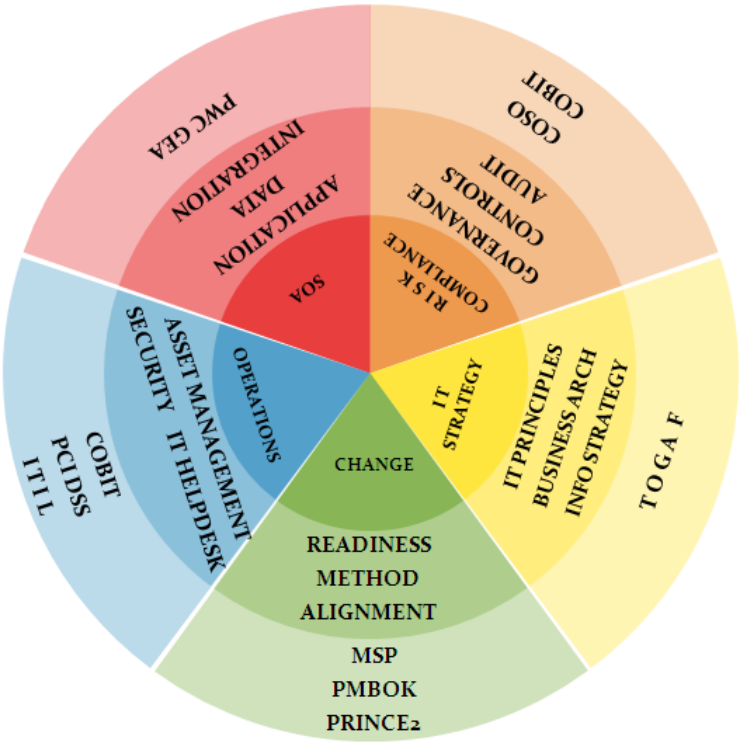


Figure Nepal GEA – Governance Dimensions

The lifecycle will involve certain actors/roles across departments at different milestones in-order to ensure the Enterprise Architecture (EA) and the eGovernance Interoperability Framework (NeGIF) is followed and is aligned to the overall objectives of the ICT projects. The following figure illustrates the different milestones in the progress of overall IT and eGovernance maturity and the respective governance mechanisms.

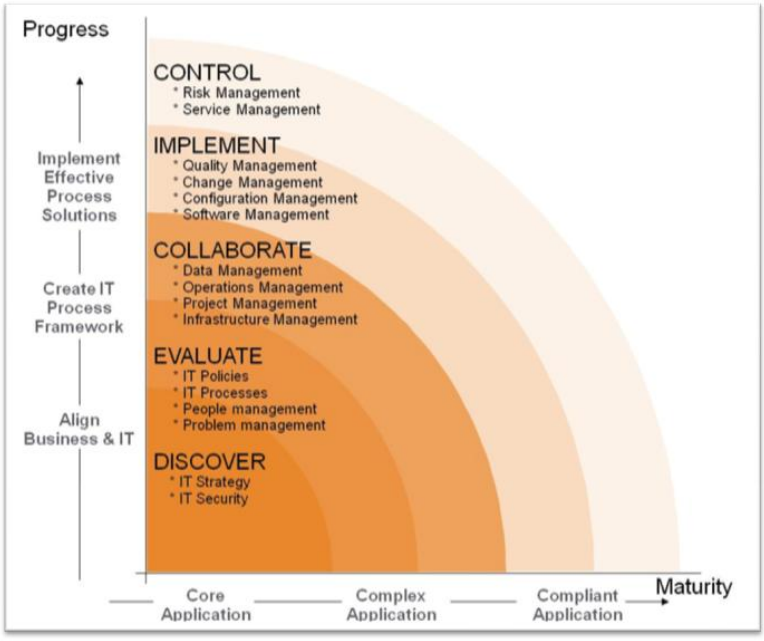


Figure: Nepal GEA – Governance Milestones

Objectives

The objective of this Phase is to formulate recommendations for each implementation project, and govern and manage an architecture contract covering the overall system implementation and deployment. The system is then implemented and deployed during this phase. Following is the list of objectives

- Formulate generic architecture recommendations to be utilized by each implementation project.
- Adherence to sustainable governance model for implementation of any ICT project.
- Construct an Architecture Contract to govern the overall implementation and deployment process.
- Perform appropriate governance review functions while new systems are being implemented and deployed.
- Ensure conformance with the defined architecture standards by implementation projects.

The Approach

- This phase brings together all the information for successful management
- of the various implementation projects
- Recommended approach is to deploy the Target Architecture as a series of incremental transitions, each delivering business benefit in its own right:
    - Establish an implementation program that will enable the delivery of the Transition Architectures agreed for implementation during the Migration Planning phase
    - Adopt a phased deployment schedule that reflects the business priorities embodied in the Architecture Roadmap.
    - Follow the organization's standards for corporate, IT, and architecture governance
    - Use the organization's established portfolio/program management approach, where this exists
    - Define an operations framework to ensure the effective long life of the deployed solution
- This phase establishes the connection between architecture and implementation organization
    - Using the Architecture Contract
- Implementation Governance is closely allied to overall Architecture Governance
- Key aspect of the phase is ensuring compliance with the defined architecture(s)
    - Implementation projects
    - Other ongoing projects within the enterprise

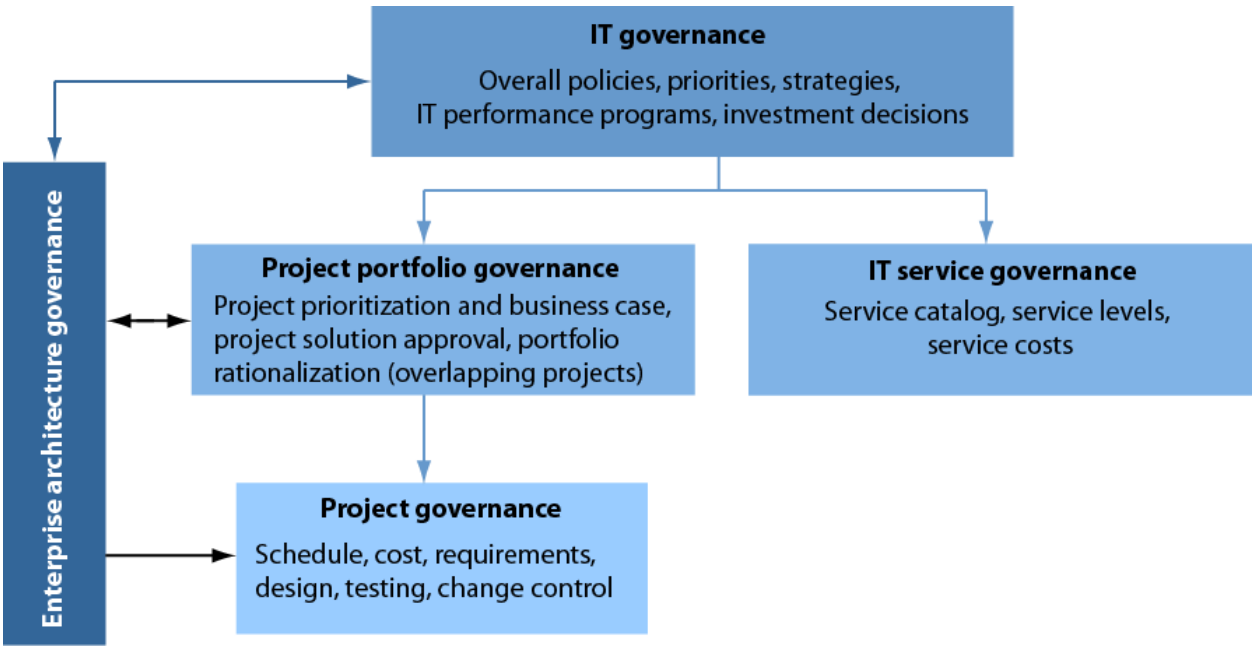
Enterprise Architecture Governance is an aggregation of multiple architecture governances such as SOA governance, Data Governance, Application Governance, Technology/infrastructure governance and IT Security governance. Each of this Governance has its lifecycle to govern with the identified roles ensuring the adherences to the standards around individual milestones.

10.1 Need for GEA Governance

- Making enterprise architecture effective involves the substantial issue of attempting to affect the behavior of staff not under direct control, which brings with it serious political difficulties that can undermine the best of efforts.
- Periodic review is critical to determining what is working and what needs improvement. Architecture groups that attempt to move forward without regular feedback on their value to their organization risk dissipating their resources rather than focusing on high-impact areas.
- Once the architectures have been defined, it is necessary to plan how the transition architecture that implements the architecture will be governed through implementation.

10.2 Introduction & Approach to EA Governance

Enterprise Architecture Governance Is Part of IT Governance at Multiple Levels



IT Governance Defines How Enterprise Architecture Fits Into the Organization's Practices

The role of EA in governance should be defined by IT policy. Ideally, IT policies should lay out the role of the EA function in setting directions, influencing plans, and approving project decisions.

IT strategic plans should drive and be informed by EA road maps. IT strategic plans can cover a wide range of concerns, depending upon what is important to the organization, but when considering alignment with business drivers and plans, IT planners must reference EA "to-be" states and associated road maps.

The EA function should participate actively in all governing bodies. IT organizations typically implement governing bodies, such as IT steering committees for major strategic priorities, or operating and program management committees to track more localized decisions. EA group heads should use the IT steering committee to put the stamp of approval on the EA program, but they should also decide which governing boards to sit on. And CIOs must recognize EA governing boards, such as an architecture review board, as an extension of IT governance.

EA in Project Portfolio Governance

As the Enterprise Architecture has defined application and technical architectures, the EA team can assess whether projects' proposed solutions are appropriately aligned with the standards. Through project portfolio planning, the team can uncover interdependencies between projects that can affect feasibility and cost, or it can determine if there are opportunities to combine projects to build better solutions at lower cost and in less time. Conversely, portfolio assessment provides input to EA regarding ongoing business needs, which feed into architecture needs and priorities. At this level of governance:

Chief architects sit on portfolio management committees. The portfolio management committee reviews project initiatives proposed by departments and IT and makes decisions on project priority, scope, and high-level solution architecture. For example, these committees make decisions on build versus buy, whether

the project scope should be broadened or narrowed to accommodate other initiatives, and when to initiate projects based upon available resources.

Without architecture participation, this committee can do little more than assign resources to projects based upon business demand. With architecture participation, it can help maximize the value to the organization through better designed, scoped, and sequenced initiatives.

PPM review processes combine the project business case with architecture road maps. Architects can use the knowledge from planning and road-map-building activities to provide insights into decision-making at portfolio review sessions. Once the organization learns the value of EA input at these meetings, project business sponsors and application project leads will seek out EA team members ahead of decision-making sessions to rationalize their projects and resolve any potential conflicts that could inhibit funding.

Project Governance Ensures Consistency between EA and Day-To-Day Project Decisions

Project governance is the most basic level of EA governance and is common to most EA programs. EA provides detailed guidance regarding technology selection and design best practices to ensure that projects adhere to the technology strategy and pass quality criteria. EA groups use two basic governance approaches: collaborative and review. In the collaborative model, a solution architect provides guidance from the earliest stages of a project, either as a full-time or part-time consultant to the project team. In the review model, an architecture review board acts as a gating process to approve progress to the next project stage. EA gets involved in project governance at three points in time:

Prior to design. Architects examine requirements and test assumptions regarding the need for scalability and integration with other applications. Early involvement at the requirements stage enables them to identify patterns that can jump-start the design process and obviate one-off development work. As organizations adopt service-oriented architecture (SOA), early involvement will also enable architects to determine which available services can be employed in the project. Guidance at this stage is most typically provided via the collaborative consulting model, although some EA groups employ early "informational reviews" to enable early-stage brainstorming via architecture review boards. Guidance in this early stage is extremely effective and can obviate the need for the "policing" flavor of reviews later in the development cycle.

Prior to construction. EA review at the end of design, as a gating process to the construction stage, is the most common type of EA governance. EA teams, typically by architecture review board but sometimes by the collaborative process (especially for lower-impact projects), scrutinize projects for adherence to standards and design best practices. The review determines whether the design addresses quality attributes for security, performance, reliability, and maintainability. This type of project governance is very effective, but if it is the first involvement of architects on a project, it gives EA governance the flavor of a policing action and can become a source of organizational conflict.

Prior to implementation. In IT organizations with an advanced degree of process orientation, projects are reviewed again post-construction to ensure that the project adhered to all infrastructure standards and that it performed in testing as expected. This is an uncommon checkpoint, and where it exists, EA participates in, rather than drives, the process.

Governance Provides a Feedback Loop to Enterprise Architecture

EA governance processes increase the degree of interaction between the architects and the business decision-makers, IT management, project sponsors, and application development team leads. They create feedback processes that ensure that the EA program does not simply dictate the EA view of how the future should be, but rather, constantly brings current-day needs and priorities into the mix to provide a strong dose of reality to EA's planning activities.

Every Organization customizes EA Governance to its needs

Because all firms are different, they approach governance differently. A large organization will likely have more formalized processes and roles, whereas a smaller organization will emphasize consulting relationships. Similarly, an organization using extensive outsourcing will need to approach architecture governance differently than one where most development is in-house by, for example, emphasizing documented assessments and specifications.

GOVERNANCE ISN'T ABOUT POLICING — IT'S ABOUT RESULTS

Organizations that have implemented successful governance models have gained management support, as well as widespread buy-in from the IT practitioners, because they have effectively communicated the value of EA to these audiences. While no organization is conflict-free — nor should it wish to be — participants in successful governance processes welcome architects' input and consider EA to be a valued and integral part of planning and development. To ensure that governance processes don't sidetrack your organization with unproductive conflict but instead move you closer to your goals:

Build your governance approach starting with IT governance. When EA governance is viewed by the organization as standalone from the core governance processes, it loses clout. Rather, you should ensure that the connection of the EA governance processes to the goals, plans, and success of the overall organization is made clear.

Be inclusive in planning and EA development activities. When individuals have participated in EA plan, road map, and artifact development, they tend to take ownership of EA's goals and become part of the solution. Thought leaders left out of the loop are potential opponents to the spirit of EA governance processes.

Integrate EA with IT planning and prioritization. IT organizations are often challenged during the planning process by the volume of business proposals and the difficulty in assessing their implications to IT resources and technology. The EA group should offer its knowledge of the enterprise's systems and its design skills to help shape these proposals into projects that best maximize business benefits and IT capability.

Get involved early in project governance. The best time to begin project governance is before decisions have been made. When projects progress from a twinkle in the project sponsor's eye to a meaningful set of requirements, get an architect to start brainstorming solutions with the application team.

Approach 1: Publishing architecture documentation

- This is the if-you-build-it-they-will-come approach to governance.
- Architecture documentation is made available and the IT community is expected to simply fall in line.
- While architecture documentation can be an important part of governance processes, this approach never works by itself.
- No processes of IT practitioners are engaged, and the impact of simply publishing architecture documentation is usually nil when no governance processes exist.
- However, publishing the documentation is a starting point which could be referred at any stage for adherence to standards. This serves as a reference point at any stages of the project.

Approach 2: Controlling the IT purchasing process

- The Purchasing team that purchases IT products and services should report within IT.
- The products this team buys, the purchasing cycle, the speed of change and the liability associated with these products are unique to IT.
- Furthermore, by controlling purchasing, it can become a tool for guiding people to buy products that are consistent with the architecture.

- A purchasing process that makes it very easy to buy products that are aligned with the architecture and onerous to buy nonstandard items encourages compliance with standards.
- At the very least, the purchase of nonstandard technology because of ignorance of standards is eliminated.
- Linking IT purchasing processes to architecture standards is a key way to institutionalize a concern for enterprise architecture into an organization's culture.

Approach 3: Convening Architecture Review board

- Architecture review boards are bodies that convene regularly to review the architecture of new initiatives.
- The architecture review is intended as a gating process that approves or rejects designs based on their adherence to the established architecture and general design principles.
- It can be extremely effective when system development and project management processes and methodologies are in widespread use and the architecture review is included as a standard step in those processes.
- While few architecture review boards rule with quite the iron fist implied by their ostensible approve/reject authority, the very existence of the architecture review process can have a dramatic impact on technology selection and application design.
- Drawbacks of this governance method include the potential bureaucracy of adding the review step, the difficulty in gaining widespread participation in some environments, the lack of authority to modify designs and the potential backlog of reviews in dynamic environments and the resulting bottleneck.

Approach 4: Providing Enterprise architecture consulting

- The most effective and least bureaucratic governance process is the use of external architecture consultants at the early stages of a project to provide guidance regarding technology selection and general design expertise.
- As opposed to the policing process of the architecture review board, the use of a consulting model achieves governance in the form of proactive design guidance. Having internalized the architecture standards, the consultants can guide the developers towards a design consistent with the technology strategy.
- While the consulting process can be a win-win for the architecture effort as well as the development community.
- This Approach is one that can contribute significantly to a streamlined approach to architecture governance.

10.3 Architecture Review Board

- Architecture review boards meet to approve or reject project Architecture / designs.
- Architecture reviews should occur before a project team exits the Architecture & design phase and before the project enters development / Implementation phase.

- In addition to simple approval/rejection, recommendations for bringing an errant design in line with the technology strategy can also result, in the form of conditional approvals.
- The review board membership should cover the required spectrum of technology expertise but it should also include representation from any departmental entities that expected to adhere to architecture standards. In most organizations, a concern for adherence to the architecture is effectively ingrained into the IT culture only when there is a strong sense of ownership and participation.
- The core of the board is made up of members of the central architecture group, with the head of the group acting as chair and final decision-maker. The process should include discussing the project and voting on approval; however, approval should not be a matter of simple majority. Any conflicting opinion should be resolved rather than brushed aside, with the chair making the decision to escalate conflicts or take them offline. The review board is not the place for endless discussions on the subtleties of designs; it is rather a straightforward process of presentation, discussion and vote, with one-half hour maximum allotted to each project. Any review that cannot fit into that time constraint must be dealt with in offline meetings.
- Project attendees at architecture review board meetings should include the business sponsor of the project and the application architect. The standing members of the architecture review board should include the core members of the central architecture group and the architecture representatives of the infrastructure and development organizational units.
- The review board membership should cover the required spectrum of technology expertise but it should also include representation from any political entity expected to adhere to architecture standards. In most organizations, a concern for adherence to the architecture is effectively ingrained into the IT culture only when there is a strong sense of ownership and participation.
- The core of the board is made up of members of the central architecture group, with the head of the group acting as chair and final decision-maker. The process should include discussing the project and voting on approval; however, approval should not be a matter of simple majority. Any conflicting opinion should be resolved rather than brushed aside, with the chair making the decision to escalate conflicts or take them offline. The review board is not the place for endless discussions on the subtleties of designs; it is rather a straightforward process of presentation, discussion and vote, with one-half hour maximum allotted to each project. Any review that cannot fit into that time constraint must be dealt with in offline meetings.
- The timing of reviews (that is, the end of the design phase) can be problematic - once the design is complete, there can be significant business pressure to move into construction to keep to schedules and budgets, and rejection or modification by the architecture review board can be seen as a bureaucratic obstacle to be sidestepped or forced out of the way. Such conflicts test the authority of the board and frequent failures to effectively reject designs can cause the board to appear as a useless rubber-stamps process. Reviewing a project early in the design phase can be useful, but most often a significant amount of detail is not available and the architecture review board should not grant approvals to incomplete designs. This basic conflict between the need for a completed design for review and approval and the unwillingness of business sponsors to delay projects that the architecture review board votes to reject is the chief difficulty of the architecture review board as a governance process. However, architecture review boards can be extremely effective when part of a comprehensive governance program that includes active CIO support, a communication program that promotes grassroots awareness of the value of architecture and architecture consulting.
- Funding for this governance process is usually in the form of a "corporate tax" for the central architects´ time and the willingness of infrastructure and development groups to fund an architect position to participate in architecture-related activity.

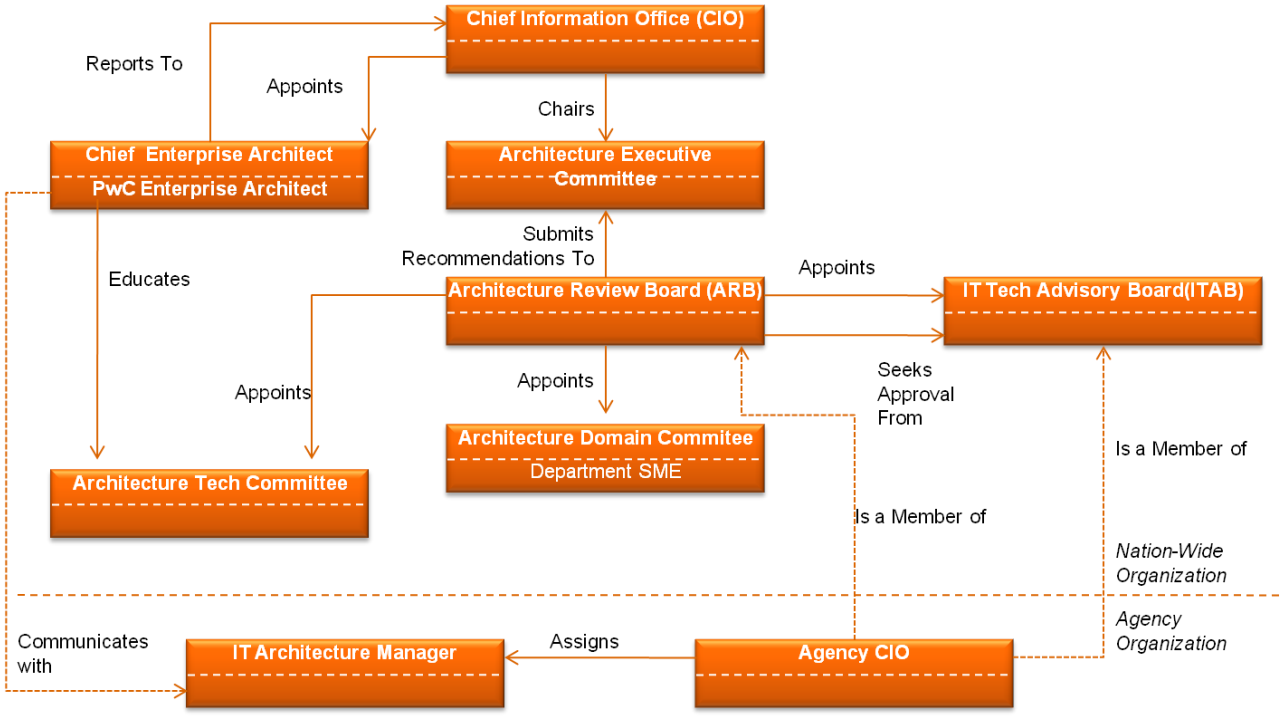
Pros	Cons
Designs get reviewed by highly qualified IT practitioners.	The architecture review occurs late in project design, giving rise to rework or refusal to modify the design.
Awareness of the importance of architecture is heightened in the IT community.	Failures to enforce compliance due to business pressure to stay on schedule undermine the architecture effort and demoralize participants.
The IT organization realizes an increased conformance to standards.	An overburdened board can create a bureaucratic bottleneck in the implementation process, doing harm to the architecture effort.
The IT organization obtains a heightened awareness of valid business reasons for noncompliance and the need to expand the architecture standards.	

10.4 Enterprise Architecture Governance Lifecycle

10.4.1 Enterprise Architecture Governance Structure

The indicative proposed GEA governance model is depicted below –

GEA Architecture Review Board Structure

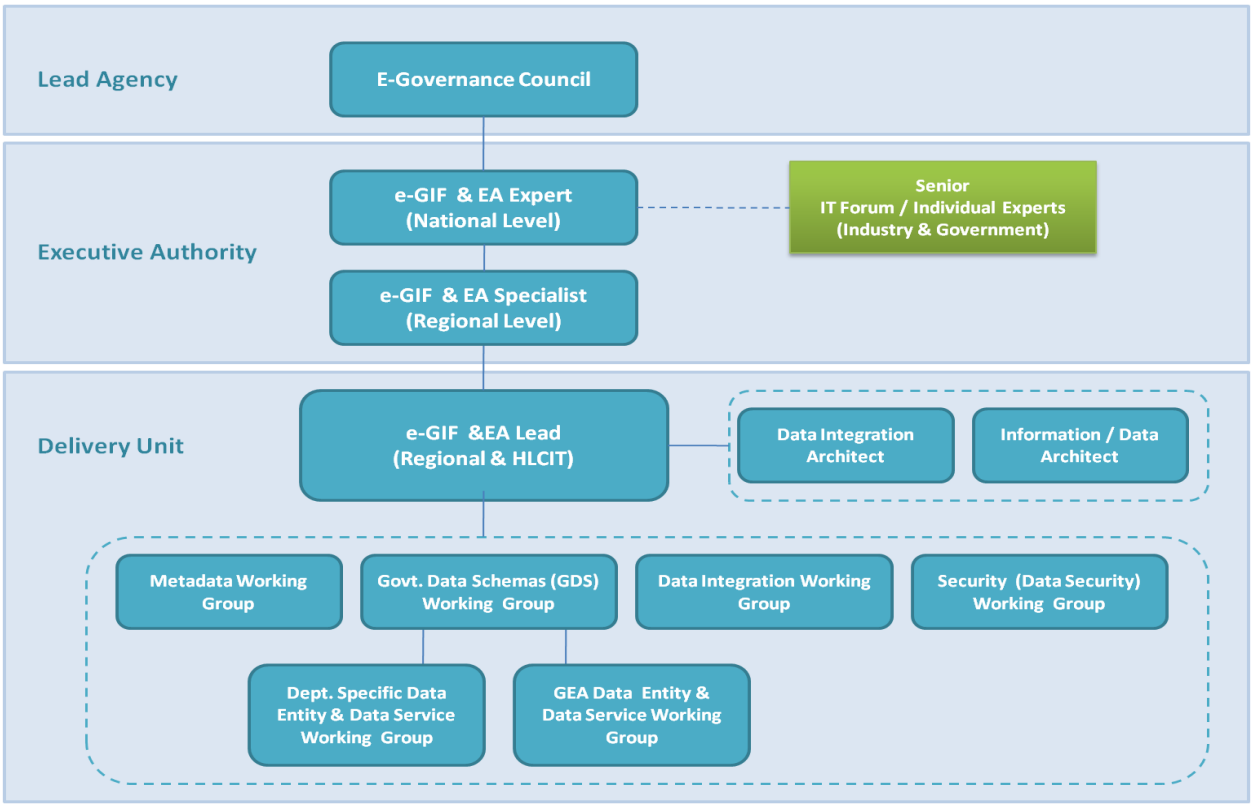


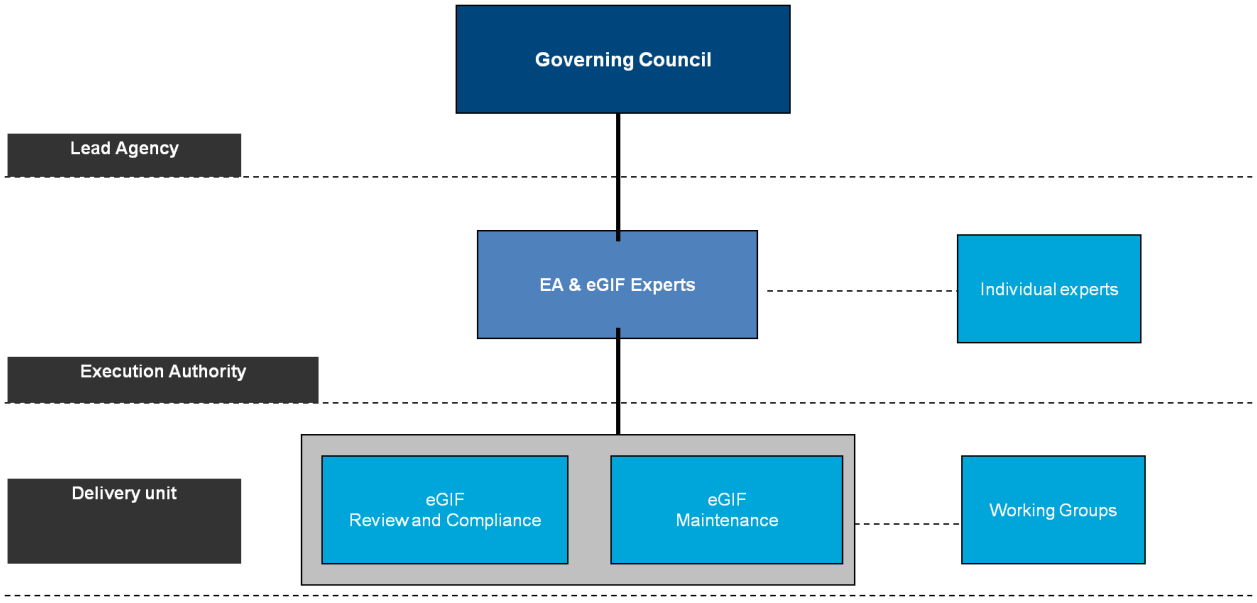
The governance structure proposed above is an indicative one. This structure will be revised and finalized after discussion with HLCIT, PMO & other concerning bodies and will be provided as an addendum to this report

Functions	Descriptions	Gov Mapping	GEA Mapping
Chief Information Officer (CIO)	Champions the architecture effort, promotes architecture value, ensures architecture success, assigns appropriate resources, and manages architecture principles. Has IT project approval for large budget projects and supports the budget and appropriation Process on behalf of other agencies.		
Architecture Executive Committee (AEC)	Approves architecture variations, reviews project plans, risk strategy for consistency with architecture.		
Chief Architect	Implements management processes; educates facilitators and users; manages targets and performance measures, manages implementation plan; manages architecture contents; administers Compliance reviews; develops domain templates; and administers ARC.		
Architecture Review Committee (ARC)	Submits architecture recommendations to AEC, reviews Architectural changes, reviews requests for variance, establish architecture management processes; appoints Facilitators and Architecture domain committees & chairs.		
Architecture Domain Committees (ADC)	Recommend architecture standards, provides domain guidance to agencies, and provide technical assistance on architecture domain issues.		
Architecture Technical Committee (ATC)	Educate domain committees, facilitate domain sessions, assure adherence to methodology, ensure consistent enterprise view, gain consensus of ADC members, serve as methodology experts, and handle special projects.		
Information Technology Advisory Board (ITAB)	This board consists of the department level CIOs and/or IT Directors. Implements strategic plan and develops IT strategies. Critical to endorsing CIO initiatives. Functions as the key contact with project stakeholders. Staff many of the committees for policy and standards.		

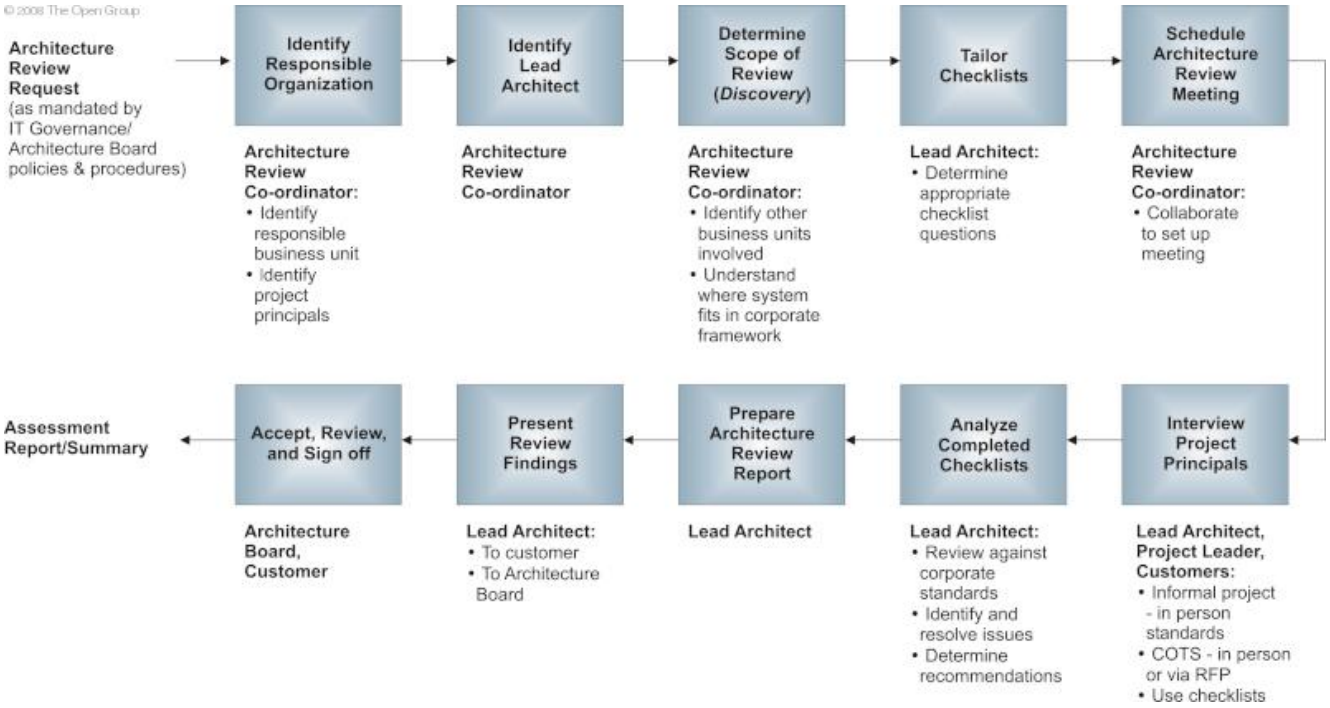
Functions	Descriptions	Gov Mapping	GEA Mapping
IT Architecture Manager	Establishes & manages departmental compliance process; communicates to and educates developers, users, & mgrs; Establishes architecture targets and measurements; manages departmental architecture database; manages architecture implementation plan; assures adherence to methodology; and acts as a potential members of ATC.		
Architecture Review Committee (ARC)	Submits architecture recommendations to AEC, reviews Architectural changes, reviews requests for variance, establish architecture management processes; appoints Facilitators and Architecture domain committees & chairs.		
Agency CIO	Owns department-level architecture.		

10.4.2 NeGIF Governance





10.4.3 The Architecture compliance review process

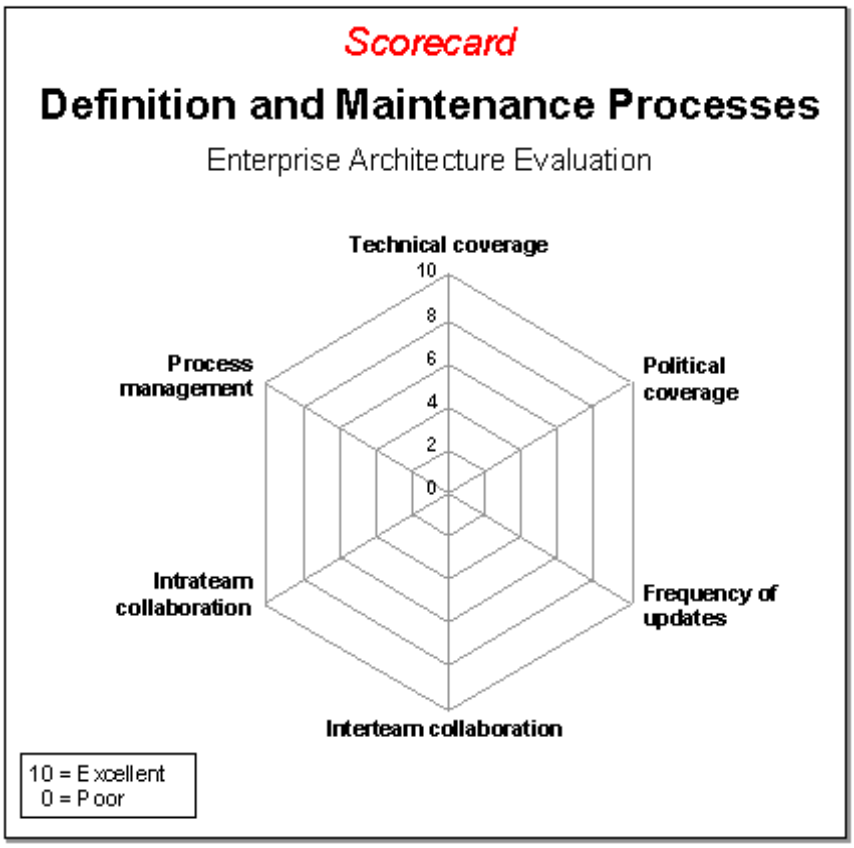


10.4.4 Compliance and evaluation of GEA

Evaluation: Definition and Maintenance Processes

- *Technical coverage*
- *Political coverage*

- *Frequency of updates*
- *Interteam collaboration*
- *Intrateam collaboration*
- *Process management*



Source: Giga Information Group

Figure 1

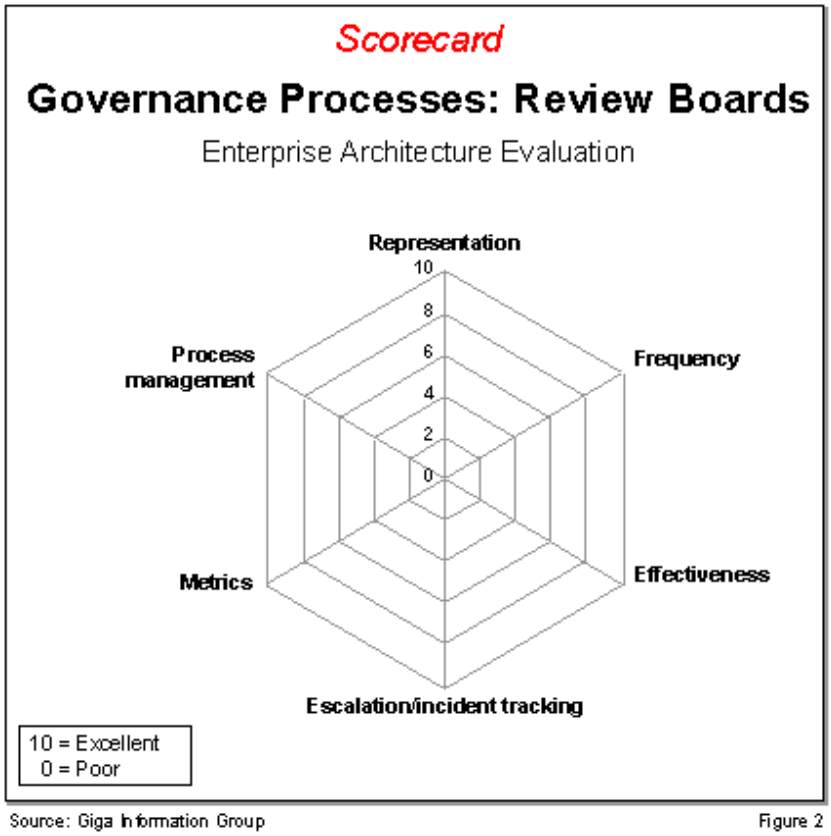
10.4.4.1 Assessment Maturity

Governance Processes: Review Boards

Use of architecture review boards is a common approach to architecture governance. They can be effective in providing a broad and highly skilled audience for design reviews and as a means of communicating architecture information about high-impact projects. Flawed implementations, however, can frustrate architects and architecture stakeholders as well a variety of factors influence the review board´s potential for effectiveness, including board makeup, the frequency of reviews and the implementation of incident-tracking mechanisms.

- *Representation*
- *Frequency*
- *Effectiveness*
- *Escalation/incident tracking*
- *Metrics*

- *Process management*

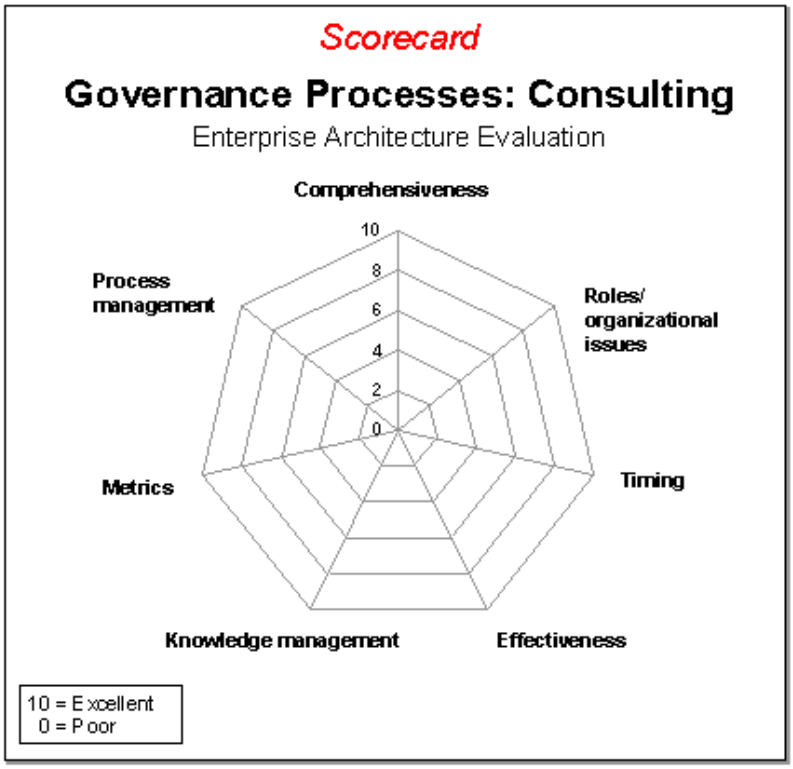


Source: Giga Information Group Figure 2

Governance Processes: Consulting

Although internal architecture consulting is typically seen as a means for sharing technical expertise, it can also be a very powerful mechanism for architecture governance and agile consulting regimen can avoid the chief difficulties inherent in an architecture review board as a governance mechanism, namely timeliness and the imposition of bureaucracy and the perception of architecture as a policing action. However, it is difficult to provide consulting well; excellent technical and soft skills are necessary, making appropriate individuals scarce, and managing consulting resources across a broad landscape

- *Comprehensiveness*
- *Roles/organizational issues*
- *Timing*
- *Effectiveness*
- *Knowledge management*
- *Metrics*
- *Process management*



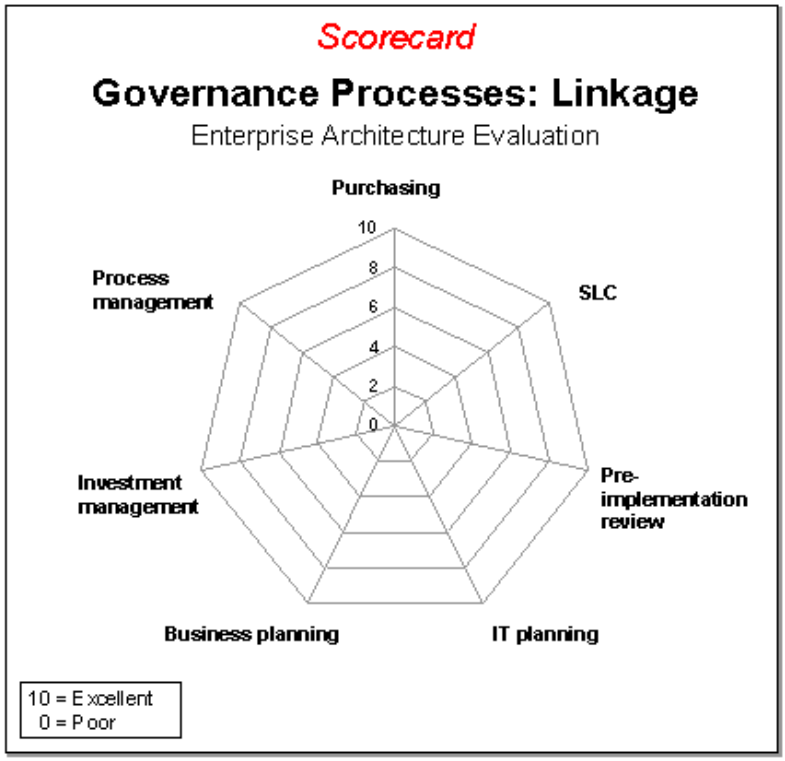
Source: Giga Information Group

Figure 3

Governance Processes: Linkage

Linkage of architecture processes to other key IT and business processes is critical to effective architecture governance. For example, linking architecture standards to the purchasing process can eliminate inadvertent purchases of non-standard technology and discourage conscious efforts to acquire non-standard components. Linkage to system development life-cycle processes can be critical to impacting development activity. And the need for linkage to planning processes should be apparent to anyone who has attempted to keep architecture in synch with business requirements.

- *Purchasing*
- *System life cycle (SLC)*
- *Pre-implementation review*
- *IT planning*
- *Business planning*
- *Investment management*
- *Process management*

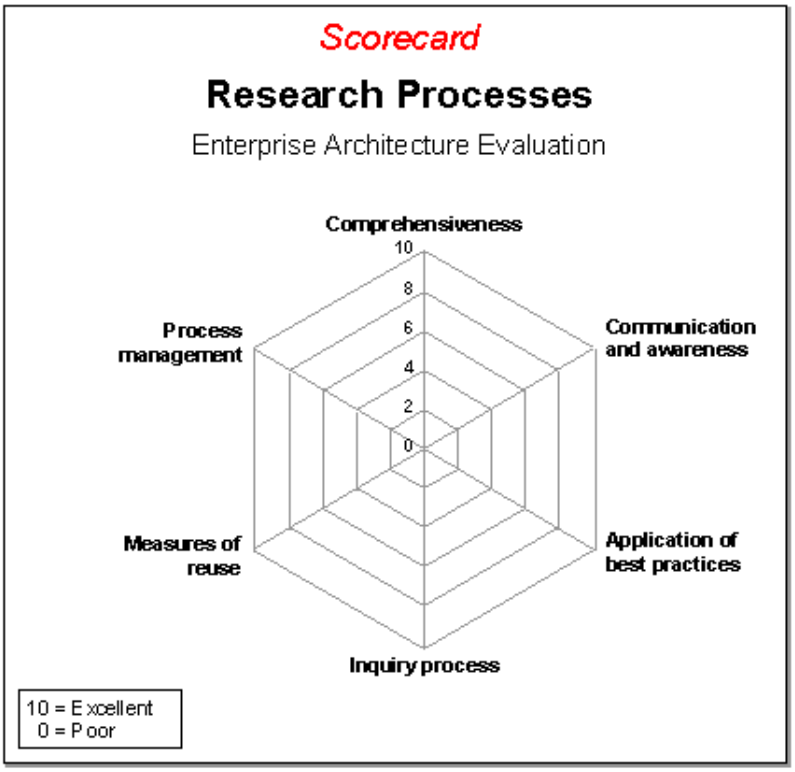


Source: Giga Information Group Figure 4

Governance Processes: Linkage

Every architecture group engages in research processes, whether they consider their processes formal constructs or not. The degree to which these processes are structured to make effective use of the resources expended in the research varies considerably from organization to organization. These criteria evaluate the architecture group´s ability to use its research processes to the general betterment of the enterprise.

- *Comprehensiveness*
- *Communication and awareness*
- *Application of best practices*
- *Inquiry process*
- *Measures of reuse*
- *Process management*



Source: Giga Information Group Figure 5

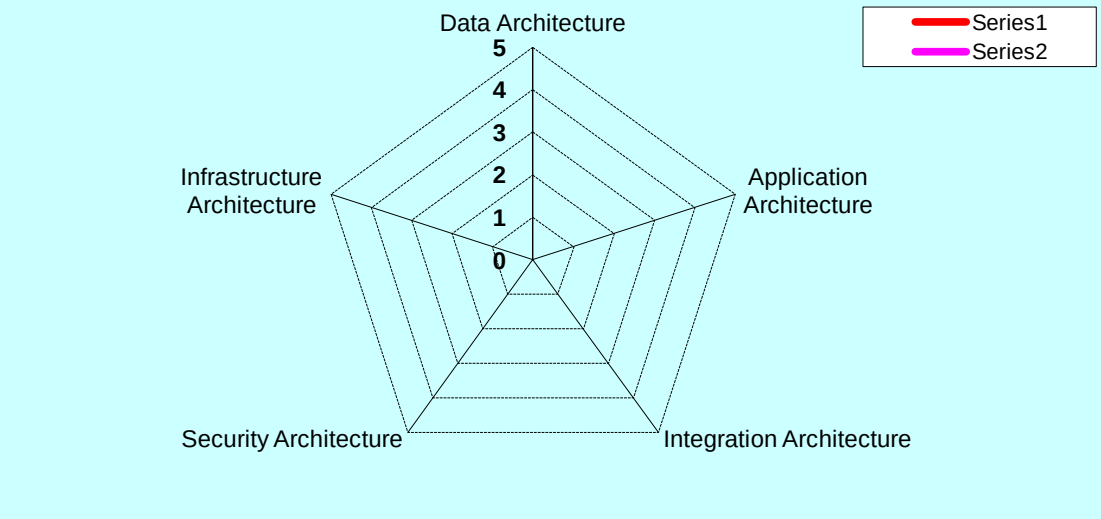
10.4.4.2 Architecture Evaluation Checklist

ID	Section	Relevance to Project	Changed (Y/N)?	Select Response	Additional Details / Comments	Score
1.	**Data Architecture**					
a01a	Is the system responsible for master data management?					
a01b	Is data available to user in a timely manner					
a01c	How is data entered & validated?					
a01d	How is referential Integrity maintained or enforced through the data update / copy process?					
a01e	What is the data architecture model of this system?					
a01f	Is a strategy for data retention, archiving & disposal defined and implemented?					
a01g	Are there single business owners for each key category of data?					
a01h	Has the reuse of existing data assets been taken into					

ID	Section	Relevance to Project	Changed (Y/N)?	Select Response	Additional Details / Comments	Score
	consideration with this design?					
2.	**Application Architecture**					
a02a	What types of access methods (technical channels) are supported by this application?					
a02b	How flexible is the application to interface with third-party systems?					
a02c	How is database access implemented?					
a02d	How is database concurrency and transaction management implemented?					
a02e	How are business rules & logic defined in this application?					
a02f	What application logging is provided?					
a02g	What level of effort would be required to migrate this application to a different platform?					
a02h	How are exceptions / errors managed and communicated to users in this application?					
a02i	How is data validation performed for the online screens?					
a02j	Has accessibility (e.g. AAA) been designed into the application?					
3.	**Integration Architecture**					
a03a	What application programming interfaces (APIs) are supported by this application (Note: some 'lower' scoring APIs may be appropriate in some circumstances, e.g. for performance)?					
a03b	Can standard / existing BI / reporting tools access this system?					
a03c	Does this application ready for SSO?					

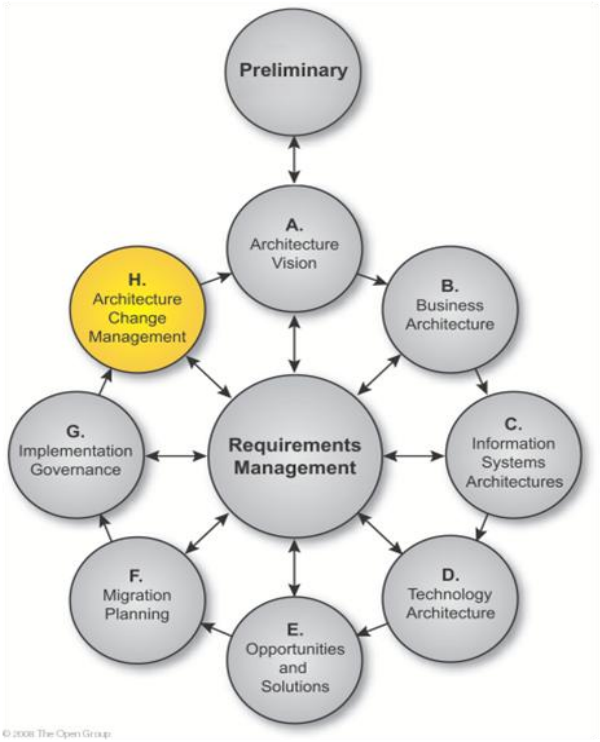
ID	Section	Relevance to Project	Changed (Y/N)?	Select Response	Additional Details / Comments	Score
a03d	Is direct external access to core source system data allowed or possible?					
a03e	Does this application use well-defined XML schema definitions (XSDs)?					
a03f	What protocols are supported by this application?					
a03g	Does this application interface with middleware (e.g. MQSeries, ESB, EAI, TP monitor)?					
a03h	How does this application support enterprise master data?					
a03i	Are interfaces developed once per function / data item or point-to-point on an application by application basis?					
4.	**Security Architecture**					
a04a	Does this application has authentication and authorization model in this application					
a04b	Is Auditing Enabled in the application					
a04c	Has the security classification defined for all data and combination of data					
a04d	Has all non-anomysied data exchange with external organization and individuals using public networks are encrypted securely					
a04e	security and identity management has been implemented separately from the business process					
a04f	Has it pass the independent penetration testing					
5.	**Infrastructure Architecture**					
a05a	Does this application going to be deployed in a secured environment?					
a05b	Does this application tested on a similar environment during pre					

ID	Section	Relevance to Project	Changed (Y/N)?	Select Response	Additional Details / Comments	Score
	production testing?					
a05c	Have all the assumptions on which performance commitments are based been documented?					
a05d	Has the application been adequately sized (storage, performance / throughput, users, etc.)?					
a05e	Is this application performance tested for scalability?					
a05f	Is this application deployable in a distributed environment allowing scalable hardware, load balancing, n-tiers?					
a05g	Have potential performance bottlenecks / problems been identified and addressed?					
a05h	Have cost-effective paths for performance improvements been provided for any problem areas?					
a05i	Does the application currently have performance issues?					
a05j	What is the measured maximum volume (transactions, users) that this application can support?					
a05k	Does this application satisfy stated availability requirements?					
a05l	Does this system incorporate business continuity or disaster recovery capabilities?					
a05m	How is data secured for transport over the network					


Data Architecture
5
4
3
2
1
0
Application Architecture
Integration Architecture
Security Architecture
Infrastructure Architecture
Series1
Series2

11. TOGAF ADM Phase H - Architecture Change Management

11. Phase H : Architecture Change Management



Phase Overview

The goal of an architecture change management process is to ensure that the architecture achieves its original target business value. This includes managing changes to the architecture in a cohesive and architected way to establish and Support the implemented enterprise architecture as a dynamic architecture. This process will typically provide for the continual monitoring of such things as new developments in technology and changes in the business environment, and for determining whether to formally initiate a new architecture evolution cycle

11.1 Request for architecture work

Management of the Architecture Contract between the architecture function and the business users of the enterprise

11.2 Changes to architecture framework and principles

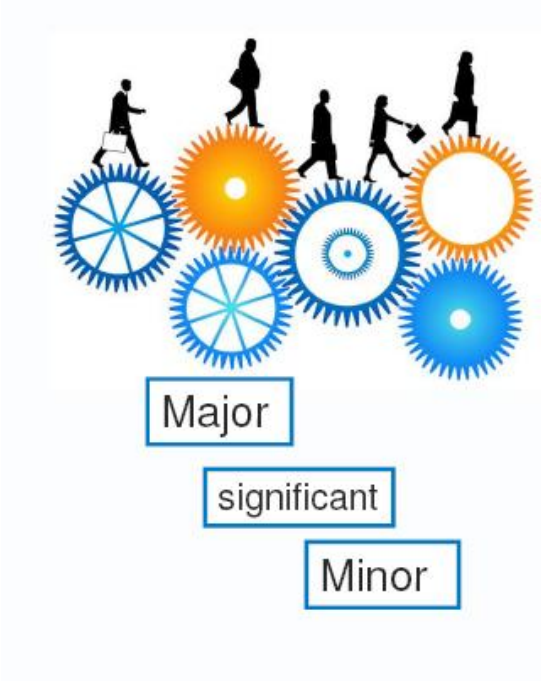
Approach

Determine whether a Change Request warrants

- Starting a new cycle of the Architecture Development Method (ADM)
- Just an architecture update
- It is important to avoid "creeping elegance", and the governance body must continue to look for changes that relate directly to business value
- An Architecture Compliance report should state whether the change is compliant to the current architecture
- If it is non-compliant, an exemption may be granted with valid rationale
- If the change has high impact on the architecture, then a strategy to manage its impact should be defined Drivers for change

There are three ways to change the existing infrastructure that have to be integrated:

- Strategic, top-down directed change to enhance or create new capability (capital) [Re-architecting Change]
- Bottom-up changes to correct or enhance capability (operations and maintenance) forinfrastructure under operations management [Incremental Change]
- Experiences with the previously delivered project increments in the care of operations management, but still being delivered by ongoing projects [Simplification Change]



11.3 Architecture Change management process

To determine whether a change is simplification, incremental, or re-architecting, the following activities are undertaken:

- Registration of all events that may impact the architecture
- Resource allocation and management for architecture tasks
- The process or role responsible for architecture resources has to make assessment of what should be done
- Evaluation of impacts

Drivers for Change

Business drivers for architecture change, including:

- Business-as-usual developments
- Business exceptions
- Business innovations
- Business technology innovations
- Strategic change

Often results in a complete (or partial) re-development of the architecture

Technology-related drivers for architecture change requests includes for example:

- New technology reports
- Asset management cost reductions
- Technology withdrawal
- Standards initiatives
- Normally manageable through an enterprise's change management and architecture governance processes

Maintenance or Change Management

To determine the extent of change a good rule-of-thumb is:

- If the change impacts two stakeholders or more, then it is likely to require an architecture redesign and re-entry to the ADM
- If the change impacts only one stakeholder, then it is more likely to be a candidate for change management
- If the change can be allowed under a dispensation, then it is more likely to be a candidate for change management
- If the impact is significant for the business strategy
  - There may be a need to redo the whole enterprise architecture
  - If a new technology or standards emerge,
  - There may be a need to refresh the Technology Architecture, but not the whole Enterprise Architecture - thus an incremental change
- If the change is at an infrastructure level
  - For example, ten systems reduced or changed to one system - this may not change the architecture above the physical layer, but it will change the baseline description of the Technology Architecture
  - This would be a simplification change handled via change management techniques

Architecture Board and Change Requests

The Architecture Board assesses and approves Requests for Change (RFC)

- A challenge for the Architecture Board when handling an RFC is to determine whether it should be approved or whether a project in a Transition Architecture will resolve the issue
- When assessing project or solution fit into the Change Management architecture, there may also be the case when an innovative solution or RFC drives a change in the architecture

11.4 Change Implementation process

Establish Value Realization Process	Deploy Monitoring Tools	Manage Risks	Provide Analysis for Architecture Change Management	Develop CR to Meet Performance Targets	Manage Governance Process	Activate the Process to Implement Change
Influence business projects to exploit the enterprise architecture for value realization (outcomes)	Monitor technology changes which could impact the Baseline Architecture	Manage enterprise architecture risks and provide recomm--endations for IT strategy	Conduct enterprise architecture performance reviews with service management	Make recomm-endations on change requirements to meet performance targets and development of position to act	Arrange meeting of Architecture Board (or other Governing Council)	Produce a new Request for Architecture Work and request for investment
	Monitor business changes which could impact the Baseline Architecture		Assess Change Requests and reporting to ensure that the expected value realization and Service Level Agreement (SLA) expectations of the customers are met		Hold meeting of the Architecture Board with the aim of the meeting to decide on handling changes (technology and business dispensations)	Ensure any changes implemented in this phase are captured and documented in the Architecture Repository
	Monitor enterprise architecture capability maturity		Undertake a gap analysis of the performance of the enterprise architecture			
	Track and assess asset management programs		Ensure change management requests adhere to the enterprise architecture governance and framework			
	Track the QoS performances and usage					

	Determine and track business continuity requirements					

11.5 Deploy Monitoring tools

Monitoring tools are commercially available COTS products that helps maintain the repository of all documents related to ADM based on TOGAF. This enables the traceability of any principle from the preliminary stages till its implementation.

12. Annexure

12. Annexure

12.1 Typical example of ePayment Gateway solution

An e-payment gateway solution would typically offer the following basic functionality:

1. Payment Gateway through Internet – Govt. of Nepal will be able to receive various payments from the e-Governance website. The modes of payments could be Credit Card, Debit Card, net-banking etc depending on the services offered by the e-Payment gateway solution provider
2. Direct Pay – This is a facility that will provide Govt. of Nepal with the option of accepting on-line payments from its citizens who are also account holders in government approved banks and any other bank's account holders having Net banking password to make online payments.
3. Debit Electronic Clearing System (ECS) – The ECS facility would help citizens across Nepal having an account with any bank/branch which is member of ECS clearing. The ePayment gateway service provider (bank) will act as the sponsor bank to implement Debit ECS for receiving payments from the citizens on behalf of Govt.

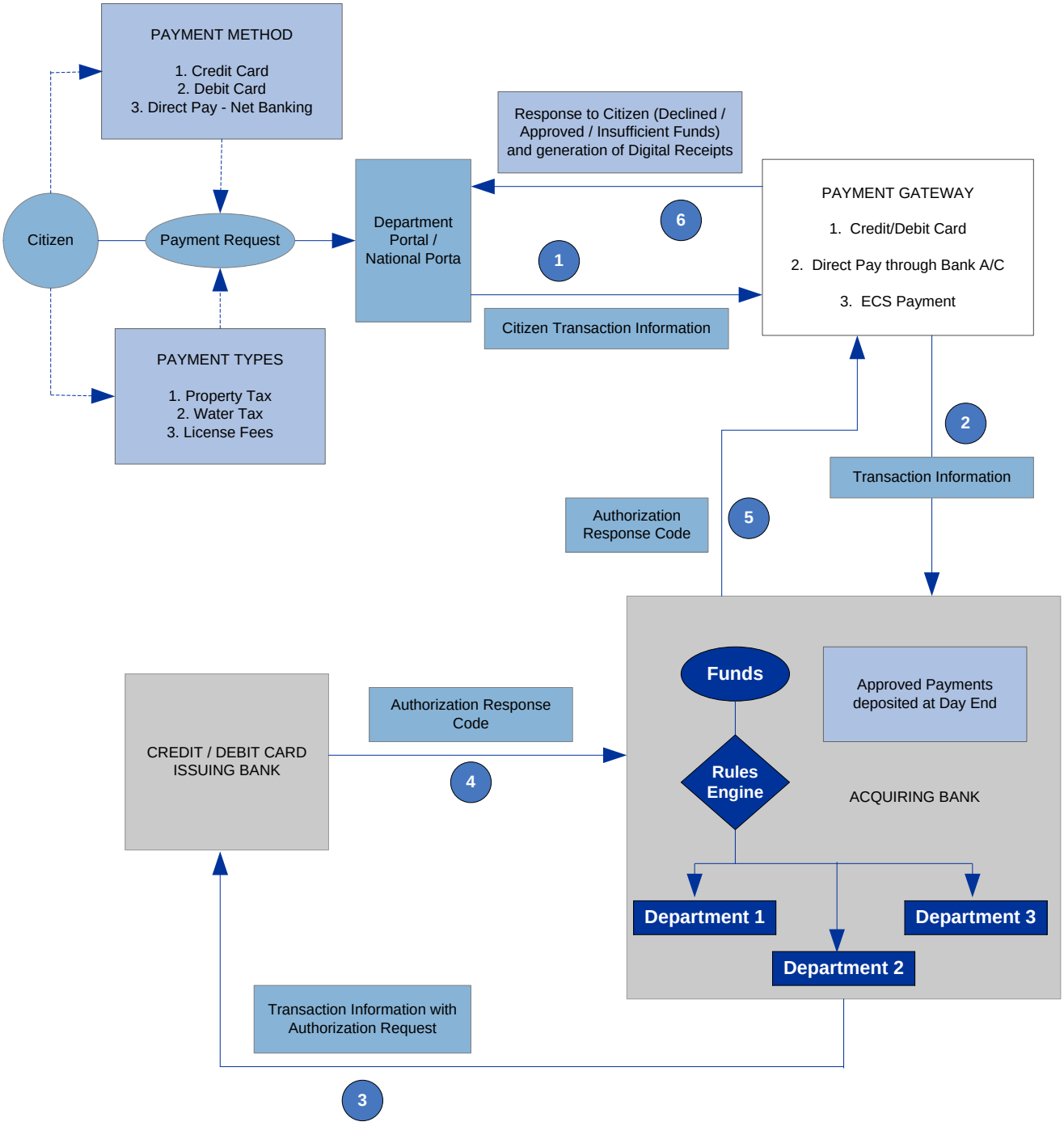
An ideal payment gateway solution should be implemented based on the following criteria:

- Authenticate parties involved in the transaction
- Route messages securely between the parties for authorization and settlement of the transaction
- Ensure integrity and privacy of all messages
- Provide administration support to the parties involved

A typical operational flow for collection of payment through the internet portal is shown below –

1. The citizen visits a government department portal or the national portal. He submits eService request andchooses the option for online payment if a payment transaction is required.
2. Merchant's web server receives the message and sends a digital order to the payment gateway over a secure link. The digital order contains the merchant's id, signature, amount and the return URL address. The payment gateway verifies the merchant.
3. It then presents the citizen with the payment options screen over a secure link.
4. The citizen gives his payment information. The information is passed on to the payment gateway over a secure link.
5. The payment gateway then transmits this information to the acquiring bank. The acquiring bank verifies the merchant's limits and then transmits the message to the issuing bank for payment authorization. The issuing bank authorizes the payment and transmits the confirmation back to the payment gateway through the acquiring bank.
6. The payment gateway sends digital receipts to department and the citizen.

The entire process takes few seconds. The payment gateway ensures that the citizen's payment information is not exposed to the merchant. It also ensures that the citizen's information is not compromised at any point. It also enables the acquiring bank to verify the merchant.


PAYMENT METHOD
1. Credit Card
2. Debit Card
3. Direct Pay - Net Banking
Response to Citizen (Declined / Approved / Insufficient Funds) and generation of Digital Receipts
PAYMENT GATEWAY
1. Credit/Debit Card
2. Direct Pay through Bank A/C
3. ECS Payment
Citizen
Payment Request
Department Portal / National Porta
6
1
Citizen Transaction Information
PAYMENT TYPES
1. Property Tax
2. Water Tax
3. License Fees
2
Transaction Information
Authorization Response Code
5
Funds
Approved Payments deposited at Day End
CREDIT / DEBIT CARD ISSUING BANK
Authorization Response Code
4
Rules Engine
ACQUIRING BANK
Department 1
Department 3
Department 2
Transaction Information with Authorization Request
3

pwc.com/india