IndEA

… for ONE Government

NeST-FMK-GEN.03
Version 1.0
October,2018
Status: Released

IndEA Framework

(India Enterprise Architecture Framework)

Ministry of Electronics and Information Technology
Government of India

Change History

Sr. No.	Author	Version No.	Release Date	Change Details

Metadata of the Standard

S. No.	Data elements	Values
1.	**Title**	India Enterprise Architecture Framework
2.	**Title Alternative**	IndEA
3.	**Document Identifier**	NeST-FMK-GEN.03
4.	**Document Version, month, year of release**	Version 1.0 October, 2018
5.	**Present Status** *(Draft/Released/Withdrawn)*	Released
6.	**Publisher**	Ministry of Electronics and Information Technology (MeitY), Government of India (GoI)
7.	**Date of Publishing**	October,2018
8.	**Type of Standard Document** *(Standard/ Policy/ Technical/ Specification/ Best Practice /Guideline / Framework /Procedure)*	Framework
9.	**Enforcement Category** *(Mandatory / Recommended)*	Recommended
10.	**Creator** *(An entity primarily responsible for making the resource)*	NeST (STQC)
11.	**Contributor** *(An entity responsible for making contributions to the resource)*	**1.** MeitY **2.** NIC **3.** C-DAC **4.** STQC
12.	**Brief Description**	
13.	**Target Audience** *(Who would be referring / using the Standard)*	
14.	**Owner of approved Standard**	MeitY
15.	**Subject** (Major Area of Standardization)	Enterprise Architecture
16.	**Subject. Category** (Sub Area within major area)	Institutional Mechanism
17.	**Coverage. Spatial**	INDIA
18.	**Format** *(PDF/A at the time of release of final Standard)*	PDF
19.	**Language** *(To be translated in other Indian languages later)*	English
20.	**Copyrights**	MeitY
21.	**Source** *(Reference to the resource from which present resource is derived)*	
22.	**Relation** *(Relation with other e-Governance standards notified by MeitY)*	None

Table of Contents

Foreword ..... **xi**

IndEA Overview ..... **xiv**

About the Document ..... **xx**

Background xx

Purpose xx

Scope xx

Intended Audience xx

Related Documents xxii

Acknowledgments xxii

1. The IndEA Context & Vision **1**

1.1. The Context 1

1.2. IndEA defined 1

1.3. Vision & Value Proposition of IndEA 2

2. IndEA Structure & Principles **4**

2.1. Structure of IndEA 4

2.2. Principles of IndEA 5

3. Performance Reference Model **9**

3.1. PRM Objectives 10

3.2. PRM Concepts and Definitions 10

3.3. PRM Principles 11

3.4. PRM Schematic 11

3.5. PRM and Business Reference Model 14

3.6. Enterprise Architecture Measurement 15

4. Business Reference Model **18**

4.1. Objectives 18

4.2. BRM Concepts & Definitions 18

4.3. BRM Principles 19

4.4. The Business of Government and the BRM Landscape 20

4.5. The Value Lifecycle of BRM 20

4.6. BRM Schematic 21

4.7. BRM and Other Reference Models of IndEA 25

4.8. Business Landscape of IndEA 26

4.9. Business Process Re-Engineering 29

4.10. Approach to ONE Government 29

5. Data Reference Model 31
5.1. DRM Objectives 31
5.2. DRM Concepts & Definitions 32
5.3. DRM Principles 33
5.4. DRM Schematic 34
5.5. Metadata and Data Standards 41
5.6. Data Governance 43
5.7. Empowering Government with Analytics 46
5.8. DRM and Other Reference Models of IndEA 48
5.9. Developing Enterprise Data Architecture from DRM 49
6. Application Reference Model 50
6.1. ARM Objectives 51
6.2. ARM Concepts & Definitions 51
6.3. ARM Principles 52
6.4. ARM Schematic 52
6.5. Application Architecture Meta-Model 64
6.6. Application Architecture Standards 66
6.7. Rationalization of the existing Application Portfolio 70
6.8. ARM and Other Reference Models of IndEA 71
6.9. Preparing for AI in Government with Enterprise Architecture 73
6.10. Developing Enterprise Application Architecture from ARM 74
7. Technology Reference Model 75
7.1. TRM Objectives 75
7.2. Definitions 75
7.3. TRM Principles 76
7.4. TRM Schematic 77
7.5. Technology Architecture Trends 79
7.6. Technology Architecture Standards 81
7.7. TRM and Other Reference Models 85
7.8. Developing Enterprise Technology Architecture from TRM 87
8. Integration Reference Model 88
8.1. IRM Objectives 88
8.2. IRM Concepts and Definitions 88
8.3. IRM Principles 89
8.4. IRM Schematic 90

8.5. Enterprise Integration & Application Integration 93
8.6. Integration of Legacy Applications 97
8.7. IRM and Other Reference Models of IndEA 97
9. Security Reference Model 98
9.1. SRM Objectives 98
9.2. SRM Concepts and Definitions 99
9.3. SRM Principles 100
9.4. SRM Schematic 100
9.5. Security Standards 120
9.6. SRM and Other Reference Models of IndEA 121
9.7. Developing Enterprise Security Architecture from SRM 122
10. IndEA Governance Reference Model (GRM) 123
10.1. Objectives of IGRM 123
10.2. GRM Concepts and Definitions 124
10.3. IGRM Principles 125
10.4. IGRM Schematic 125
10.5. Roles & responsibilities of key actors in Architecture Governance 127
10.6. Importance of Communications in Architecture Governance 127
10.7. Strategic Control in IT Governance 128
11. IndEA Implementation Approach 130
11.1. From Framework to Architecture to Implementation 130
11.2. EA Capability Assessment 130
11.3. Customizing the IndEA Framework to the Enterprise 131
11.4. Converting IndEA Reference Models to corresponding architectures 132
11.5. Implementing IndEA 133
11.6. EA Program Risk Management 135
Annexures 140
I. Key Performance Indicators for Primary Sector **140**
II. Example of Services Provided by the Government **143**
III. Technology Standards for Application Layers **145**
IV. Technology Standards for Infrastructure Components **150**
V. TRM Service Standard – Cloud Computing Stack **160**
VI. Commonly used Application Integration Patterns **163**
VII. Controls at Security Layers **165**
VIII. Security Policy Document **169**

IX. Framework for Strategic Control **178**
X. Reference Models in UML Notations **180**
XI. List of Acronyms..... **185**

List of Figures

Figure 1.1: Vision of IndEA 3
Figure 2.1: Reference Models of IndEA 5
Figure 3.1: Metamodel of Enterprise Performance Management 9
Figure 3.2: Performance Reference Model (PRM) - Conceptual View 12
Figure 3.3: Relationship between PRM & BRM 15
Figure 3.4: EA Business Value Chain 16
Figure 4.1: Framework for Defining & Realizing Value 20
Figure 4.2: The IndEA Business Reference Model (BRM) – Conceptual Model 21
Figure 4.3: Service Prioritization 23
Figure 4.4: Template for Service Definition 25
Figure 4.5: BRM and Other Reference Models 25
Figure 4.6: BRM and ARM 26
Figure 4.7: Business Landscape of IndEA 27
Figure 4.8: Sub-Sectors and Functions of Primary Sector 28
Figure 4.9: Modules of the Financial Management Horizontal 29
Figure 5.1: DRM Areas and their Interlinkages 35
Figure 5.2: DRM Abstract Model 36
Figure 5.3: Abstract model of Data Description 38
Figure 5.4: Abstract Model of Data Context 40
Figure 5.5: Abstract Model of Data Sharing 41
Figure 5.6: DRM and Other Reference Models 48
Figure 5.7: Relationship Between DRM and SRM 49
Figure 6.1: Application Reference Model 53
Figure 6.2: Template for Application Description 53
Figure 6.3: IndEA Application Portfolio 55
Figure 6.4: Components Of Interoperability Layer 56
Figure 6.5: Sample Application Portfolio Catalogue 56
Figure 6.6: Application Mapping 57
Figure 6.7: Logical Layers of Enterprise Application Architecture (SOA & MSA) 65
Figure 6.8: ARM and Other RMs 71
Figure 6.9: Relationship between DRM and ARM 72
Figure 6.10: Relationship between ARM and IRM 73
Figure 7.1: TRM Conceptual Map 78
Figure 7.2: TRM Functional Representation - for Cloud, Open-API and MicroServices 80
Figure 7.3: TRM Application Layers 82
Figure 7.4: TRM Solution Building Blocks 82
Figure 7.5: TRM and Other Reference Models 86
Figure 7.6: Relationship between TRM and ARM 87
Figure 8.1: Integration Design Principles 90
Figure 8.2: Staged Approach To Integration Maturity 91
Figure 8.3: Integration Reference Model (IRM) – Conceptual View 92
Figure 8.4: Integration Reference Model (IRM) – Logical View 93
Figure 8.5: Reference Architecture for Enterprise Application Integration 96
Figure 8.6: IRM and Other Reference Models 97
Figure 9.1: Security Reference Model 100

Figure 9.2: Layers of Security Architecture 102
Figure 9.3: SRM and Other Reference Models 121
Figure 9.4: Relationship between SRM and TRM 122
Figure 10.1: Architecture Governance Reference Model 126

List of Tables

Table 2.1: Principles of IndEA 8
Table 5.1: Publications on Data Standards and Data Policies 42
Table 5.2: Indicative List of Master Data Entities 45
Table 6.1: Application Number Encoding 57
Table 6.2: Indicative List of Core Applications 59
Table 6.3: Indicative List of Common Applications 61
Table 6.4: Indicative List of Group Applications 64
Table 6.5: Indicative List of Department Applications 64
Table 6.6: Non-Functional Requirements of Applications 70
Table 6.7: AI Adoption 74
Table 7.1: Technology Options For Multiple Service Delivery Scenarios 85
Table 8.1: ESB v/s API Gateway Integration Factors 95
Table 9.1: Top risk factors and preventative measures 103
Table 9.2: Vulnerability/ Threat Pair 105
Table 9.3: Template to safeguard implementation plan 106
Table 9.4: Controls to be defined at Business Layer 110
Table 9.5: Controls at the Perimeter Layer 111
Table 9.6: Controls Related to Cyber Intrusion 112
Table 9.7: Control related to Audit 113
Table 9.8: Control related to Disaster Recovery 113
Table 9.9: Controls for Endpoint Layer 116
Table 9.10: Controls at Application Layer 117
Table 9.11: Security Controls related to Logging and Monitoring 118
Table 9.12: Controls Related to Data Backup 120
Table 10.1: List of Communication Tools 128
Table 11.1: Indicative List of Artefacts 133
Table 11.2: Risk Matrix for EA Initiative (showing High Risks only) 139

Foreword

The United Nations e-Government Survey 2016 emphasizes three things - a Whole-of-Government approach, Policy Integration and use of Big Data Analytics - as the important means of achieving the Sustainable Development Goals (SDGs). The purpose of adopting the Whole-of-Government Approach is to provide integrated and joined up services that cut across not only the economic, social and environmental dimensions but also various sectors, sub-sectors and activities. Policy integration entails recognition of the inter-linkages between different areas of policy and adopting a holistic approach. Big Data Analytics is a tool for gaining deep insights into a range of complex issues and using the same for policy formulation and decision-support. All these three globally significant trends invariably require breaking of sectoral barriers and silos and **re-architecting the Government as a single enterprise**.

While India has made reasonable progress in improving its e-Government Development Index (EGDI) from 0.3730 in 2003 to 0.4637 in 2016, it is a matter of concern that we have been consistently below the global average. The latest EGDI of India is 0.4637, which is far below the global best of 0.9193.

India has noteworthy history of e-Government development. The National e-Governance Program, launched in 2006 gave a good push to the e-Governance initiatives in the country, through a portfolio of 33 projects. Infrastructure in the form of SWANs and State Data Centres came up and a number of impactful projects like the MCA21 and Passport Seva got launched. There have been quite a few success stories and pockets of critical mass in the central ministries and the states. The Digital India movement created a large vision in 2014. Fortunately for us, we already have the key building blocks in place, which include – Aadhaar, Mobile and Bharatnet to mention a few. **NIC** has designed enterprise architectures for the Ministries of Panchayati Raj and RWS & Sanitation. Andhra Pradesh has designed a State Enterprise Architecture called **e-Pragati**.

If India is to make big strides in e-Governance and climb up steeply on the EGDI, we need to rise above designing individual projects. We need to **architect** the big vision of Digital India. The key tenets suggested by the UN in its Survey report quoted above have to be considered seriously and adopted. Hence the case for the design and adoption of an **Enterprise Architecture Framework**, tailor-made for the Indian conditions, which can fulfil the aspirations of this large and diverse country. Such an Enterprise Architecture should be able to address the needs of both large national initiatives as well as the varied needs of the States.

Enterprise architecture has been found to be an effective tool for delivering high-quality government services in complex and heterogeneous environments. The importance of an integrated approach to policy formulation and governance reform has been acknowledged by agencies like the UN, World Bank, OECD, WHO and ADB among others. Oftentimes, government is seen as a nebulous construct, with which citizens have difficulty in interacting. Governments spend more time on operational fire-fighting on immediate issues, than on taking a planned and structured approach to good governance. In reality, a planned and structured approach that enterprise architecture advocates, also prepares governments for emergency scenarios, and improves the overall responsiveness. Architecture-based structured planning and guided execution is, therefore, an imperative both, during normal and emergency times.

There is a school of thought which believes that enterprise architecture is command-and-control driven by its very nature. Such belief may be arising out of the fact that any EA initiative calls for significant architectural effort, time and specialized skillsets. It is also buttressed by several emerging technologies that can provide rapid development and service delivery at micro-level, without having to think of a central

architecture. However, contrary to such a belief, enterprise architecture does not mandate or even suggest a centralization of all the IT design, development and operations. Enterprise Architecture recommends a federated architecture, whereby the participant entities design their own solutions adhering to the principles and standards laid down by the Enterprise Architecture, so as to make them interoperable with all other entities within and outside the enterprise. Enterprise Architecture does not amount to a monolithic architecture. It is technology-agnostic and therefore, enables heterogeneous technologies to coexist and interoperate. It facilitates an autonomous evolution of multiple solutions in different domains of the enterprise, all conforming to a set of principles and standards. The centralization, if at all, is confined to the EA Principles and Standards, but does not extend to the technologies, solutions and implementations.

Not adopting an enterprise architecture framework, on the other hand, leads to duplicative and wasteful efforts, and consequently to the loss of efficiency, effectiveness and productivity arising out of a large number of standalone systems that can't inter-operate. The continuous proliferation of new technologies makes it more compulsive now to have an enterprise architecture framework in the middle so as to make the enterprise future-proof in the medium and long-term.

Viewed in the above context, the constitution of a Working Group on National Enterprise Architecture by Ministry of Electronics and IT, Government of India could not have come about at a more appropriate time. The Group has had 7 day-long meetings and attempted a delicate balance between idealism and pragmatism, between national and state requirements, between advanced and not-so-advanced players in e-Governance. The Group has come up with a framework, aptly named as **IndEA** for **India Enterprise Architecture**.

Enterprise Architectures are typically driven by the business vision and expected outcomes. To this end IndEA is founded on a performance focus. The framework is guided by the national priorities, and the SDGs and KPIs arising out of the same. The design considerations of IndEA include **citizen-centric, efficiency-focused and event-driven** architectural patterns and Reference Models. IndEA provides a **generic framework,** comprising of a set of reusable building blocks, which can be converted into a Whole-of-Government Architecture or architectures appropriate to one or more of **16 verticals or sectors and 12 'horizontals'** identified in the framework. Open Standards defined by IndEA promote interoperability and lead to **unity in diversity**. The federated architectural pattern predominantly adopted by IndEA enables flexibility to decentralize, yet consistently permits it to be implemented with ease by a wide variety of government entities, irrespective of their size, functions and current state of IT adoption.

The IndEA Framework comprises of a set of Reference Models, some of which are derived from established frameworks while others have been developed by the IndEA Working Group. These are the Performance Reference Model (PRM), the Business Reference Model (BRM), the Application Reference Model (ARM), the Data Reference Model (DRM), the Technology Reference Model (TRM), the Integration Reference Model (IRM), the Security Reference Model (SRM) and the Governance Reference Model (GRM). The Government enterprises – Ministries, States, Local Bodies and PSUs – can further develop these 8 Reference Models to create their own domain-specific architectures and implementation models.

The design of IndEA Framework recognizes the need to accommodate both greenfield (new) and brownfield (existing/ legacy) initiatives in the area of e-Governance. While greenfield projects shall be mandated to conform to the IndEA framework at the architectural and design stages, brownfield projects need to converge with IndEA through process re-engineering and conformance to the IndEA standards.

The vision of IndEA is to enable **ONE Government** – a Government that is least visible but is most effective, a Government that is **'not fragmented by narrow domestic walls'** but presents a single interface to the constituents, a Government that is citizen-centric, efficient, transparent and responsive. With this in view,

Foreword

IndEA suggests that significant further work be carried out in creating the functional, technological and organizational eco-systems based on the concept of 'Virtualization of Departments' as a possible way of bringing a better synergy across departments.

IndEA is a large **Digital Dream** as yet. Realization of this dream calls for widespread capacity building, allocation of significant resources and above all, a humungous coordination at the national and State levels through executive sponsorship. Quick wins and game changers will generate the momentum for the medium term and keep interest alive to embrace the transformation journey. Partnership with industry will be critical to success.

I acknowledge the keen interest shown by the members of the Working Group and the significant contributions made by them in shaping **IndEA**.

J Satyanarayana
Chairperson
Enterprise Architecture Working Group

IndEA Overview

The Context of IndEA

The e-Governance initiatives in India have acquired a new momentum with the launch of the Digital India program by the Central Government. The thrust given to Aadhaar and the emphasis on its adoption in the various welfare schemes have created the expediency for painting the big picture of e-Governance so as to derive the maximum out of this soft infrastructure. The need for adopting a holistic approach in the domain of e-Governance has become evident from the interoperability issues within and across the multiple clusters of stand-alone applications developed by the States and Central Ministries over the last decade. Against this background, the Working Group constituted by the Central Government came up with a holistic framework, named **IndEA**, for streamlining, standardizing, and optimizing the e-Governance efforts across the country so as to address the much-needed interoperability and integration.

IndEA defined

IndEA, a catchy acronym for the **India Enterprise Architecture**, is a framework for developing a holistic architecture treating the Government as a single enterprise or more realistically, as an **Enterprise of Enterprises**, which are functionally inter-related. IndEA is a structured combination of several Reference Models that, together, enable a **boundary-less flow of information** across the length and breadth of the government and facilitate the delivery of **integrated services** to the stakeholders, namely, the citizens, businesses and employees. Strictly speaking, IndEA is not an Enterprise Architecture as its name seems to connote. It is a comprehensive and convenient *framework* for developing Enterprise Architecture to support ICT enabled transformation across governments. It is an authoritative reference providing an integrated, consistent and cohesive view of strategic goals, business services and enabling technologies across the entire organization. IndEA can be adopted and used successfully, by the Central, State and Local Governments alike, irrespective of their size and current status of technology implementation. It can also be used by PSUs, large departments and agencies of the Government to derive the envisaged benefits.

Simply stated, IndEA is a way to establish **Unity in Diversity** in the domain of e-Governance. It is a framework that enables the development and implementation of Enterprise Architectures independently and in parallel by all governments and their agencies across India, conforming to the same models and standards.

Vision & Value Proposition of IndEA

The Vision of IndEA is "***to establish best-in-class architectural governance, processes and practices with optimal utilization of ICT infrastructure and applications to offer ONE Government experience to the citizens and businesses***".

IndEA brings to the table the entire value proposition of adopting Enterprise Architecture plus more. It derives its approach from the globally known architectural frameworks like the TOGAF, Zachman and the Federal Enterprise Architecture. The models and concepts contained in these global frameworks have been substantially simplified and suitably contextualized to the Indian conditions. The principles of 'Just-in-Time' and 'Just Enough' have been advocated in the design and implementation of Enterprise Architecture.

The major benefits envisaged by the adoption of IndEA framework are:

1. Provide a **ONE Government Experience** to the citizens and businesses, by offering integrated services through multiple channels, in a contactless, frictionless manner.
2. Enhance the **efficiency** of delivery of services, by defining and enforcing service levels of a very high order
3. Improve the **effectiveness** of implementation of the developmental and welfare schemes through a holistic performance management.
4. Enhance the **productivity** of employees and agencies through easy access to information.
5. Provide integrated and cross-cutting services through seamless **interoperability** across the Whole-of Government.
6. Bring in **flexibility** and **agility** in making changes to the systems to align with the best practices and to leverage the latest technologies.
7. Realize **cost-effectiveness** through use of shared infrastructure and services.
8. Enable establishing a Connected Government that works for **inclusive development**.
9. Maintain the right balance between **security** of data and **privacy** of personal information.

Architectural Patterns Adopted by the Working Group

It is significant to mention the following major strategies adopted by the Working Group:

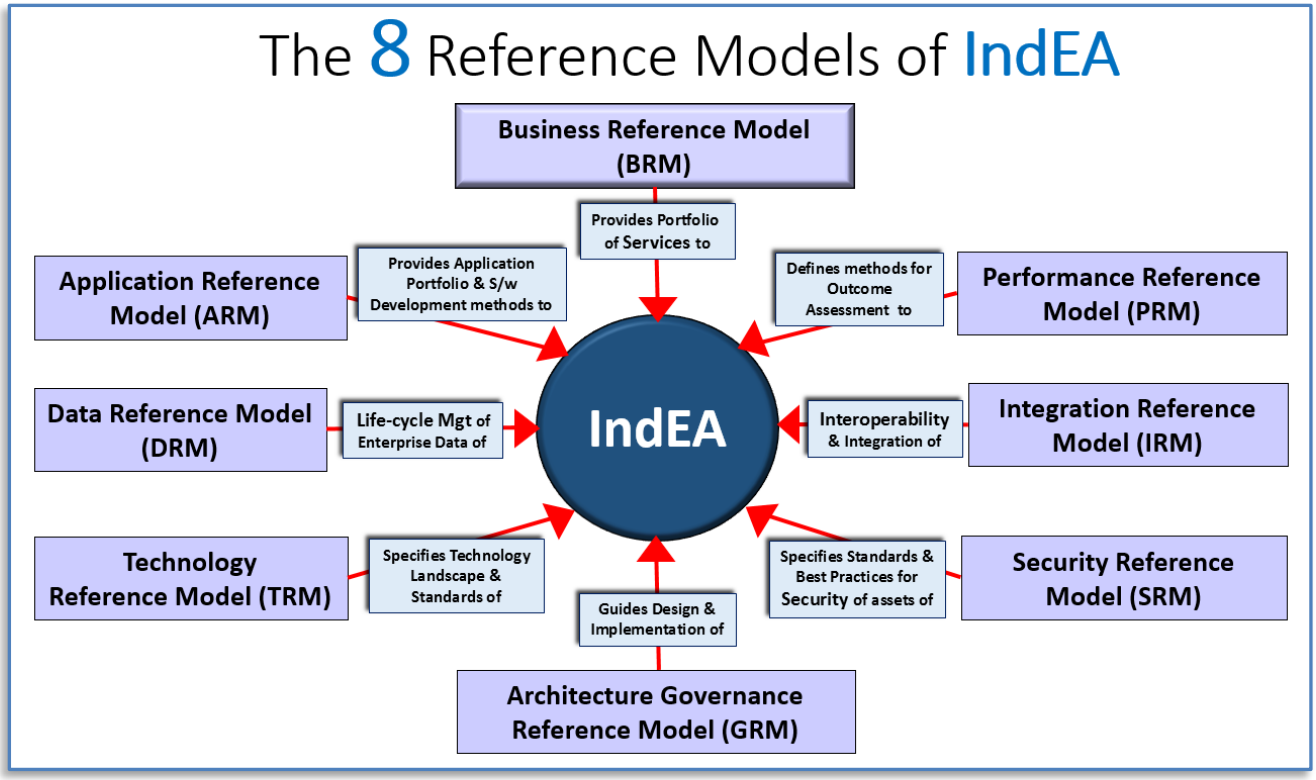
1. IndEA Framework is basically designed keeping the **architectural needs of the State Governments**. However, the Models are developed in a sufficiently generic manner, adopting standard notations, such that the Framework can be adopted by the Ministries of the Central Government and the CPSU's in the upper tier and the Local Governments in the lower tier.
2. Federated Architectural Pattern is chosen for IndEA framework for better administrative feasibility, need for decentralization of implementations, on-boarding of legacy/ ongoing efforts of e-Governance and above all, the need for state governments to have the flexibility to build state specific ICT services. The Core Platform is the backbone to provide ONE Government Experience and interoperability. Any Government or agency delivering ICT services should centrally deploy the Core Platform. In this sense, **IndEA Framework adopts a hybrid architectural pattern** – a combination of centralization of core and common assets and decentralization of domain platforms.

Structure of IndEA

In line with other globally known architectural frameworks, the structure of IndEA consists of a number of Reference Models, each dealing with a specific domain of the Enterprise Architecture. **A Reference Model is an abstract representation of the entities relevant to a domain of the Enterprise Architecture, the inter-relationships among those and the standards to be followed.** The representation is both **graphical** - adopting standard notation like the **UML**, and **descriptive** - specifying the capabilities of each of the components (entities) comprising the Reference Model. Each Reference Model also contains the list of standards that should govern the entities, their relationships and the manner of communications between them. All the Reference Models comprising IndEA are technology-agnostic. These Reference Models are, by definition, devoid of the details specific to their implementation. The Performance, Business, Data, Application and Technology Reference Models using UML notations are depicted in the **Annexure (X)** – Reference Models in UML Notation.

Through a combination of the above-stated 3 basic attributes of all the Reference Models, namely, **abstraction, standards-base and technology-neutrality**, the IndEA framework is sufficiently generic for its widespread adoption by various entities of Government from national to state to local authorities and organizations.

IndEA framework comprises of 8 Reference Models, represented graphically below, viz., **Business, Application, Data, Technology, Performance, Security, Integration and Architecture Governance**.



Principles of IndEA

An Enterprise Architecture is to be founded on a set of **Principles** that inform and guide the Architecture Development process. A good set of Principles should satisfy five criteria, namely, **Understandable, Robust, Complete, Consistent and Stable**.

Citizen-centricity, Outcome-focus, Standardization, **Reusability** and **Integration** are the key *mantras* followed while designing IndEA. While individual sets of principles have been stated and explained in the respective Chapters relating to the 8 Reference Models, the most important of these principles are given below.

1. **SDG Linkage**: Performance Measurement Systems and associated metrics are aligned to Sustainable Development Goals prioritized by the Government.
2. **Integrated Services**: Integrated Services that cut across agency-silos are identified, designed and delivered through multiple delivery channels, to realize the vision of ONE Government.
3. **Sharing & Reusability**: All commonly required Applications are abstracted to be built once and deployed across the Whole-of-Government through reuse and sharing. Sharing & Reusability shall be subject to conformance with the principles of Security & Privacy.
4. **Technology Independence**: Application Design is open standards-based and technology-independent.
5. **Data-sharing**: Data is shared across the Government, subject to rights and privileges, so as to prevent development and use of duplicative sets of data by different agencies. Data Sharing shall be subject to conformance with the principles of Security & Privacy.
6. **Cloud First**: Cloud infrastructure is chosen by default for deployment of applications and on-site option is resorted to only with strong justification.

7. **Mobile First**: Mobile channels are mandatory for delivery of all services, among all delivery channels.
8. **Federated Orchestration**: Integration services, capabilities and orchestration processes are federated.
9. **Primacy of Principles**: The principles specified in this framework govern all reference models and their implementations.

Eight Reference Models of IndEA

An overview of the 8 Reference Models of IndEA is given below:

Performance Reference Model (PRM)

The key objective of PRM is to provide a uniform and consistent mechanism to measure the efficiency and effectiveness of the different sectors or domains in achieving the overall goals of the Government. The principal instrument of the PRM is a set of KPIs designed rationally to measure the outputs and outcomes of the various programs, schemes, projects and activities. A prioritized and phased approach for implementation of PRM is recommended so as to avoid the situation of creating a plethora of KPIs, which hide the actual performance and outcomes.

Business Reference Model (BRM)

The BRM is pivotal for the design of a good Enterprise Architecture, in so far as it looks at **purely** the business vision and the functions/ services required to fulfil that vision **but not** the technologies required to be used. The key entity in BRM is **Service**, be it customer-facing or internal. The watchwords of BRM are – Service Portfolio, Citizen/Business-centricity, Service Prioritization and Integration. A successful implementation of BRM requires a fundamental re-engineering of the Business Processes, elimination of non-value-adds and above all, identification of services that are common across the Government or across groups of departments and abstracting them to a combination of **uniform** processes and workflows.

With a view to give a concrete shape to the BRM, the Group attempted an identification of the **16 vertical domains** and **12 horizontal functions**, which, together, represent most of what a Government does.

An aspirational goal of IndEA is to support the concept of '**ONE Government'** with a single interface offered to the citizens, hiding the boundaries of government agencies. It necessarily involves the breaking of the departmental silos. Since it is not practically feasible to break the silos physically, this laudable objective is sought to be achieved by breaking them virtually, through the new concept of **Virtualization of Departments**.

Application Reference Model (ARM)

The Application Reference Model provides the foundation to automate *Services*, identified as a part of the Business Reference Model. It enables government to achieve its objective through collaboration and data-sharing between & within departments thereby providing effective business services to its stakeholders.

ARM provides a framework for grouping similar applications to maximize re-use. To this end, a **concentric set of layers represent the ARM Meta-model** within IndEA. The inner-most layer **of ARM** is the **Core Platform**, which provides the most generic services in a **domain-agnostic, application-agnostic and technology-agnostic** manner. The three layers around the IndEA Core relate to **Common Applications**, **Group Applications** and **Domain-specific Applications**.

ARM also captures guidelines and recommendations on Application Architecture Standards, use of Open APIs, **Microservices Architecture** and **Open Source Software**. It also specifies the **Secure Coding Standards** for Application Development.

Data Reference Model (DRM)

DRM provides the structure and description of the department's data (metadata), the logical data model (depicting the relationship between various data elements), taxonomy, the security associated with each data element and its sharing. It provides the framework to design the 3 components of Data Architecture, namely, **Data Description, Data Context and Data Sharing**. These 3 areas deal with Discovery, Creation, Management and Exchange of enterprise data. **Database Schema, Data Steward and Exchange Package** are the key concepts/ components in the 3 areas respectively. Defining **Metadata** and **Data Standards** are key activities in the design of Enterprise Data Architecture.

Technology Reference Model (TRM)

TRM depicts the **layout of the technology foundation** of ICT-based systems to be designed for delivery of identified business services. **TRM lists all the components** of the technology system on an end-to-end basis, including IT Infrastructure, Applications, Access Devices, Communication Systems and Service Delivery modes. TRM also **defines the currently applicable open standards** for all the solution building blocks and components and **identifies the Open Source Products** for each technology component.

TRM also deals with the various considerations for designing the solution architecture besides the options for application deployment and service delivery. Important among these are insourcing or outsourcing strategy, **cloud strategy**, and the **mobile strategy**.

Integration Reference Model (IRM)

Integration of Governmental Business processes and services across the breadth of the enterprise is needed for delivering the services conveniently to the citizens on a sustainable basis. Government entities need to organize, secure, prioritize, classify, and publish the information needed by other entities for seamless interoperability. IRM consists of 6-layers of integration, namely, Performance, Process, Service, Application, Data and Infrastructure.

The objective of the IRM is to identify **all the technology options for integration** and provide guidelines and recommendations for integrating business applications, services, information systems and platforms for a **boundary-less information flow**.

Given the accent of IndEA on providing ONE Government experience to the users, the Integration Architecture assumes special importance.

Security Reference Model (SRM)

The SRM delineates the overall framework for providing information security to the entire gamut of IT systems in the enterprise. Integrity, privacy, confidentiality, and availability of information / IT systems are the key concerns addressed by SRM.

SRM adopts a layered approach to identifying and meeting the information security needs of the enterprise. The model identifies the security controls to be applied at **6 layers**, namely, the **Business Layer, Data Layer, Application Layer, Perimeter Layer, Network Layer and the End Point Layer**. SRM also touches upon the manner of designing **Security Policies** and **Standard Operating Procedures**.

Enterprise Architecture Governance Reference Model (GRM)

The objective of GRM is to manage and maintain architecture requirements and artefacts. It comprises of enterprise structure, processes and standards to ensure that the architecture is consistent with the business vision and objectives of the enterprise. Effective and efficient EA Governance ensures that priorities are based on broad consensus across the enterprise. EA is a continuous activity and governance is an integral part for its successful implementation and maintenance.

IndEA framework recommends a **3-tier governance structure**, namely, at the **political, executive and technology** levels.

The framework further recommends the establishing of 2 entities with distinct roles and responsibilities namely, Architecture Governance Board and IT Governance Board. Blurring or overlap of these two roles is likely to create conflicts and delays.

EA Program has to be governed keeping in view the triple constraints, namely, Scope, Time and Cost, which represent the 3 sides of a Project (Program) Management triangle. One side can't be changed without affecting the other. A brief treatment of the implications of Scope, Time and Cost has been given as a part of GRM.

Needless to say, an effective EA Governance system is critical to the success of IndEA.

Implementation Framework

IndEA is a framework for developing full-scale Enterprise Architecture for Governments. The 8 Reference Models comprising it need to be converted into respective sets of Architecture Artefacts so as to derive the maximum benefits out of IndEA. Such a conversion of RMs into Enterprise Architecture Artefacts involves Government-specific and/ or domain specific details to be worked on. **IndEA Adoption Guide** describes the methodology to be adopted for using IndEA to develop Enterprise Architectures.

At the whole-of-government level, an Architecture team shall maintain the IndEA framework by continuously evolving reference models through the transformation journey. Thereby, IndEA is kept relevant and as a means of identifying new common capabilities.

It is to be emphasized that developing and implementing the Enterprise Architecture is a medium-term exercise that can spread typically over **3 to 5 years**, depending upon the size of the enterprise and the availability of resources.

About the Document

Background

The Standardization Testing and Quality Certification (STQC) in the Ministry of Electronics and Information Technology (MeitY), Government of India designed the India Enterprise Architecture (IndEA) Reference Models (RMs) during the period Oct 2016 - June 2017. The development of IndEA RMs included various participating agencies like the National Informatics Centre (NIC), Centre for Development of Advanced Computing (CDAC), STQC, The Open Group, academic institutions and industry representatives from the Open Group members. During the course of the development, views and comments were sought from the broader ecosystem through a process of public consultation.

Purpose

The primary purpose of IndEA is to help state governments, ministries and departments in the governments at various levels to adopt a structured approach for developing their enterprise architecture. This is necessitated due to inconsistent maturity levels that exist in various government entities with respect to architecture driven approach to digital governance, yet mandated to adopt Digital India. Therefore, IndEA is expected to fill a clear gap in current capability and drive its adoption in an effective manner to build a digital economy.

Scope

IndEA is a collection of architecture reference models. Reference models are documented best practices for solutions delivery teams to make effective design and technology choices. The purpose of the reference models is to increase adoption of standards, speed up service design and delivery, and advance towards the target state architecture. IndEA aims at:

- Documenting and sharing explicit and implicit architecture best practices;
- Providing guidance in the development of enterprise architectures;
- Capturing the key elements of architecture and inter-relationships between them;
- Providing the means for architecture governance by enabling an audit process;
- Enabling the adoption of standards based on common understanding; and

Intended Audience

IndEA is intended for the following groups:

- All state governments, central government ministries and other government departments especially those that do not currently have an enterprise architecture initiative or are just in the early stages of their enterprise architecture development;
- Senior government officials who have been tasked to oversee and guide enterprise architecture initiatives to augment their understanding and promote active commitment;
- Government Leaders, Chief Architects, Analysts and Designers seeking better, quicker and easier approaches to respond to the needs of their internal and external customers;

The following groups will also find IndEA useful:

- Policy Analysts, Line-of-Business Managers concerned with maximizing business value of IT and business competitiveness;

- Consultants and practitioners desirous of new solutions and technologies to improve the productivity of their government clients;
- Business management, public policy and IS management educators interested in imparting knowledge about this vital discipline; and
- Electronic government professionals involved in organizational technology strategic planning, technology procurement, management of technology projects, consulting and advising on technology issues and management of total cost of ownership.

Structure

There are two documents provided in the **IndEA**.

IndEA Framework: Describes eight reference models.

IndEA Adoption Guide: Elaborates how IndEA can be used in conjunction with an industry standard architecture methodology, the TOGAF® ADM.

IndEA Framework is organized as follows:

Chapter 1 explains the context, purpose, value and rationale for IndEA, its Vision and how it aims to guide state governments and central ministries in developing their own enterprise architectures.

Chapter 2 presents the principles of Enterprise Architecture and the structure of IndEA framework.

Chapter 3 deals with the measurement of the performance of the enterprise, aimed to focus and direct the efforts towards specifically defined outcomes and their impact on governance.

Chapter 4 covers the business of government, by focusing on services governments deliver to the citizens, businesses and other government entities. The section aims to provide a business frame of reference for the architecture initiative.

Chapter 5 deals with structuring the data essential for digitizing government services and forms a critical link to the technical domains of the architecture. This section also provides the inputs to make governments more data-driven and evidence-based.

Chapter 6 covers the applications and systems that are designed, developed, deployed and managed to automate government services. This section also identifies common, shared and specific applications facilitating economies of scale benefits to government entities.

Chapter 7 provides the means to organize and take benefit of the technology landscape by standardizing the technology infrastructure and providing the means to derive economies of scale benefits.

Chapter 8 provides the framework for the integration of applications, processes and data aimed to ensure that individual applications and systems operate in a well-orchestrated and coherent manner, rather than in a piecemeal and fragmented way. This section provides the ability to build line-of-sight.

Chapter 9 covers the means to provide information at the right time, in the right place, to the right people, in the right form using the right channel in a secure manner.

Chapter 10 presents the governance mechanisms required to ensure that the architecture is adopted and its benefits are derived, by delineating the roles and accountabilities.

Chapter 11 provides guidance to deal with specific implementation issues, covers best practices from field-tested initiatives and directions to navigate the implementation complexities and challenges.

About the Document

IndEA Adoption Guide is provided as a separate accompanying document.

Related Documents

This document is to be read in conjunction with the following:

- **IndEA Adoption Guide – A Method Based Approach**

Acknowledgments

A working group constituted by STQC, under the leadership of Shri J. Satyanarayana, Chairman, UIDAI, Government of India developed the IndEA Framework during October 2016 - June 2017. The group represented an eclectic collection of experts and professionals. Following were the contributors during the development of IndEA Framework & IndEA Adoption Guide:

1. **Shri. J. Satyanarayana**, Chairman, UIDAI, Govt of India (Chairman of EA)
2. **Shri. Ashok K K Meena,** Secretary E&IT, Govt of Odisha
3. **Shri. Talleen Kumar,** Principal Secretary, Government of West Bengal
4. **Shri. V. K. Gautam**, Principal Secretary (IT), Govt of Maharashtra
5. **Shri. R.N. Palai**, Special Secretary (E & IT), Govt of Odisha
6. **Shri. Lalhmachhuana,** Secretary & Commissioner IT, Govt of Mizoram
7. **Shri. Dhananjay Dwivedi,** Secretary, Govt of Gujarat
8. **Shri. U. K. Nandwani**, Director General, STQC, Govt of India
9. **Shri. D.C. Misra**, Deputy Director General, NIC, Govt of India
10. **Dr. Rajesh Narang,** CTO, Government e-Marketplace
11. **Smt. Kavita Bhatia,** Director, MeitY, Govt of India
12. **Shri. C.S. Bisht**, Senior Director, ERTL (N), STQC, Govt of India
13. **Shri. B.S. Kumar** (Member Convener of EA), Scientist 'F' & Director-in-Charge, ETDC-Bangalore, STQC, Govt of India
14. **Shri. Muraleedharan Manningal**, Head of e-Governance, SeMT, Govt of Kerala
15. **Shri. Gunalan I.**, Head, SEMT, Representing Govt. of Telangana/ AP
16. **Dr. Pallab Saha**, Chief Architect, The Open Group
17. **Smt. Rama Hariharan**, Senior Technical Director, NIC, Govt of India
18. **Shri. James De Raeve**, Vice President, The Open Group
19. **Dr. Padmaja Joshi**, Joint Director, CDAC, Govt of India
20. **Shri. Abraham Koshy**, Country Manager, The Open Group
21. **Shri. Padmanabhayya**, Director-in-Charge, ETDC-Hyderabad, STQC, Govt of India
22. **Shri. Prasanna Anantharamaiah**, Chief Technologist, HP Enterprise Software Services
23. **Smt. Seemantini SenGupta,** Senior Technical Director, NIC, Government of India
24. **Shri. Manojit Bose,** Sr. Director, NASSCOM
25. **Dr. Gargi Keeni,** Ex.VP of TCS
26. **Shri. Atul Gupta**, Director, STQC, Govt of India
27. **Smt. P. Gayatri**, Technical Director, NIC, Govt of India
28. **Shri. SivaPrasad Inokondu,** Scientist 'C', STQC Directorate, MeitY, Govt of India
29. **Shri. Jitender Mittal**, Scientist 'C', STQC Directorate, Govt of India
30. **Prof. Krishna Moorthy Sivalingam,** Head of CSE Dept, IITM

31. **Dr. Uday Khedker,** Professor & Head, Department of Computer Science & Engg. IIT Mumbai
32. **Shri. Srikanth Akula,** IT Architect, Representing GoAP
33. **Shri. Sreekanth R. Iyer,** Cloud Security Architect – IBM
34. **Shri. Akhilesh Kumar,** SEMT, Govt. of Telangana/ AP
35. **Shri. Rituparna S. Kadam,** Enterprise Architecture Consultant, Wipro Limited
36. **Shri. Abhishek Ojha,** Enterprise Architecture Consultant, Wipro Limited
37. **Shri. Sarat Sankar,** Enterprise Architecture Consultant, Wipro Limited
38. **Shri. Linga Murthy,** Enterprise Architecture Consultant, Wipro Limited

1. The IndEA Context & Vision

1.1. The Context

The e-Governance initiatives in India have acquired a new momentum with the launch of the Digital India program by the Central Government. The thrust given to Aadhaar and the emphasis on its adoption in the various welfare schemes have created the expediency for painting the big picture of e-Governance so as to derive the maximum out of this soft infrastructure. A large number of e-Governance initiatives have been implemented in the country during the last decade by the Central and State Governments. An analysis of e-TAAL portal, which displays in real-time the number of e-Transactions happening across the country reveals the following:

a. The volume of e-transactions has been increasing significantly during the recent years. The annual volume during the calendar year 2016 has been 11 Billion. It is likely to exceed 13 Billion during the year 2017.
b. The volume of **transactions availed per day** has increased from 6.5 million in 2013 to 37.2 million in the current year – representing a 5-fold increase in 4 years.
c. There is a significant variation across the States in **the number of transactions per 1000** population p.a. – from a high of 22,000 to a low of 200.
d. There is also a huge variation across the States (with large and medium population) in the **number of transactions per service p.a.** – from a high of 4.1 million to a low of 0.1 mil.

The above analysis indicates that there is a huge potential to scale up the volume and variety of e-services provided to the citizens, if a systematic and holistic approach is adopted to design and implement hundreds of e-Governance initiatives across the country.

The need for adopting a holistic approach in the domain of e-Governance has become evident from the interoperability issues within and across multiple clusters of stand-alone applications developed by the States and Central Ministries over the last decade.

While India has made reasonable progress in improving its e-Government Development Index (EGDI) from 0.3730 in 2003 to 0.4637 in 2016, it is a matter of concern that we have been consistently below the global average by three to ten percentage points during this period. The latest EGDI of India is 0.4637, which is far below the global best of 0.9193. In this regard, it is to be noted that the UN e-Government Survey 2016 points out the need for national governments to adopt a Whole-of-Government strategy while designing their e-Governance programs.

Against this background, the Working Group constituted by the Central Government has come up with a holistic framework, named **IndEA**, for streamlining, standardizing, and optimizing the e-Governance efforts across the country.

1.2. IndEA defined

IndEA, a catchy acronym for the **India Enterprise Architecture**, is a framework for developing a holistic architecture treating the Government as a single enterprise or more realistically, as an **Enterprise of Enterprises**, which are functionally inter-related. IndEA is a structured combination of several Reference Models that, together, enable a **boundary-less flow of information** across the length and breadth of the government and facilitate the delivery of **integrated services** to the stakeholders, namely, the citizens, businesses and employees. Strictly

speaking, IndEA is not an Enterprise Architecture as its name seems to connote. It is a comprehensive and convenient *framework* for developing Enterprise Architectures by governments. It can be adopted and used successfully, by the Central, State and Local Governments alike, irrespective of their size and current status of technology implementation. It can also be used by large departments and agencies of the Government to derive the envisaged benefits.

Simply stated, IndEA is a way to establish **Unity in Diversity** in the domain of e-Governance. It is a framework that enables the development and implementation of Enterprise Architectures independently and in parallel by all governments and their agencies across India, conforming to the same models and standards.

1.3. Vision & Value Proposition of IndEA

The Vision of IndEA is "***to establish best-in-class architectural governance, processes and practices with optimal utilization of ICT infrastructure and applications to offer ONE Government experience to the citizens and businesses***".

IndEA brings to the table the entire value proposition of adopting Enterprise Architecture plus more. It derives its approach from the globally known architectural frameworks like the TOGAF, Zachman and the Federal Enterprise Architecture. The models and concepts contained in these global frameworks have been substantially simplified and completely contextualized to the Indian conditions. The principles of 'Just-in-Time' and 'Just Enough' have been advocated in the design and implementation of Enterprise Architecture.

The following is a list of major benefits to be derived by the adoption of IndEA framework:

1. Provide a **ONE Government Experience** to the citizens and businesses, by offering integrated services through multiple channels, in a contactless, frictionless manner.
2. Enhance the **efficiency** of delivery of services, by defining and enforcing service levels of a very high order
3. Improve the **effectiveness** of implementation of the developmental and welfare schemes through a holistic performance management.
4. Enhance the **productivity** of employees and agencies through quicker access to up-to-date information and single-sign-on features.
5. Provide integrated and cross-cutting services through seamless **interoperability** across the Whole-of Government.
6. Bring in **flexibility** and **agility** in making changes to the systems to align with the best practices and to leverage the latest technologies.
7. Realize **cost-effectiveness** through use of shared infrastructure and services.
8. Enable establishing a Connected Government that works for **inclusive development**.
9. Maintain the right balance between **security** of data and **privacy** of personal information.

IndEA aims to define the strategic use of Information and Communication Technology by the Government to enable transformation of Government and Governance towards a connected ***ONE GOVERNMENT***. It offers the effective process for translating Government's vision and strategy into effective change in the Government Enterprise from people, process and technology perspective and their relationship with one another and with the external systems to create an integrated environment that is agile, pro-active and predictive.

The Vision of IndEA is represented schematically in **Figure 1.1**.

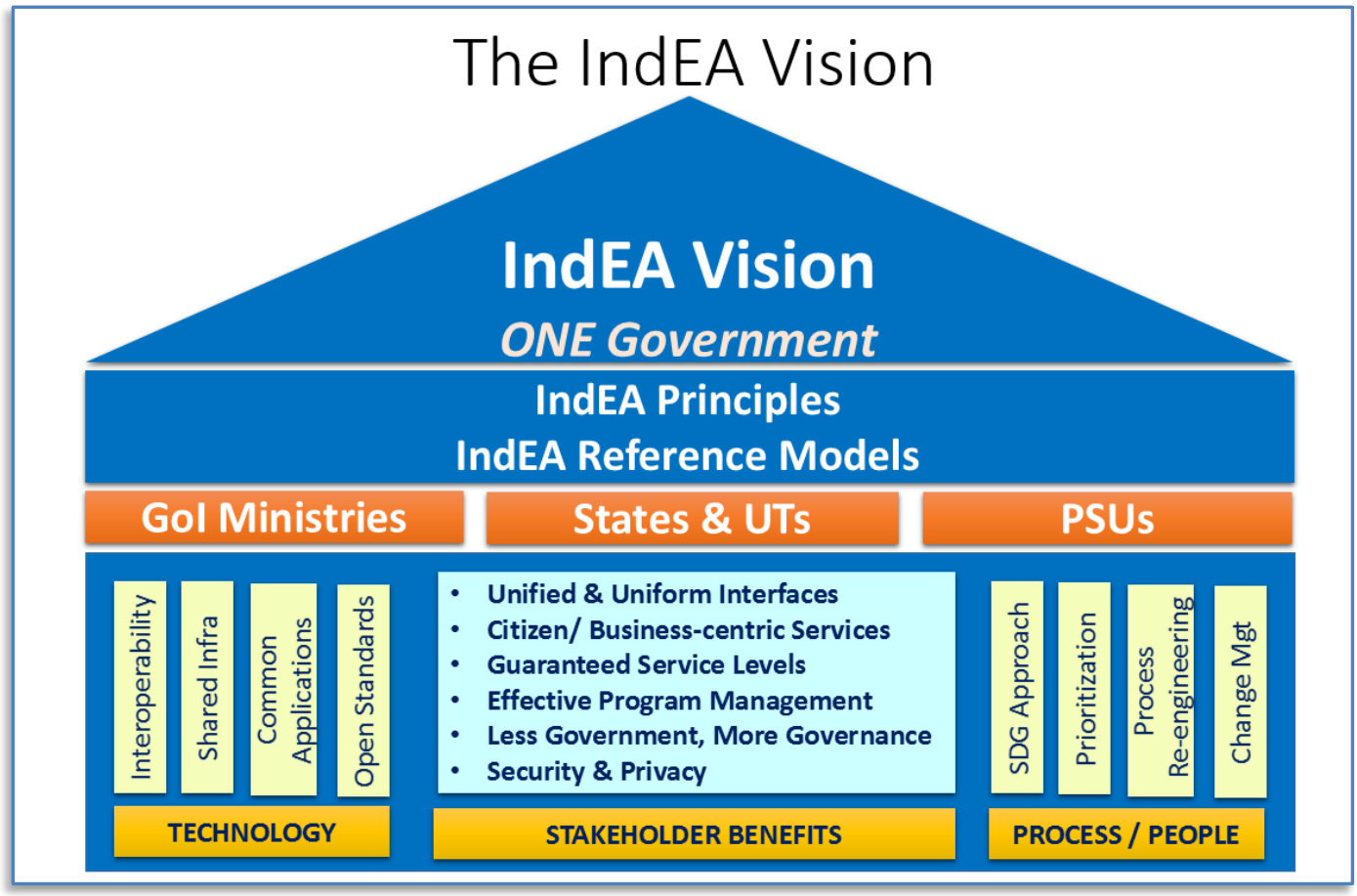


FIGURE 1.1: VISION OF INDEA

The long-term vision of IndEA is to create a ONE Government Experience. In the short and medium-term, however, the **IndEA** framework seeks to enable the Central Ministries, States / Union Territories, State Departments, Zilla/District/Gram Panchayats, and large PSUs to establish a **better governance** though a concerted approach to implementing the Enterprise Architecture. The **Figure 1.1** highlights the major benefits sought to be given to the stakeholders and the methods required to be adopted in the areas of **Technology, Process and People**, to achieve the end goals.

IndEA has been designed and developed broadly on the established Enterprise Architecture Frameworks and has incorporated best practices and guidelines for developing EA frameworks. Various reference architectural models, frameworks, tools and guidelines are offered to optimize the Government ecosystems to achieve the overall Vision of Digital India.

2. IndEA Structure & Principles

2.1. Structure of IndEA

IndEA is a framework for designing Enterprise Architecture for any Government Organization. IndEA does not *by itself* constitute an Enterprise Architecture. However, it is an important first stepping stone for designing and developing Enterprise Architecture for any Government or an Agency/ Department of the Government. IndEA maintains its generic nature by retaining itself at the level of Reference Models and not getting down into domain-specific architectural details, much less any of the implementation details.

In line with other globally known architectural frameworks, the structure of IndEA consists of a number of Reference Models, each dealing with a specific domain of the Enterprise Architecture. **A Reference Model is an abstract representation of the entities relevant to a domain of the Enterprise Architecture, the inter-relationships among those and the standards to be followed**. The representation is both **graphical** - adopting standard notation like the UML, and **descriptive** - specifying the capabilities of each of the components (entities) comprising the Reference Model. Each Reference Model also contains the list of standards that should govern the entities, their relationships and the manner of communications between them. All the Reference Models comprising IndEA are technology-agnostic. These Reference Models are, by definition, devoid of details specific to their implementation.

By a combination of the above-stated 3 basic attributes of all the Reference Models, namely, **abstraction, standards-base and technology-neutrality**, the IndEA framework is sufficiently generic for its widespread adoption by a variety of entities in the domain of the Government from the national to state to local authorities and organizations.

IndEA framework comprises of 8 Reference Models, represented graphically in Figure 2.1. viz., Business, Application, Data, Technology, Performance, Security, Integration and Architecture Governance.

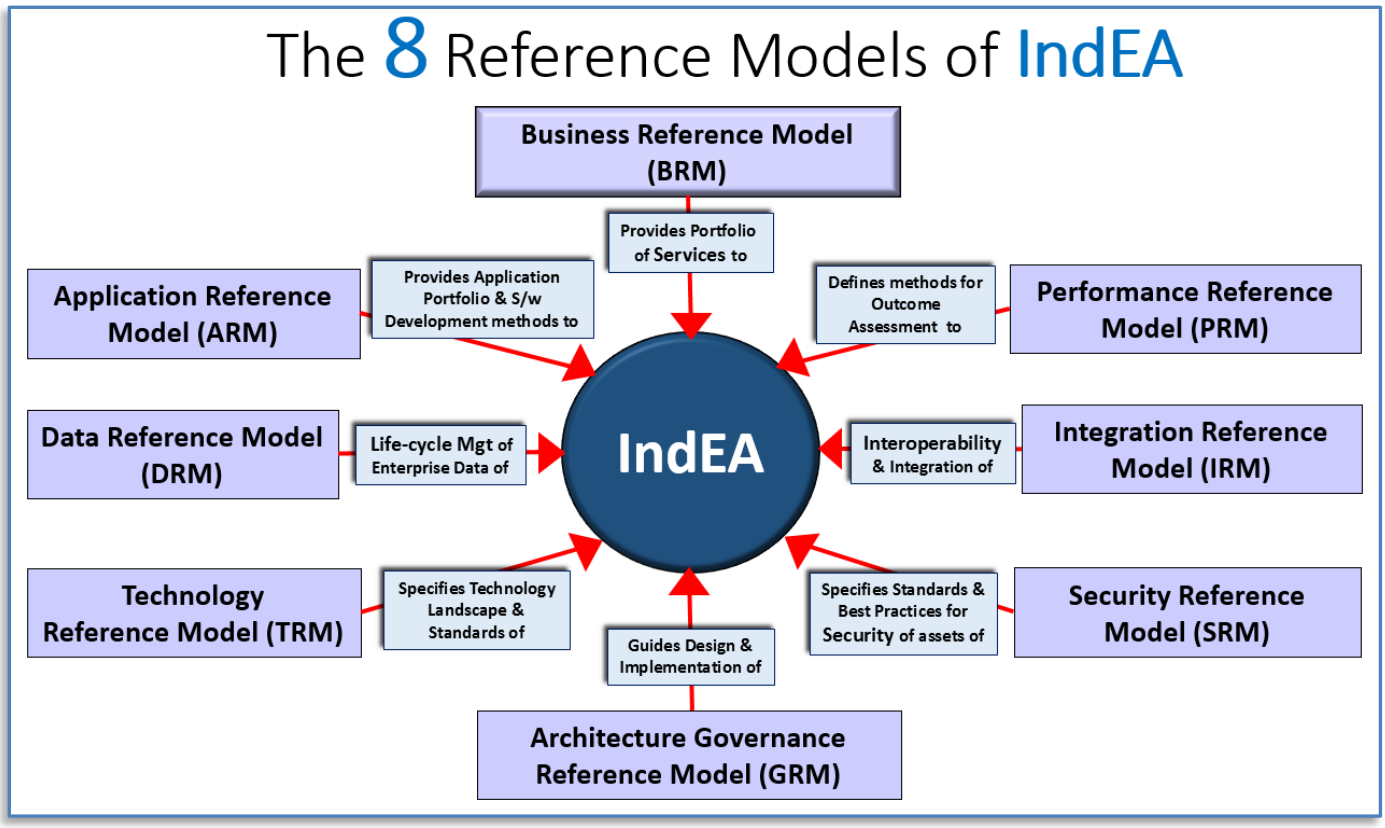


FIGURE 2.1: REFERENCE MODELS OF INDEA

2.2. Principles of IndEA

An Enterprise Architecture is to be founded on a set of **Principles** that inform and guide the Architecture Development process. Principles are of two types – **Enterprise Principles** and **Architecture Principles**. Enterprise Principles provide the basis for high-level decision-making for fulfilling the organizational goals and mission. Architecture Principles derive from the spirit of the Enterprise Principles and govern the process of development, maintenance and use of the Enterprise Architecture. Enterprise Principles relate to the functions in the domains of Performance, Business and Architecture Governance. Architecture Principles relate to the domains of Application, Data, Technology, Security and Integration.

A good set of Principles should satisfy five criteria, namely, **Understandable, Robust, Complete, Consistent and Stable**.

While individual sets of principles have been stated and explained in the respective Chapters relating to the 8 Reference Models, an aggregate view of these principles is given in **Table 2.1**.

Citizen-centricity, Outcome-focus, Standardization, **Reusability** and **Integration** are the key ***mantras*** followed while designing IndEA. Accordingly, the Principles stated below reflect these pivotal concepts.

All the Reference Models must conform to the standards laid down by the Enterprise Architecture, keeping the enterprise requirements above the domain compulsions.

Name of Principle	Principle Statement
Performance	
SDG Linkage	Performance Measurement Systems derive from and are linked to Sustainable Development Goals prioritized by the Government.
Outcome Orientation	All Performance Measurement Systems are outcome-oriented.
Identifying Performance Categories through Value-Chain	Performance Measurement Categories must cover the entire value chain such that the KPIs at each step of the service can be monitored and performance optimized.
Enable quantitative and qualitative data driven decisions	The PRM must enable quantitative and qualitative data driven decisions through a better analysis of the actual output & outcome.
Business	
Maximization of benefit	All Information Management decisions are made to maximize the benefit to Government as a whole.
Prioritization of SDG Initiatives	Enterprise Architecture efforts focus on the SDG Initiatives prioritized by the Government.
Integrated Services	Integrated Services that cut across agency-silos are identified, designed and delivered through multiple delivery channels, to realize the vision of ONE Government.
Process Re-engineering	Existing processes are re-engineered to eliminate non-value-adds and to make the services citizen-centric / business-centric.
Application	
Ease of Use	Applications are easy to use, with the underlying technologies being transparent to the users.
Sharing & Reusability	All commonly required Applications are abstracted to be built once and deployed across the Whole-of-Government through reuse and sharing. Sharing & Reusability shall be subject to conformance with the principles of Security & Privacy.
Technology Independence	Application Design is open standards-based and technology-independent.
Application Security	Applications are secure by design and developed using secure coding standards and practices.
Data	

Name of Principle	Principle Statement
Data Asset	Data is an asset that has a specific and measurable value to the Government and is managed accordingly. Archive and preserve all information (both in raw and aggregated form) exchanged, especially outside the government ecosystem, for future reference and if needed, for resolution of disputes. The Archival and preservations must be in accordance with the applicable regulatory requirements.
Data-sharing	Data is shared across the Government, subject to rights and privileges, so as to prevent duplicative sets of data by different agencies. Data Sharing shall be subject to conformance with the principles of Security & Privacy.
Data Trustee	Each dataset has a trustee accountable for data quality and security.
Data Security	Data is protected from loss, unauthorized use and corruption, through adoption of international standards and best practices, duly protecting the privacy of personal data and confidentiality of sensitive data.
Common Vocabulary and Data Definitions	Data is defined consistently throughout all levels of Government, and the definitions are understandable and available to all users.
Technology	
Technology Independent Architecture	Enterprise Architectures are developed in a technology-neutral manner so as to avoid captivity to a specific product or implementation method.
Future-proof Architecture	Enterprise Architectures are suitably designed and developed so as to be future-proof, not requiring frequent revisions with the advent of every new technology.
Open Standards	Open Standards are adopted in the design and implementation of all greenfield systems. Legacy systems are incentivized to migrate to open standards, where required.
Shared Infrastructure	IT Infrastructure is shared to ensure optimal utilization and effective maintenance.
Cloud First	Cloud infrastructure is chosen by default for deployment of applications and on-site option is resorted to only with strong justification.
Mobile First	Mobile channels are the mandatory for delivery of all services, among all delivery channels.
Availability	The information systems along with the applications and services are available 24 x 7.

Name of Principle	Principle Statement
Integration	
Openness and Transparency	Government data is made open, barring exceptions, so that external parties can build services.
Interoperability	Interoperability is assured through adoption of open standards and open interfaces.
Data Portability	Data is easily transferable and usable across jurisdictions, applications and systems.
Primacy of User Experience	All service interactions are designed with citizens at the core, by providing integrated multi-channel service delivery.
Elimination of Digital Divide	Digital public services are available to citizens and users belonging to all groups, and there are no differences and discrimination based on location (rural versus urban), access to technological infrastructure, and physical abilities.
Multilingualism	Services are delivered in language/s that are preferred by the consuming populations with the option of multi-lingual support, wherever feasible.
Security	
Data Integrity	Data is correct, consistent and un-tampered.
Data Privacy and Confidentiality	Data is shared on a Need-To-Know basis and is collected/accessed/ modified only by authorized personnel.
Architecture Governance	
Primacy of Principles	These principles of enterprise information management apply to all organizations in Government.
Discipline	All stakeholders of EA Governance structure need to follow the discipline of conformance to the principles and standards.
Transparency	The architectural decisions taken are transparent to all stakeholders.
Accountability	Stakeholders, including service providers are accountable for the responsibility assigned to them in the Architecture Development and Implementation, and in strict adherence to these principles.

TABLE 2.1: PRINCIPLES OF INDEA

One of the important responsibilities of Architectural Governance is to ensure that the IndEA Principles are strictly adhered to while designing each component of the Enterprise Architecture. This enforcement is to be done initially during the stage of converting the Reference Models into respective Architectures and subsequently at the stage of design of solution(s).

3. Performance Reference Model

It is well said that Enterprise Architecture is NOT about making a better *Architecture* but is about making a better *Enterprise*. This translates to the need for the EA effort to drive the efforts of the organization to a **better performance**, measured along multiple complementary dimensions. These multiple dimensions include results in the four Measurement Areas – Vision, Citizen, Processes and Technology. The **Figure 3.1** represents the approach to measuring the performance of the enterprise along these areas and the relevant Measurement Categories in each area.

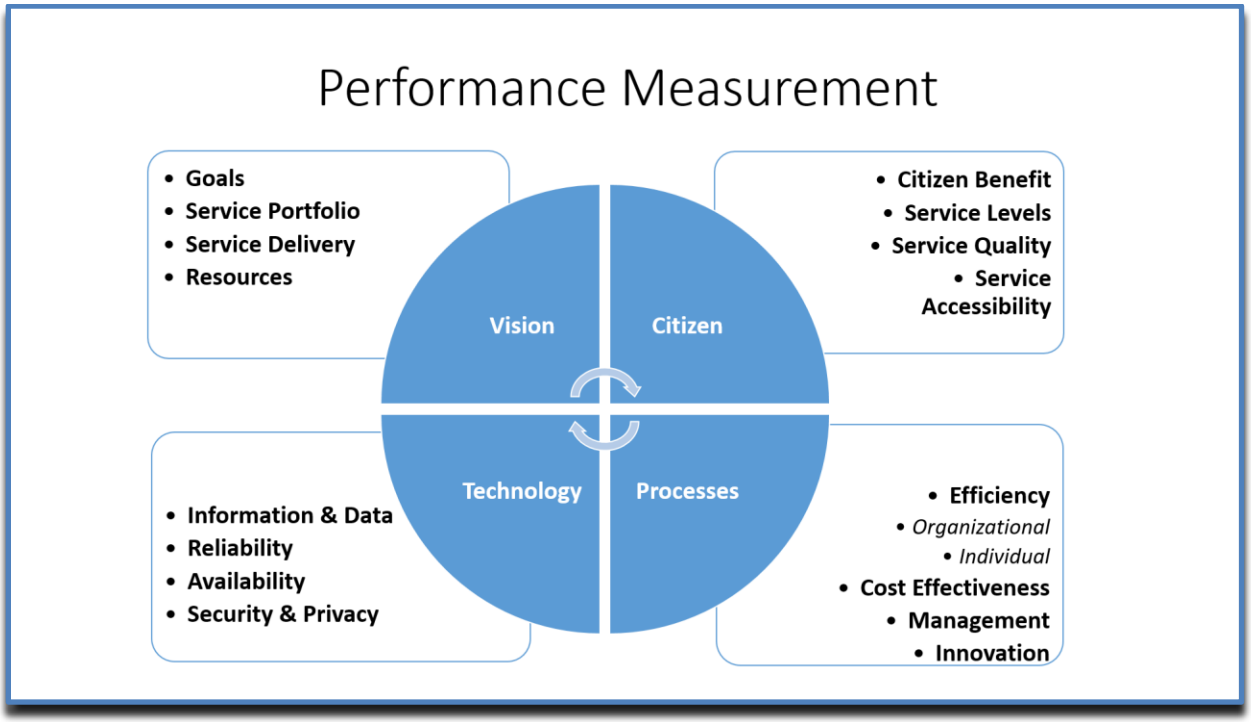


FIGURE 3.1: METAMODEL OF ENTERPRISE PERFORMANCE MANAGEMENT

The metamodel represented in the **Figure 3.1** has to be applied at multiple levels of the Enterprise, like the Ministries and Departments of Government. It should also be applied in respect of each of the major Goals of the Enterprise, like the **Sustainable Development Goals** in the context of Government. The measurements done at the granular levels of the Enterprise like the departments and divisions need to be integrated, aggregated and represented at the Enterprise level. All these performance measurement and management functions can be designed using the Performance Reference Model.

Performance Reference Model (PRM) *provides a uniform and consistent mechanism to measure the efficiency and effectiveness of the different sectors or domains in achieving the overall goals of the Government in a cost-effective manner. The principal instrument of the PRM is a set of KPIs designed rationally to measure the outputs and outcomes of the various programs, schemes, projects and activities. A prioritized and phased*

approach for implementation of PRM is recommended so as to avoid the situation of creating plethora of KPIs, which hide the actual performance and outcomes.

3.1. PRM Objectives

The Objectives of PRM are:

a. Developing the Architecture for **measuring** the Government (Enterprise) Performance along multiple dimensions like the Business, Citizen, Process and Technology.
b. Defining the framework for developing an **outcome-oriented** Performance Management system, which establishes a strong co-relation between Services provided by Line Department(s)/ Business Function(s) and its impact on Stakeholders.
c. Aligning the IT and e-Governance efforts to the **vision** of the Government, aimed at the development and welfare of the society.
d. Enabling a focused and streamlined approach to measuring the progress of the country or State towards achieving the **Sustainable Development Goals** and the targets set for the same.
e. Creating a framework for defining a set of consistent, sustainable, integrated and self-policing **Key Performance Indicators (KPIs).**
f. Setting out an improvement plan to optimize services towards internal and external customers, to improve collaboration between agencies and 3rd parties and to optimize the usage of ICT assets.

3.2. PRM Concepts and Definitions

Concepts[1]:

a. Effectiveness: Meeting the enterprise objectives and achieving the intended outcomes, by pursuing the **right set of Goals.**
b. **Efficiency:** The relationship between resources employed and outputs delivered; in terms of quantity, quality and timeliness.
c. **Economy:** Minimizing the cost of resources used by acquiring them in due time, appropriate quantity and quality and at the best price.

Definitions:

a. **Key Performance Indicator or KPI** is a metric designed to evaluate the success of an organization or of a particular activity - such as a project, program, scheme or initiative undertaken by it.
b. **Output** is a measure of the quantity of applications, access points, or services produced by a government entity in a given period of time.
c. **Outcome** is a measure of the **impact** produced by the output of a project, program, scheme or initiative undertaken by an organization.
d. **Impact** is a measure of the changes – both quantitative and qualitative - that can be attributed to a particular intervention, such as a project, program or policy, both the intended ones, as well as the unintended ones.

[1] Source: http://www.cag.gov.in/sites/default/files/cag_pdf/PA_Guidelines2014.pdf

e. **Measurement Parameters** are the parameters which reflect the efficiency/ effectiveness/ economy of the Service. They determine the output, outcome and economic delivery of the service. A single Service may have one/ more measurement parameters.
f. **Measurement Frequency** indicates how often the efficiency/ effectiveness must be evaluated. Measurement Frequency is based on the nature of the Service that is being fulfilled.

3.3. PRM Principles

Principle PRM 1: KPIs in PRM must be linked to the Goals & Objectives defined by Government
The Government defines its goals and objectives, which may be derived from and are linked to the Sustainable Development Goals. The KPIs in the PRM must have parameters to measure the extent to which the Goals and Objectives are achieved.

Principle PRM 2: Performance Reference Model must be Outcome Oriented
The overall objective of the Government is to deliver Services efficiently and effectively to the Stake-holders. The impact of these services on the stake-holders is measured via the effectiveness i.e. Outcome of the Services.

Principle PRM 3: Performance Measurement Categories must be identified throughout the Value Chain
The Value Chain comprises of all the Line-departments and Business Functions that participate in fulfilling a Service. Performance Measurement Categories must cover the entire value chain such that the KPIs at each step of the service can be monitored and performance optimized.

Principle PRM 4: PRM must enable quantitative and qualitative data driven decisions
The PRM must enable quantitative and qualitative data driven decisions to through a better analysis of the actual output & outcome.

3.4. PRM Schematic

The Performance Reference Model provides a mechanism to measure the efficiency and effectiveness of the different domains in achieving the overall **goals and objectives** of the government as depicted in **Figure 3.2** below.

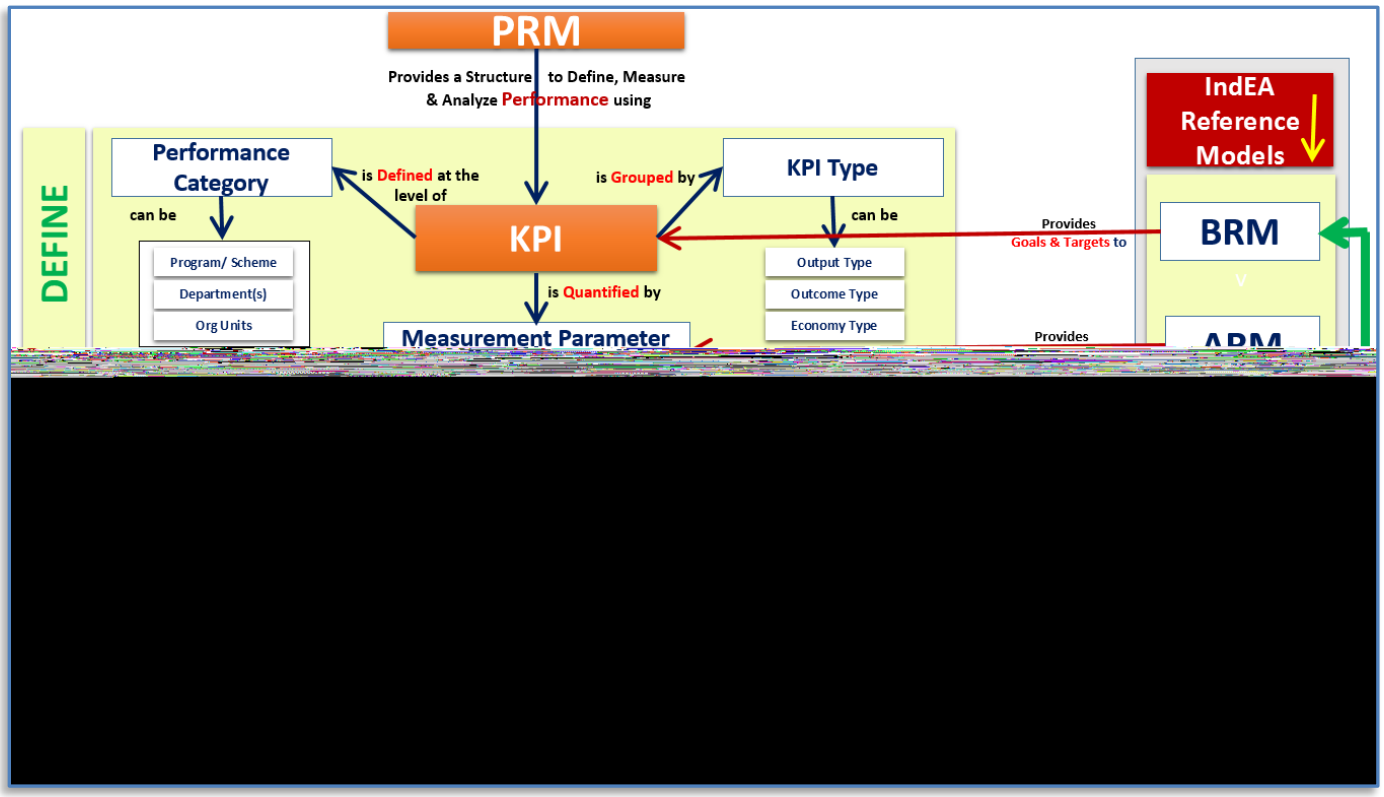


FIGURE 3.2: PERFORMANCE REFERENCE MODEL (PRM) - CONCEPTUAL VIEW

PRM Explained

PRM Stages

As revealed from graphic in Figure 3.2, PRM consists of **3 major Parts**, which, by virtue of the fact that they have to be developed sequentially, may also be called the **Stages**. These are

(A) DEFINE **(B) MEASURE** and **(C) ANALYZE** stages.

A. The DEFINE Stage

The **DEFINE** Stage starts with identification of the Goals prioritized by the Government, collecting the lists of Programs, Projects and Schemes that are undertaken or planned to realize the goals and defining the measurable KPIs for each of the shortlisted Programs, Projects and Schemes. The DEFINE Stage concretizes **WHAT** to measure. The following guidelines enable defining a more rational set of KPIs:

a. KPIs set the **targets** to be achieved to attain the *Goals & Objectives* established by the Government.
b. KPI's are of 3 types – **Output KPIs, Outcome KPIs and Economy KPIs**. Output KPIs measure the **efficiency** of a Program, Project and Scheme, basically in a **quantitative** manner. Outcome KPIs are designed in such a manner as to assess the **quality** of services provided to the stakeholders. Economy KPIs elicit the

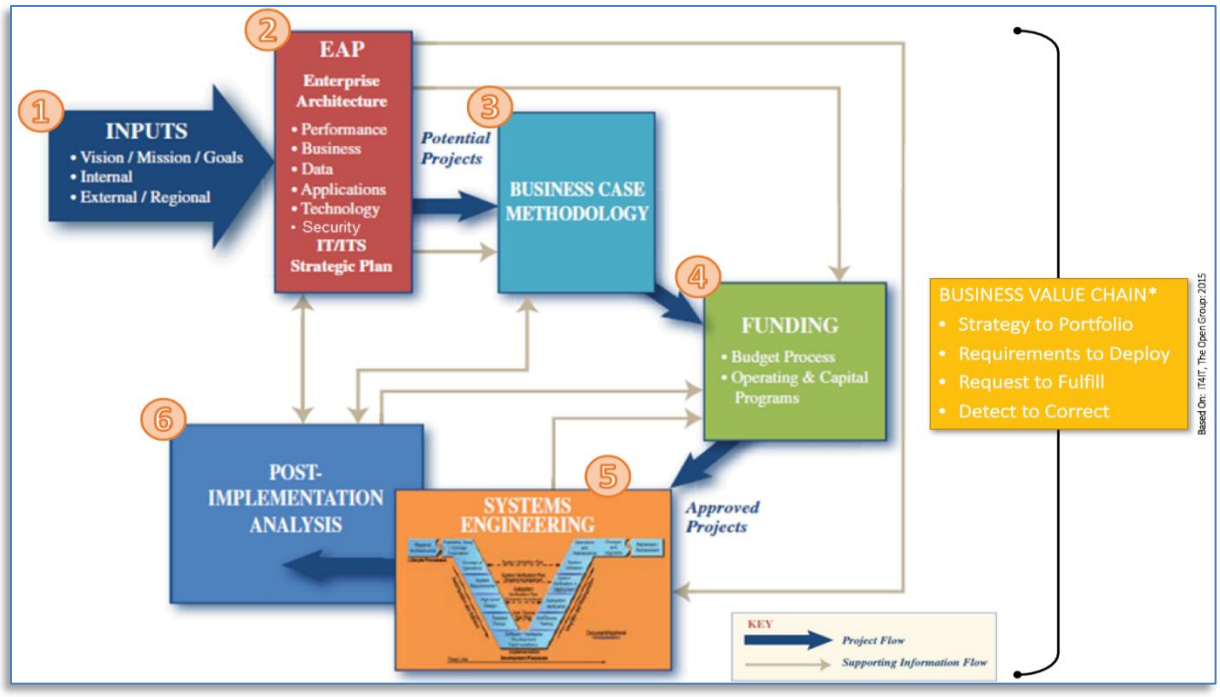


FIGURE 3.4: EA BUSINESS VALUE CHAIN

Measuring EA Value (Financial Metrics)

Common financial metrics for EA value include:

- Return on Investment (ROI):
- Benefits-to-Cost Ratio (B/CR):

The key to financial metrics is the measurement of benefits. Some benefits are easily quantified and monetized, while others tend to be qualitative and difficult to measure. The other aspect to be factored in is the "lag" in derivation of visible benefits. It usually takes between 24 – 36 months before any impact of the enterprise architecture even becomes apparent.

Measuring EA Value (Non-Financial Metrics)

The actual metrics to be adopted depends very greatly on the EA programme goals and objectives, business and operational priorities, intended outcomes, stakeholders, availability of metrics data, and targeted benefits. The most commonly used EA metrics are categorized into: (1) IT metrics; (2) business metrics; and (3) compliance metrics.

To summarize, the list of metrics adopted by government agencies should be a balance between the dimensions of:

- **Completion**: The extent to which the major phases of architecture conceptualization, development is completed, measured in terms of design of the 8 Architectures and the associated Artefacts, listed in Table 11.1.

- **Use**: The extent to which the architecture is put to use for strategy execution, programme and project management, investment decisions and portfolio analysis, measured by a comparison of the portfolio of Services and portfolio of applications that have been envisaged with the number implemented.
- **Benefits**: The extent to which the architecture is used to derive and report benefits, relevant to the organization. The benefits are in terms of the cost-reduction due to standardization and re-use, cost avoidance due to procuring only the 'just in time' and 'just enough' to meet the needs, cost savings due to more efficient and effective implementation of the development and welfare programs in various sectors, and enhanced effectiveness in planning and coordination due to availability of right information to the right people at the right time.

4. Business Reference Model

The Business Reference Model or **BRM** is pivotal for the design of a good Enterprise Architecture, in so far as it looks at purely the **business vision** and the **functions/ services** required to fulfil that vision, but not the technologies required to be used. The key entity in BRM is **Service**, be it customer-facing or internal. A successful implementation of BRM requires defining or redefining the Enterprise **Vision and Goals**, re-engineering of the **Business Processes**, building of the **service portfolio**, and above all, identification of services that are common across the Government or across groups of departments and abstracting them into a set of reusable/shared services, processes and workflows. In short BRM is about **WHY, WHAT**, **HOW MUCH**, **HOW FAST** and **WHO**.

4.1. Objectives

The Objectives of BRM are:

a. To provide a context and a framework for defining / redefining the **Enterprise Vision, Goals and Objectives**;
b. To describe the customers and the channels they use to interact with the government.
c. To delineate the **Scope** of the Enterprise Architecture effort;
d. To identify the broad parameters on which to assess the **performance** of the enterprise and the success of its endeavor;
e. To describe the **portfolio of services** and functions, which include the existing and new;
f. To enable preparation of a **role-responsibility** matrix;
g. To identify the broad areas requiring **process re-engineering** and recommend methods for undertaking the same;
h. To enable the enterprise to redesign its **organization structure**(s) to meet its Goals and Objectives better and in a coordinated, joined-up manner.

4.2. BRM Concepts & Definitions

Concepts:

a. **'ONE Government'** is an aspirational goal of IndEA whereby a single service delivery interface is offered to the citizens, hiding the boundaries of government agencies. It necessarily involves the breaking of the departmental silos. Since it is not practically feasible to break the silos physically, this laudable objective is sought to be achieved by breaking them virtually.
b. **Virtualization of Departments** is a *conceptual* technology framework that can pave the way for establishing ONE Government through abstraction of services in such a manner that the consumer of service is not exposed to the owner(s) of the processes providing that service.
c. **Heat Map:** Heat Map is a methodology used to identify the **Gap** between current state and target state of a department/ function/ service. Heat Map is color-coded to depict whether a gap is High, Medium or Low. (Please refer to pg 18 of IndEA Adoption Guide for further details on Heat map)

There are four core dimensions to BRM – Customers (Who), Services (Why & What), Organization (With-whom and How) and Process (With-what and How).

Definitions:

a. **Business Process Re-engineering (BPR):** BPR involves re-designing the Business Processes to improve efficiency and effectiveness of a Service while reducing the operational cost.
b. **Service Definition:** Service Definition is the process of specifying the attributes of a service in terms of its Type, Category, Class, Priority and Service Level.
c. **Service Transformation:** Service Transformation is the process of creating significant additional value to the customer through enhanced and guaranteed service levels, added convenience, transparency and efficiency of the delivery system.

4.3. BRM Principles

Principle BRM 1: Maximization of Benefit
Statement: All Information Management decisions are made to maximize the benefit to Government as a whole.

Any decisions made from enterprise (Whole-of-Government) perspective will have greater long-term benefits than the decisions made from that of an individual department. In this process, some departments may have to concede their own preferences to the greater benefit of the enterprise (Government).

Principle BRM 2: Prioritization of SDG Initiatives
Statement: Enterprise Architecture efforts focus on the SDG Initiatives prioritized by the Government

Prioritization of Goals is an inevitable consequence of scarce resources competing to meet the huge expectations of the stakeholders of Government. There are two sources of such goals – the Sustainable Development Goals identified and articulated by the UN, and the goals announced by an elected Government, as part of its election manifesto.

Principle BRM 3: Integrated Services
Statement: Integrated Services that cut across agency-silos are identified, designed and delivered through multiple delivery channels, to realize the vision of ONE Government.

One of the aspirational goals of IndEA is to support establishment of ONE Government. This is made possible *inter alia* through provision of Integrated Services, obviating the need for the citizens/ businesses to interact with multiple Government agencies to achieve their objective.

Principle BRM 4: Business Process Re-Engineering
Existing processes are re-engineered to eliminate non-value-adds and to make the services citizen-centric / business-centric.

New levels of performance in terms of better Efficiencies, Effectiveness and Economy can't be achieved adopting the legacy systems and processes. A fundamental rethinking and redesigning is called for at the operational levels.

4.4. The Business of Government and the BRM Landscape

Enterprise Architecture requires that the Government is viewed as a single enterprise and the domain architectures are designed / redesigned accordingly. Such a **Whole-of-Government** perspective is hard to achieve, but is possible if a strong political will propels the EA initiative. *The key deliverables of WoG are value offered to the stakeholders, degree of coordination achieved within a Sector to realize cross-agency integration, and performance at the cutting-edge level.* WoG and EA have a symbiotic relationship. They are synergistic and mutually reinforcing. One can't undertake an EA exercise without a WoG approach and WoG can't be realized without EA. The essence of the WoG approach is that the Vision and Goals aspired at the apex level percolate to the operational layers in the form of discrete tasks and activities to be completed in a specified timeframe.

4.5. The Value Lifecycle of BRM

Success is about creating Value and delivering it. There could be several existing documents that describe and define the Vision of the Government and the Value it intends to provide. It is desirable to start applying the BRM by leveraging such vision/ strategy documents to begin to formally define value.

The process of using BRM involves traversing round the **Value Lifecycle** of BRM, depicted in **Figure 4.1**.

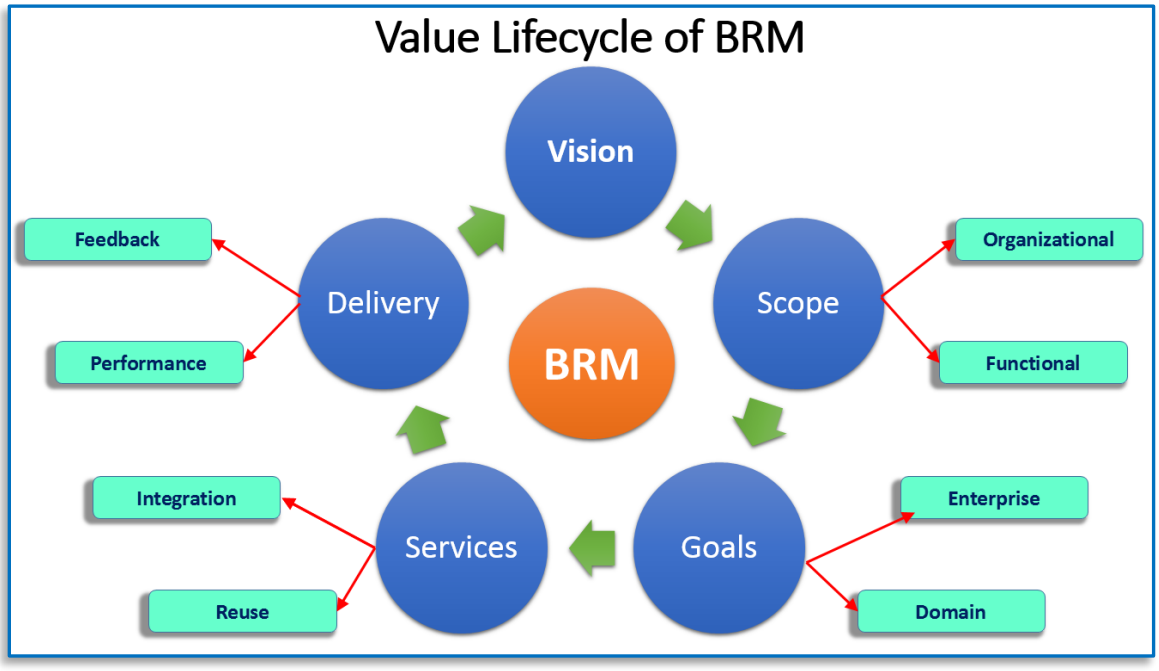


FIGURE 4.1: FRAMEWORK FOR DEFINING & REALIZING VALUE

The following brief description would enable an appreciation of the BRM and initiate the steps necessary to create the Enterprise Business Architecture.

a. Comprehending the pre-existing **Business Vision** of the Government is the necessary first step. As alluded to already it can be drawn from the prior work. It is an essential step to conduct a **Vision Workshop** involving the senior functionaries of the Government to achieve a consensus on what should go into the WoG Vision.

Documenting the IndEA Vision as applicable to a particular State Government or Central Ministry in the form of a **Vision Document** concretizes the same and acts as a useful material for communication.

b. The **Scope** of the IndEA effort has to be carved out consciously from the entire landscape of Governance such that it matches the human and financial resources that can be commanded by the Government. In the **Figure 4.7** that follows, a detailed guidance is provided for choosing from the 16 verticals and 12 horizontals that constitute most of what a State Government does. A Central Ministry, a Local Government or a PSU, which intends to embark on an EA initiative can use the framework given in the Figure **4.7** to define the scope of their EA effort.

c. **Business Goals** are of 2 classes – the Enterprise-level Goals, that apply to the entire Scope of the EA initiative and Domain-specific Goals that apply at the sectoral or departmental level.

d. **Portfolio of Services** is the most critical artefact in the BRM landscape. The focus of the design of the portfolio should be to **maximize reuse and integration** of services.

e. **Delivery** should be designed with 2 objectives in mind – conforming to the **Performance** Standards and closing the Value Loop by providing a **Feedback** to the sponsors of the EA initiative.

4.6. BRM Schematic

After understanding of the Value Lifecycle, an appreciation of the BRM itself becomes the logical next step. The BRM proposed for IndEA is depicted in **Figure 4.2**.

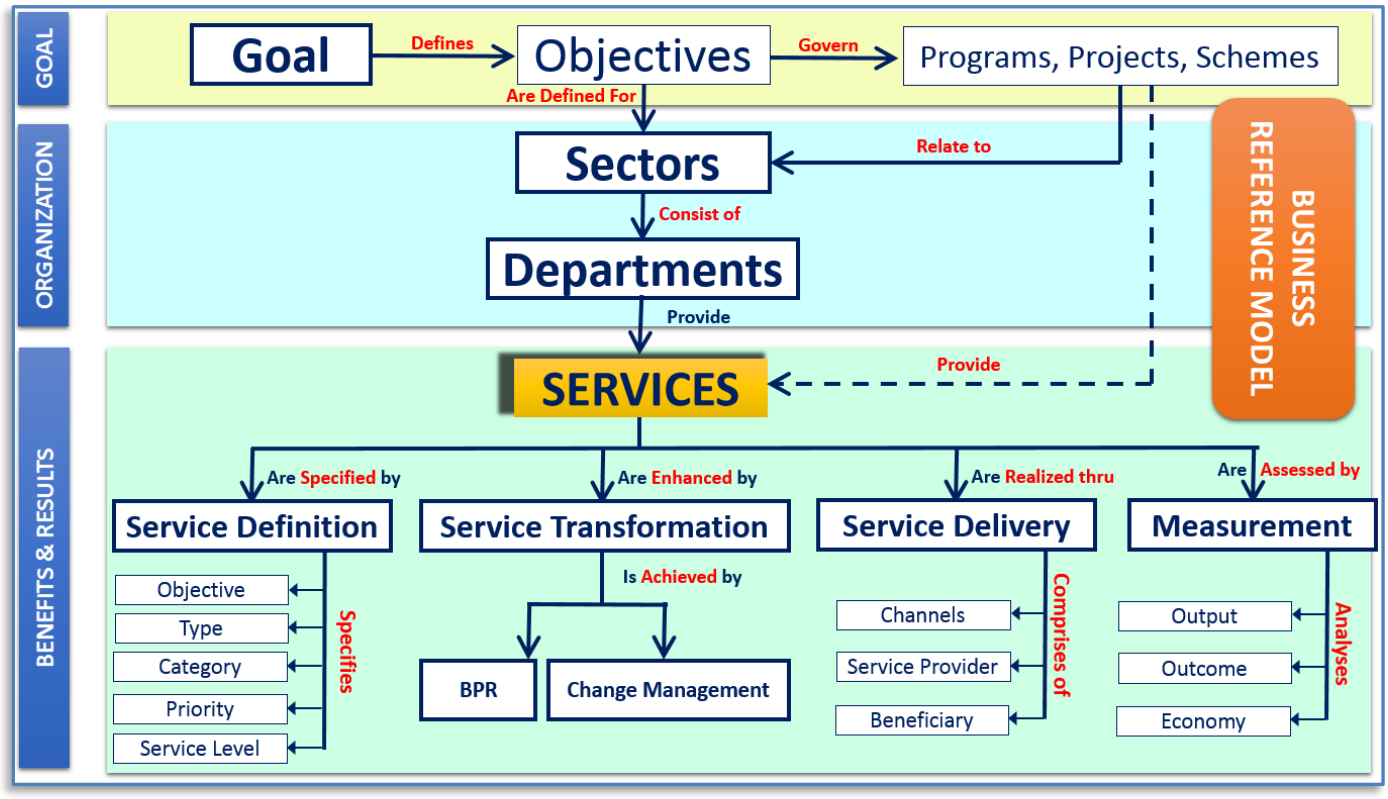


FIGURE 4.2: THE INDEA BUSINESS REFERENCE MODEL (BRM) – CONCEPTUAL MODEL

BRM Explained

The success of any EA initiative depends substantially on the quality and comprehensiveness with which the Business Architecture is designed. The first stepping stone for this is the BRM.

3 Parts of BRM

BRM has 3 major parts –

- **A Framework for Goal-setting** i.e. defining WHAT to do to achieve the Enterprise Business Vision. In fact, defining/ redefining the Vision can also be legitimately an activity within this part of the BRM. The WoG approach and the Value Circle methodology described in the previous two sub-sections contain guidance on the goal-setting role of BRM;
- **A Framework for** restructuring the organization and aligning it to the needs of the EA Vision;
- **A Service Framework** for Defining, Transforming, Delivering and Measuring the Services provided by the Enterprise in fulfilment of the Vision.

The customization and detailed design of the Enterprise Business Architecture is best done in a highly consultative manner, involving all the stakeholder groups in an iterative manner till the alignment of the of the business vision with the **stakeholder expectations** is complete and till the **ownership** of the EA initiative gets partly transferred to the line departments.

Service

Service is the cornerstone of BRM. The important aspects of Service are described in what follows:

Service Catalog or Service Portfolio

The Government achieves its goals and objectives by providing Services to the beneficiaries via various departments. The result of the initial phase of the IndEA initiative is a set of services that, together enable the Government to fulfil the vision. The following guidance is provided in this regard:

a. The typical size of a Service Portfolio of a State Government is about **500**. While the BRM canvas can contain all these services identified in a comprehensive manner, the design of Applications and the delivery of the services can be staggered. Such an approach gives benefits such as avoiding overlap and duplication of services, identifying common services that can be built once and used in multiple contexts, and planning for the interoperability and integration of the services in a more optimized fashion.
b. The BPR accompanying the BRM should enable elimination of services, as a result of simplification of procedures (like self-certification and declaration instead of insisting on production of a certificate issued by an authority), and by modifying them to be suitable for self-service by the stakeholders.
c. The Service catalog rationalized and optimized forms the basis of the design of the Enterprise Application Architecture, following the Application Reference Model.

Service Prioritization

Prioritization of services enables the government to phase them for automation. The Services which have high impact on the stakeholders and/ or have high volume of consumption by stake-holders are identified and

prioritized for Automation. Inter-dependency of services is also factored. The **Figure 4.3** depicts the approach to Service Prioritization.

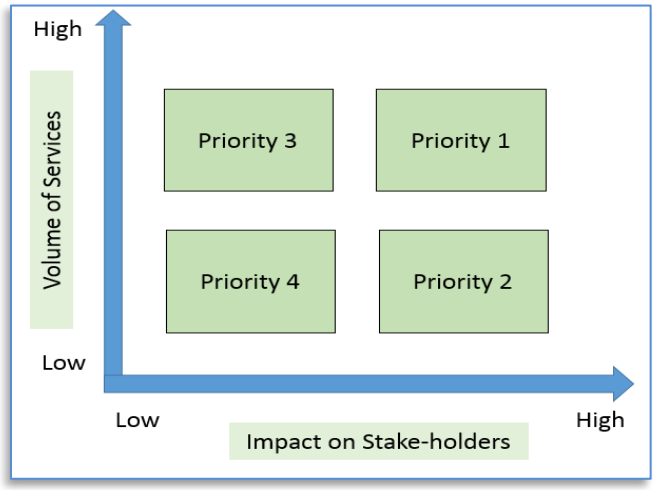


FIGURE 4.3: SERVICE PRIORITIZATION

Service Classification

Classification of Services on the basis of their amenability for reuse across agencies leads to cost-effectiveness and faster time-to-benefit. In actual practice, no two services of the legacy systems are identical. They perform at least slightly different function. However, it is necessary to group the services on 'approximate similarity' and then identify the sets of services which can be replaced by a single service, based on the greatest common requirements of the older services being replaced.

The Classification of Services basing on degree of reuse is listed below:

a. **Core Services:** These services are usually commodity by nature and are used by all the line-departments of the government. They are domain-agnostic. Examples are e-mail services and messaging services.
b. **Common Services:** These services are usually governed by the same pan-Government rules and regulations and used in the same manner by all the departments. Examples are HR, Finance, e-Procurement.
c. **Group Services:** These services are provided by a group of departments but not all. They perform comparable functions, most usually providing similar benefit/ service to different stakeholder groups/ communities. Examples are social benefits, economic assistance services, and educational services.
d. **Department Services:** These are department specific services which are provided/ utilized by one and only one department.

Service Integration

One of the aspirational goals of IndEA is to enable establishing **ONE Government**. This is to be achieved through the two ways described below, in addition to the other methods described in the IndEA framework.

a. **Integrated Services**: An Integrated Services is the single service engineered by unifying multiple services, which are often sequential and inter-related. The end-user need not access multiple outlets and channels for achieving the desired objective fulfilled by an integrated service.
b. **Cross-cutting Services:** Cross-cutting Services are services which are designed such that a single workflow cuts across multiple departments and providing the end result to the customer as a final response. Many real-life scenarios of businesses, and some times of the citizens, require the approvals of multiple departments - often in a sequential manner, leading to delay and the tedium of having to access multiple touch points of Government. Designing a cross-cutting service would greatly enhance the customer experience.

Other Attributes of Service

Service Type: Service Type is a categorization basing on the interface between the Government and the customer. The different types of Services provided by the government are:

- Government to Citizens (G2C)
- Government to Business (G2B)
- Government to Government (G2G)
- Government to Employee (G2E)

Service Priority

- Service Priority is the degree of sensitivity and/ or importance attached to the delivery of a Service. It is usually denoted as **High, Medium and Low**.

Service Level

- Service Level is the **timeline** within which a service has to be delivered by the agency responsible for it. Government departments publish Citizen Charters to notify the service levels to which they are committed. They also sign Service Level Agreements with the private service providers to back up their commitment to the customers.

Service Definition

Service Definition is one of the important components of BRM depicted in **Figure 4.2**. It seeks to capture all the attributes of a Service included in the Service catalog. The template shown in **Figure 4.4** provides a uniform basis for defining the services in terms of their attributes. The template is extended 'upward' to trace the origin of the Service to the **original goal**.

Goal
By 2030, ensure that all girls and boys complete free, equitable and quality primary and secondary education leading to relevant and effective learning outcomes (*Source- UN SDG No 4: Target 4.1*)
Sector
Education

Department/ Responsibility Commissioner of School Education								
Service	**Service Objective**	**Service Type**	**Service Priority**	**SLA**	**Service Provider**	**Beneficiary**	**Channel of Delivery**	**KPI**
Enrolment of students to schools	To enable the field officials to identify the target child and help the parents to enroll their child *online* in the eligible school.	G2C	High	Identification of target children in a village within **5 minutes**; Online Enrolment process to be completed in **15 minutes**.	Education Department	Student	Web/ Mobile/ Service Centers	• % increase annually in the gross enrolment of boys • % increase annually in the in the gross enrolment of girls

FIGURE 4.4: TEMPLATE FOR SERVICE DEFINITION

All the identified Services shall be defined in a similar manner and a Service Portfolio generated by grouping the services appropriately using the **service classification method** described earlier.

4.7. BRM and Other Reference Models of IndEA

The relation between BRM and other Reference Models is depicted in the Figure 4.5.

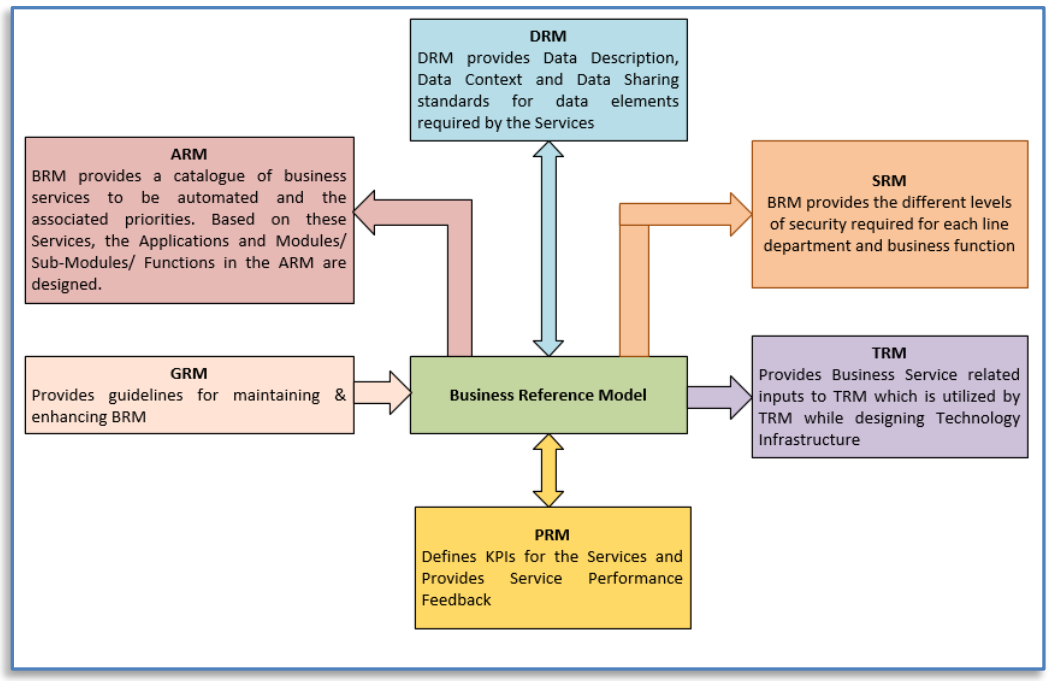


FIGURE 4.5: BRM AND OTHER REFERENCE MODELS

BRM and ARM

Figure 4.6 depicts the relationship between BRM and ARM.

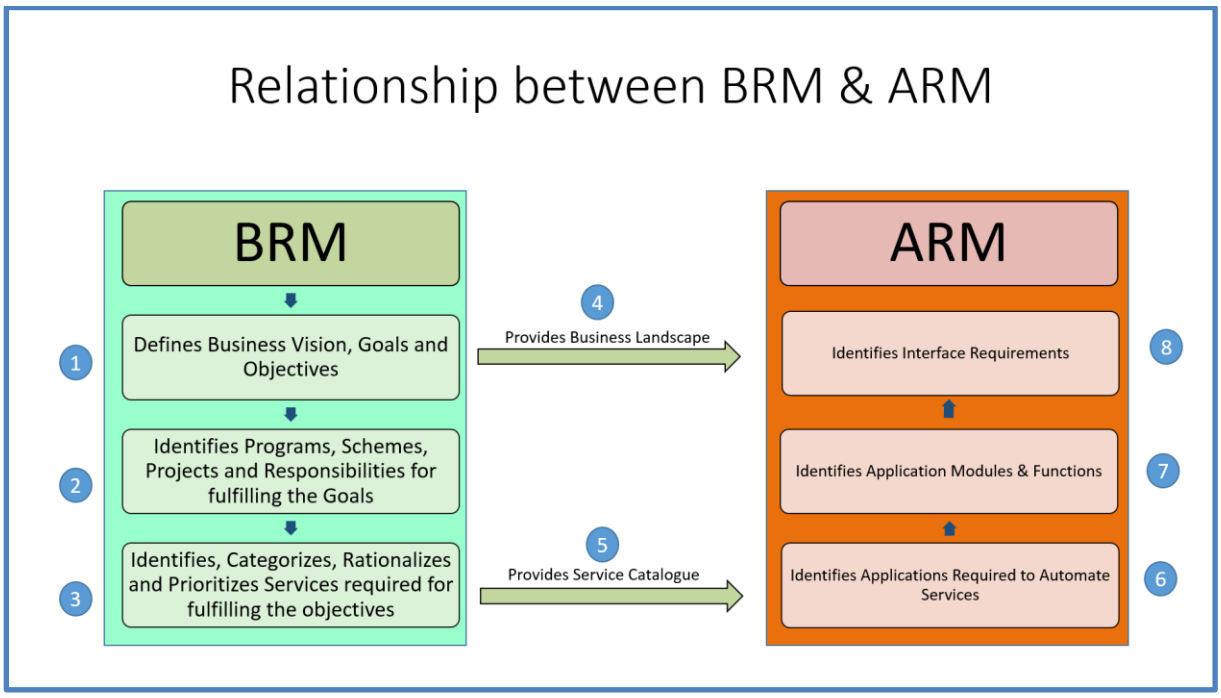


FIGURE 4.6: BRM AND ARM

Four important concepts useful in the context of BRM are described in the remaining part of this Chapter. These are:

(1) The **Business Landscape of IndEA** (useful for defining the Scope of the IndEA initiative)

(2) Business Process Re-engineering or **BPR** (useful in Service Transformation for creating **a better Government**)

(3) **Game Changers and Quick-wins** (required to create and sustain the **interest** of the sponsors of IndEA as also the stakeholders)

(4) **ONE Government**

4.8. Business Landscape of IndEA

The Business Landscape of any Government is vast, with myriad functions to be performed and a large number of services to be delivered. One of the initial steps of an EA initiative is to define its Scope so that it is manageable within the resources available and within a reasonable time. Prioritization is the key. With a view to

identify the boundaries of the IndEA Business Landscape, the earlier experiences in the area of EA in India and the information available on the website of Niti Aayog have been studied. An illustrative scope has been arrived at. This is represented in the **Figure 4.7**.

The IndEA Business Landscape consists of **16 vertical domains and 12 horizontal functions**, which, together, would represent majority of the activities of a *State Government* and its interactions with the citizens and businesses.

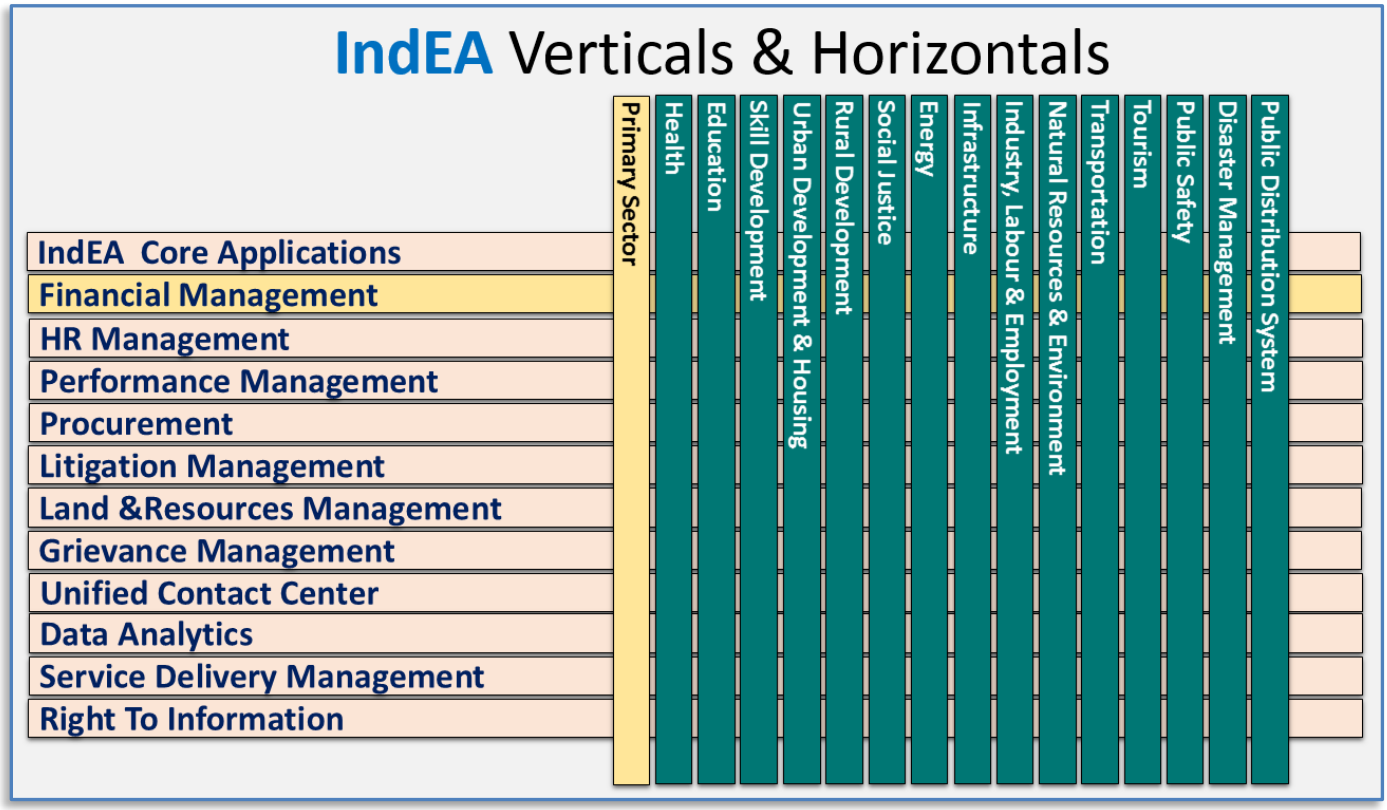


FIGURE 4.7: BUSINESS LANDSCAPE OF INDEA

The following guidance is provided in respect of the Business Landscape:

1. **Figure 4.7** is illustrative and provides a useful framework for depicting the Big Picture of the major functions of a State Government. It can be suitably modified by any State intending to implement the IndEA framework.
2. The *framework* used in Figure 4.7 for depicting Landscape can be applied to any Ministry of the Central Government, a Local Government or a Large PSU, to identify and depict the scope in terms of prioritized verticals and horizontal in its domain.
3. The foregoing model represents the master set of domains and functions. It is always better to define the scope to be more manageable, **by limiting the initial phase of the initiative to less than 10 Verticals and 6 horizontals.**

4. Each Vertical may itself be a large domain consisting of several functions, services and programs administered by several departments. Similarly, each Horizontal may consist of several functional modules. It is necessary drill down each vertical and horizontal to see the Big Picture. Such an exercise would also give an opportunity to identify the common functionalities/ services within and across verticals and horizontals and optimize the effort as also plan for the interoperability of different applications. One Vertical (Primary Sector) and one Horizontal (Financial Management) highlighted with yellow fill in **Figure 4.7** are drilled down to the next logical level to illustrate this point. The results are shown in **Figures 4.8 and 4.9 respectively**.
5. The effort made in creating the Business Landscape of the enterprise benefits in two ways – it enables defining the scope of the EA initiative, and it provides important inputs to the design of the Enterprise Application Architecture, following the **IndEA ARM**.

Primary Sector Vertical drilled down

An indicative drill-down of the primary sector represented in **Figure 4.8** shows that it has at least **10 sub-verticals** (each administered by a separate department / agency) and 8 functional areas (each supported by possibly by an application module). There could thus be up to 80 modules, derived basically from 8 common modules, thus drastically cutting the development and maintenance effort – by 72 modules. When we extrapolate the same across the entire Landscape, the saving could be well over a thousand modules.

Design of the Business Landscape provides a granular view of the Enterprise and enables the sponsors to get a view of the breadth of the Service canvas. It also an opportunity to Enterprise Architect to optimize its operations taking a holistic view of the entire Enterprise.

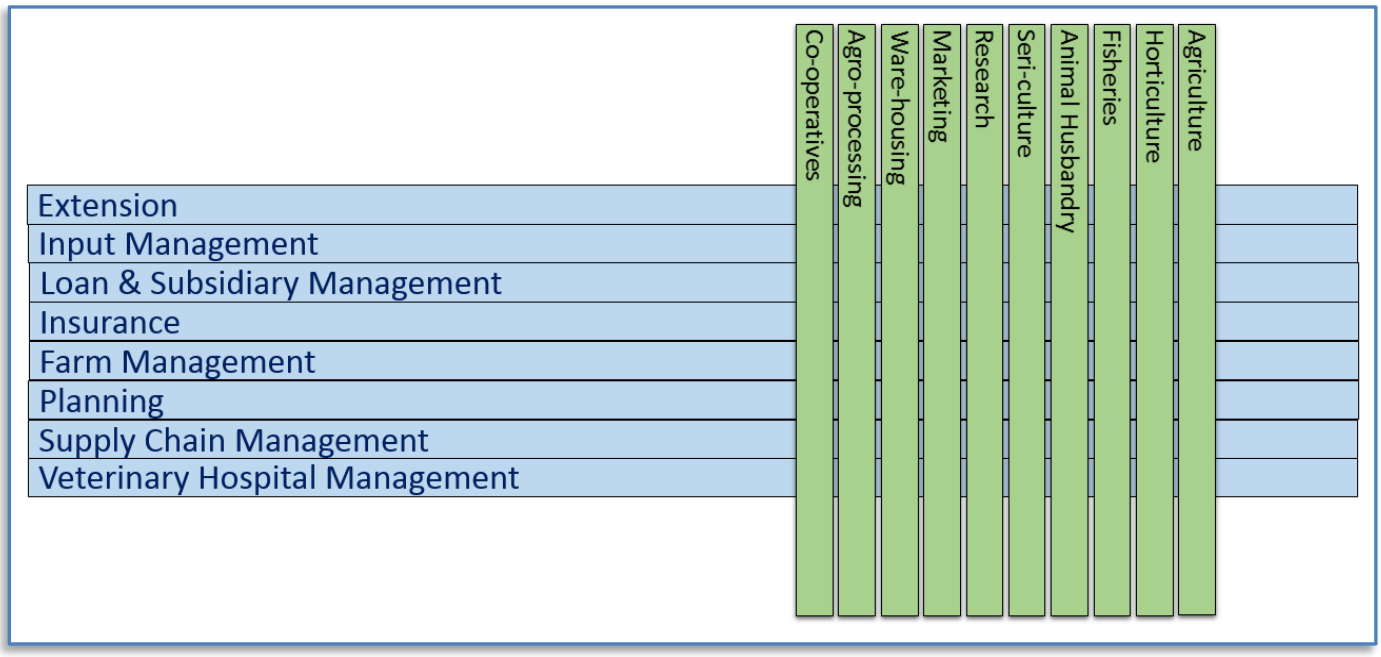


FIGURE 4.8: SUB-SECTORS AND FUNCTIONS OF PRIMARY SECTOR

Financial Management (Horizontal) drilled down

The functional modules of Financial Management are depicted in the **Figure 4.9** below:

Budgeting and Planning
Taxation
Financial Statement
Financial Policy Implementation Guidelines
General Ledger
Accounts Payable
Accounts Receivable
Expense Management
Financial Audit
Portfolio Management
Assessment of PPP Projects
Loans/ Subsidies/ Financial Schemes

FIGURE 4.9: MODULES OF THE FINANCIAL MANAGEMENT HORIZONTAL

4.9. Business Process Re-Engineering

Business Process Re-engineering or BPR '*is the fundamental rethinking and radical redesign of business processes to achieve dramatic improvements in critical measures of performance such as cost, quality, service and speed*'. The following are the basic principles of BPR

a. Organize around **outcomes**, not tasks.

b. Identify all the processes in an organization and **prioritize** them in order of redesign urgency.

c. **Integrate** information processing work into the real work that produces the information.

d. Treat geographically dispersed resources as though they were centralized.

e. **Link** parallel activities in the workflow instead of just integrating their results.

f. Put the **decision point** where the work is performed, and build control into the process.

g. Capture information **once and at the source**.

The IndEA framework, which aims to transform the domain of Governance, recognizes the critical role of BPR, both at the design stage and the implementation stage of any EA initiative.

4.10. Approach to ONE Government

The professed vision of IndEA is to enable the establishment of ONE Government, introduced as a concept in Section 4.2. The benefits envisaged of ONE Government are many, summed up as a virtual one-stop-shop for all the interactions of stakeholders with the Government. While a Whole-of-Government Portal would be a necessary first step in the movement towards ONE Government, it is not sufficient. Behind the simplicity presented by an enterprise portal lie several complexities and divisions necessitated due to the fragmented views created through the 'departmental silos'. The very representation of the Business Landscape of IndEA as applied to a State, shown in **Figure 4.8** is nothing but a number of 'stovepipes' arranged according to a pattern. It is against this background that a fundamental re-thinking of governance is called for.

The powerful concept of 'virtualization' has made a huge difference to the technological developments, leading to the creation of a host of technologies for virtualization of a variety of capabilities like the servers, storage, networks, databases and desktops. The goal of virtualization is to centralize administrative tasks while improving scalability and overall utilization of resources.

It is necessary to apply the principles and technologies behind virtualization of hardware and IT systems to the structures of governance, so as to derive very similar benefits to the efficiency, effectiveness and resource utilization across government. Virtualization of Departments is only a concept at this stage. It is necessary to undertake an extensive further research into this area, leveraging the principles behind the virtualization technologies that exist today in the digital world and applying them to brick-and-mortar organizations.

In the context of ONE Government, the following suggestions are provided for the consideration of the Enterprise Architects, embarking on an EA initiative:

1. **Services** may be redesigned taking a whole-of-government view, disregarding the departmental barriers. Common, integrated and multipurpose forms may be designed in a similar manner.
2. **Information Systems** may be designed taking the Government as a single enterprise or a group of sectors, again disregarding the departmental boundaries.
3. **Virtual institutions** may be created to take decisions that, in the normal course, would have to go through multiple agencies.
4. **Decouple processes and services**, such that a process may be used by multiple processes and a service may depend on multiple processes. Principles of orchestration and choreography will have to be used for achieving desired results more efficiently, despite and on account of such decoupling.
5. **Decouple processes and departments**, such that a process may be used by multiple departments and a department may use multiple processes.
6. A **Public Service Lake** may be created, which enables slicing and dicing of services to meet the needs of a life-cycle approach or event-driven approach to the availing of public services by the citizens.
7. Cadres of multipurpose case workers may be developed so as to optimize the utilization of human resources at the field level.

5. Data Reference Model

Data reference Model (DRM) provides a mechanism for the departments at various levels of Government to identify, discover, describe, manage, protect, and share the data it has and reuse information consistently within and across agencies and their business partners. It is expected that the departments/agencies would use the reference model to achieve a consistent and holistic view of data across the complex Government rather than a department or agency specific view. The DRM is also expected to provide guidance to Enterprise/Solution Architects to ensure and enable data sharing and standards compliance in e-Governance solutions so that data is uniformly and consistently defined and shared across all levels of Government.

Using this reference model, the data architects can arrive at a comprehensive Data Architecture for their department. The data architecture provides the structure and description of the department's data (metadata), the logical data model (depicting the relationship between various data elements), taxonomy, the security associated with each data element and sharing methodology.

Data Reference Model (DRM) *provides a means for departments to consistently define data in their data architecture. It will ensure sharing of information among departments and external agencies thereby providing opportunities for improved efficiency and effectiveness in Governance. DRM facilitates increased collaboration among departments/agencies and reduce the number of incompatible systems thereby contributing to Government-wide interoperability. It ensures that special attention is given to security and technical requirements of individual data elements so that they are implemented appropriately.*

5.1. DRM Objectives

The objectives of DRM are:

a. Improving the discovery, access and sharing of data among both internal (departments) as well as external stakeholders (citizens, businesses and developers)
b. Minimizing the duplicative efforts by capturing the data only once in the system, capturing only the incremental data as and when required in the business process and auto-populating of the existing data, with due validations as required.
c. Ensuring the accountability for the quality, consistency and and security of data through the institution of Data Stewards.
d. Developing shared vocabularies for ensuring common understanding of data
e. Facilitating collaboration among departments at all levels of the Government
f. Reducing cost and impact on citizens and businesses because of redundant collection of citizen and/or business data
g. Identifying the security requirements of different data assets
h. Identifying special technical requirements of different data assets
i. Ensuring that notified standards are adopted so that interoperability among applications is ensured

5.2. DRM Concepts & Definitions

Concepts:

a. **Digital Data Resource:** A Digital Data Resource is a digital container of information. A Digital Data Resource may correspond to three types of data: "Structured Data Resource", "Semi-Structured Data Resource", and "Unstructured Data Resource". It acts as a container for the metadata about the data resource.
b. **Structured Data Resource:** Structured Data Resource is a type of Digital Data Resource containing only structured data. A Database Schema is used to define/describe a Structured Data Resource.
c. **Semi-Structured Data Resource:** A Semi-Structured Data Resource is a Digital Data Resource containing semi-structured data. A Semi-Structured Data Resource contains partly structured and partly unstructured data.
d. **Un-structured Data Resource:** An Unstructured Data Resource is a type of Digital Data Resource that contains only unstructured data. Unstructured data is collection of data values that are likely to be processed only by specialized application programs.
e. **Document:** A Document is a file containing Unstructured and/or Semi-Structured Data Resources.
f. **Taxonomy:** Taxonomy is a collection of controlled vocabulary terms organized into a hierarchical structure. Each term in taxonomy is a topic. Taxonomy provides a means for categorizing or classifying information in a domain of discourse (invariably a department in the Government). Each term/topic in taxonomy is related to one or other terms/topics in the taxonomy in a parent child relationship.
g. **Topic:** Topic is a category within Taxonomy. A Topic is the central concept for applying context to data. For example, a department may have a Taxonomy that represents their organizational structure. In such Taxonomy, each role in the organizational structure represents a Topic. Topic in taxonomy may be in a parent-child relationship with other topics in the taxonomy. Every data asset can be categorized under a topic in the taxonomy. Taxonomies can also be used to categorize the Digital Data Resources, queries etc.
h. **Data Asset:** Data Asset is a managed container for data. In many cases, this will be a relational database; however, a Data Asset may also be a Web site, a document repository, directory or data service. For example: A document that is stored and managed within a data asset (such as a document repository) has management context provided for it through the metadata that is associated with that document within the document repository.
i. **Data Steward:** A Data Steward is a person responsible for managing a Data Asset. Ideally, it should be a person belonging to the department which manages the data asset.
j. **Supplier:** A person or organization that supplies data to a consumer. The supplier produces the exchange package.
k. **Consumer:** A person or organization that consumes the data that is supplied by the supplier.
l. **Exchange Package:** An exchange Package contains metadata about the data being exchanged such as supplier id, validity period of data etc. along with reference to the message content that is being exchanged.
m. **Data Payload:** Payload is the actual data that is transmitted in a Packet. The payload does not include any headers or metadata sent solely to facilitate Packet delivery.

Definitions:

a. **Database Schema:** Database Schema is a representation of metadata in the form of logical data models or conceptual data models. A Database Schema usually defines the entities, attributes, tables, fields, relationships, views, indexes, packages, procedures, functions, queues, triggers, types, sequences, materialized views, synonyms, database links, directories, XML schemas, and other elements.. These concepts primarily relate to the representation of structured data. A Database Schema provides a means to describe the data independent of the values of the data that it describes.
b. **Entity:** An Entity is an abstraction for a person, place, object, event, or concept described (or characterized) by common Attributes. For example, "Employee" and "Department" are Entities. An instance of an Entity represents one particular occurrence of the Entity, such as a specific employee or a specific department. An entity has one or more attributes. An entity may have relationships with one or more entities.
c. **Attribute:** An Attribute is a property or characteristic of an Entity. Different instances of an entity may have different values for an attribute. For e.g., "Name" may be an attribute of the entity "Employee". Two employees may have different values for the "Name" attribute. Every attribute has an associated data type which defines the values the attribute can hold.
d. **Data Type:** A Data Type defines the type of data an attribute may hold. For e.g. String, integer etc.
e. **Relationship:** A Relationship describes the relationship between two Entities.

5.3. DRM Principles

Principle DRM 1: Data Asset
Data is an asset that has a specific and measurable value to the Government and is managed accordingly

Archive and preserve all information (both in raw and aggregated form) exchanged, especially outside the government ecosystem, for future reference and if needed, for resolution of disputes. The Archival and preservation must be in accordance with the applicable regulatory requirements.

Principle DRM 2: Data-sharing
Data is shared across the Government, subject to rights and privileges, so as to prevent creation and maintenance of duplicative sets of data by different agencies. Data Sharing shall be subject to conformance with the principles of Security & Privacy.

Principle DRM 3: Data Trustee
Each dataset has a trustee accountable for data quality and security.

Principle DRM 4: Data Security
Data is protected from loss, unauthorized use and corruption, through adoption of international standards and best practices, duly protecting the privacy of personal data and confidentiality of sensitive data.

Principle DRM 5: Common Vocabulary and Data Definitions
Data is defined consistently throughout all levels of Government, and the definitions are understandable and available to all users.

5.4. DRM Schematic

The IndEA Data Reference Model provides a standard framework for describing the data identified by the department, its context, mode of sharing and data modeling so that a meaningful and usable Data Architecture can be developed by the departments.

The DRM framework focuses on 3 areas related to data architecture. These are:

A. **Data Description**
B. **Data Context**
C. **Data Sharing**

The DRM provides an implementation roadmap on each of these areas which may be used by the enterprise/solution/data architects who are supporting the department in building an effective Data Architecture. Each of the three areas is briefly described below:

A. Data Description

This area focuses on the semantics and syntactic structure of the identified data assets. Un-ambiguous description of data in terms of its semantics and structure will ensure appropriate usage of the data by the department as well as its external stakeholders such as other departments, citizens, businesses and application developers. Data description in terms of its metadata (data about data) is of great help in harmonizing the data description vis-à-vis other data assets and can be effectively used to respond to various questions related to metadata of the data asset. Design of a database schema is an important step in this area.

B. Data Context

In this area, the concerned department should answer the following questions about the various data assets it manages as part of its governance activity:

- What data assets does the department need?
- Who is the steward for the various data assets identified by the department? The steward for a data asset could be the department itself or it may be vested with some other department.
- How does the data relate to the Business Architecture? (Which business process/service will manage/use the data?)
- Under what category (of Government taxonomy) will the data asset be categorized?

Data context is very useful in discovering data.

C. Data Sharing

The Data Sharing area provides a framework for defining how the data can be accessed and exchanged. Data access refers to queries and data exchange refers to exchange of data between different departments/businesses etc. The effectiveness of data sharing is enabled and rendered more meaningful by data context and data description.

The three areas and their interdependencies are shown in **Figure 5.1.**

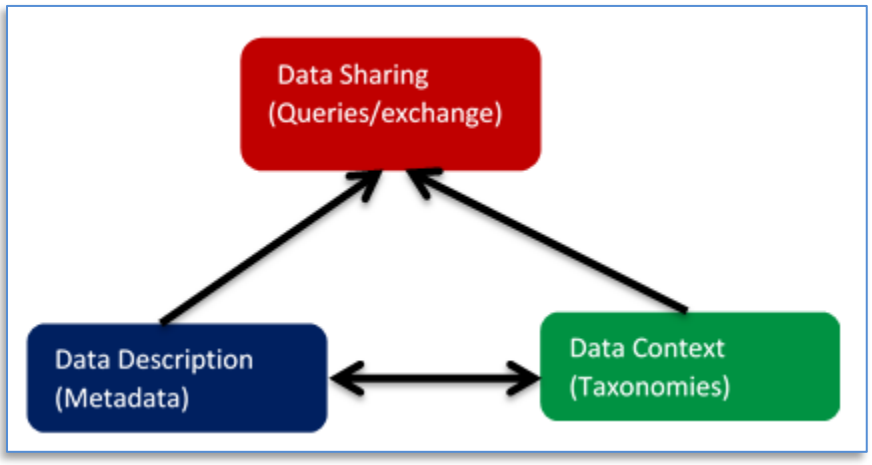


FIGURE 5.1: DRM AREAS AND THEIR INTERLINKAGES

DRM Abstract Model

Each area of the DRM should be expressed in terms of certain concepts and their relationships. These concepts and their inter-relations constitute the **DRM Abstract Model**. The DRM will provide the necessary guidance to the departments to define their data architecture in a comprehensive and complete manner so that all aspects of data are optimally covered thus enabling data discovery, interoperability and sharing. **Figure 5.2** presents the DRM abstract model. It depicts the major concepts from each area and the relationship between them. Concepts are expressed as boxes and relationships as arrows. Subsequent sections describe each area in more detail in terms of the concepts associated with that area.

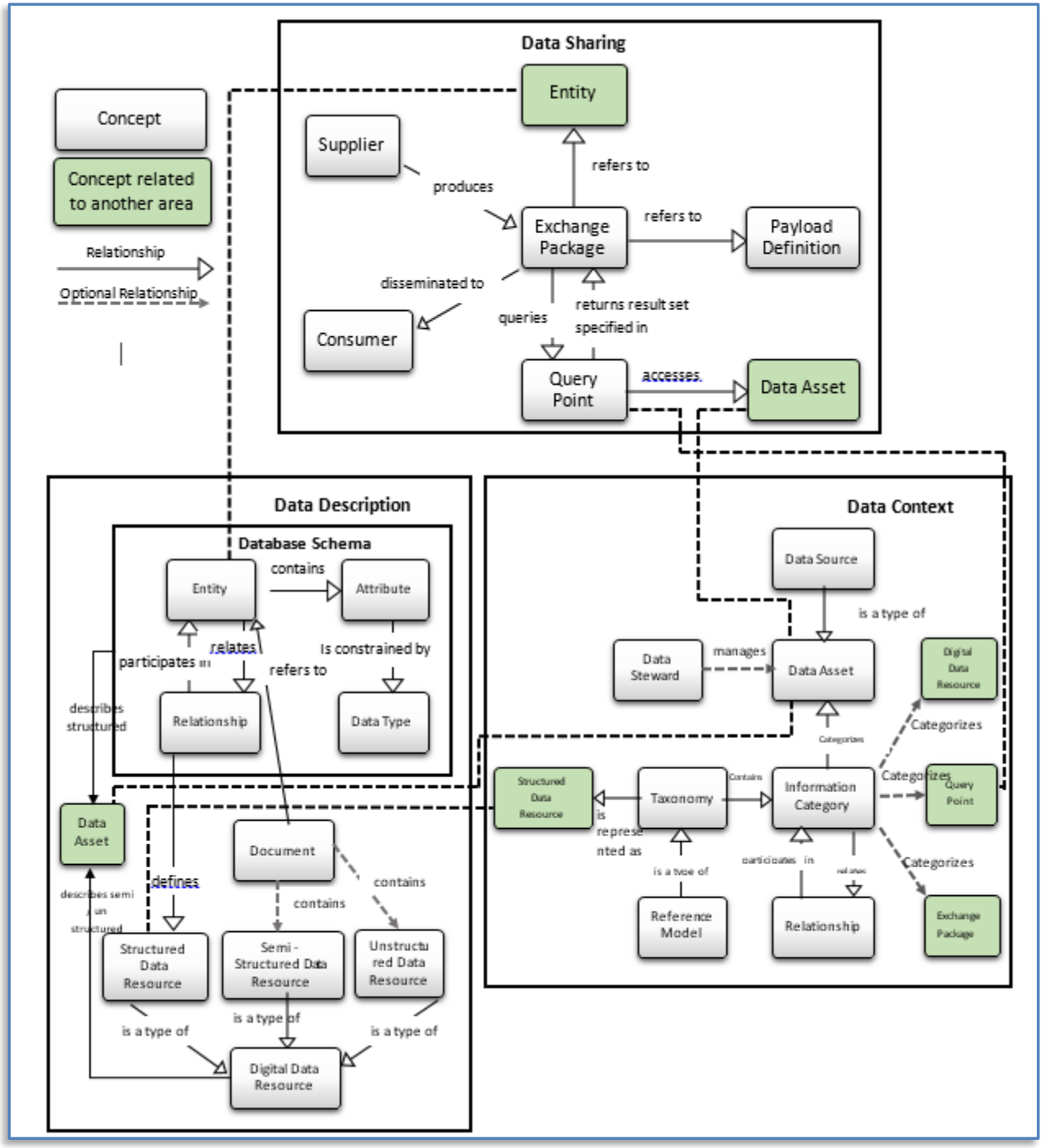


FIGURE 5.2: DRM ABSTRACT MODEL

Data Description Abstract Model

The Data Description area focuses on providing an unambiguous understanding of the data in terms of structure (syntax) and meaning (semantics). Correct and uniform description of data enables the following capabilities in government:

- **Data Discovery** – It enables a department to quickly and accurately identify the data required to fulfill its governance objectives (through functions and services). The data may be owned by the department itself or by another department in any level of Government. Data discovery is further strengthened by the categorization, search and query capabilities provided by other areas.
- **Data Sharing and Reuse** – The ability to discover data (who is generating/managing what data) and a clear understanding of its meaning ensures that the data can be easily shared and reused in many activities both within and outside the department.
- **Data Harmonization** – A uniform way of describing the data through a well-defined model enables different departments to compare the data assets and helps in harmonizing the syntax and semantics of the data assets; a useful outcome of this would be the creation of common entities which can be used across departments.

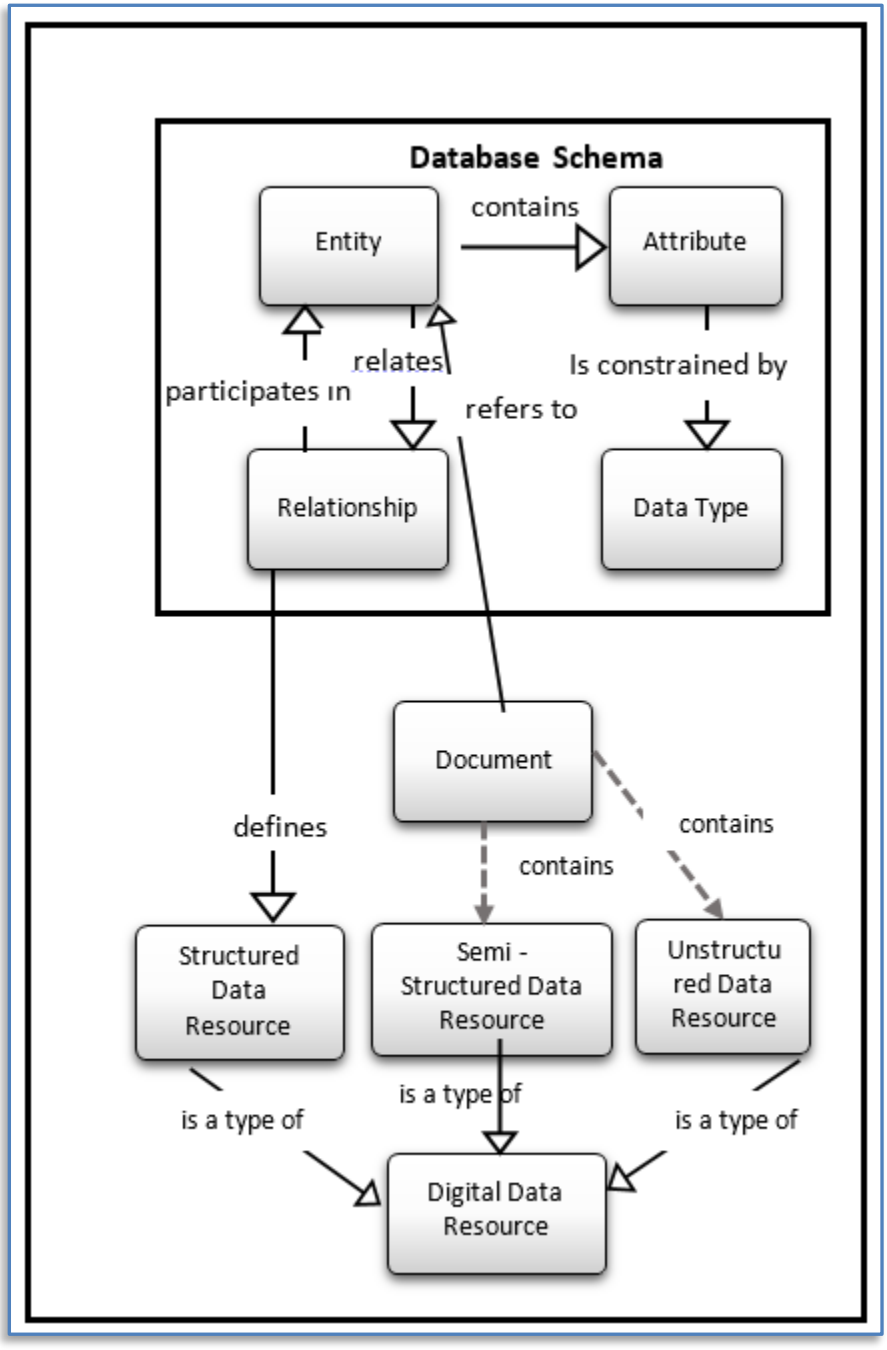


FIGURE 5.3: ABSTRACT MODEL OF DATA DESCRIPTION

The abstract model of Data Description essentially depicts the concepts that will be used to describe the Data Description area and their relationships. Two aspects of data description that are needed to be captured are:

- The metadata (data about data) and
- The mechanism for storing the metadata.

Sections below detail the Metadata and Data Standards.

Any data asset can be classified as structured, semi-structured or un-structured. Semi-structured or un-structured data would include textual material, multi-media files etc. The metadata should accordingly be captured along these two dimensions:

- As logical data models for describing structured data and
- As Digital Data Resource metadata for describing semi-structured and un-structured data (using standards such as Dublin Core Meta Data Standard)

The structured data would invariably be implemented in the Data Architecture as Entity – Relationship diagram. The Digital Data Resource would be captured as metadata records.

Data Context Abstract Model

Data context is any information that provides additional meaning to the data in terms of nature of data (category), the organization which is responsible for creating/managing the data, which business process created the data etc. The data context along with the data description makes it possible for a potential consumer of data to discover the data (if such a data discovery service is available) and understand the context in which the data was created so that a decision can be taken on whether the data is relevant for his/her purposes.

The Data Context provides important information to potential consumers of data so that they can take an informed decision on whether the data is appropriate to the specific context in which they wish to use it. It may be noted that the data context of a data asset should always be defined from the perspective of the owner (steward) department.

The abstract model of Data Context is given in **Figure 5.4**. It depicts the concepts that will be used to describe the Data Context and the inter-relations between the different concepts.

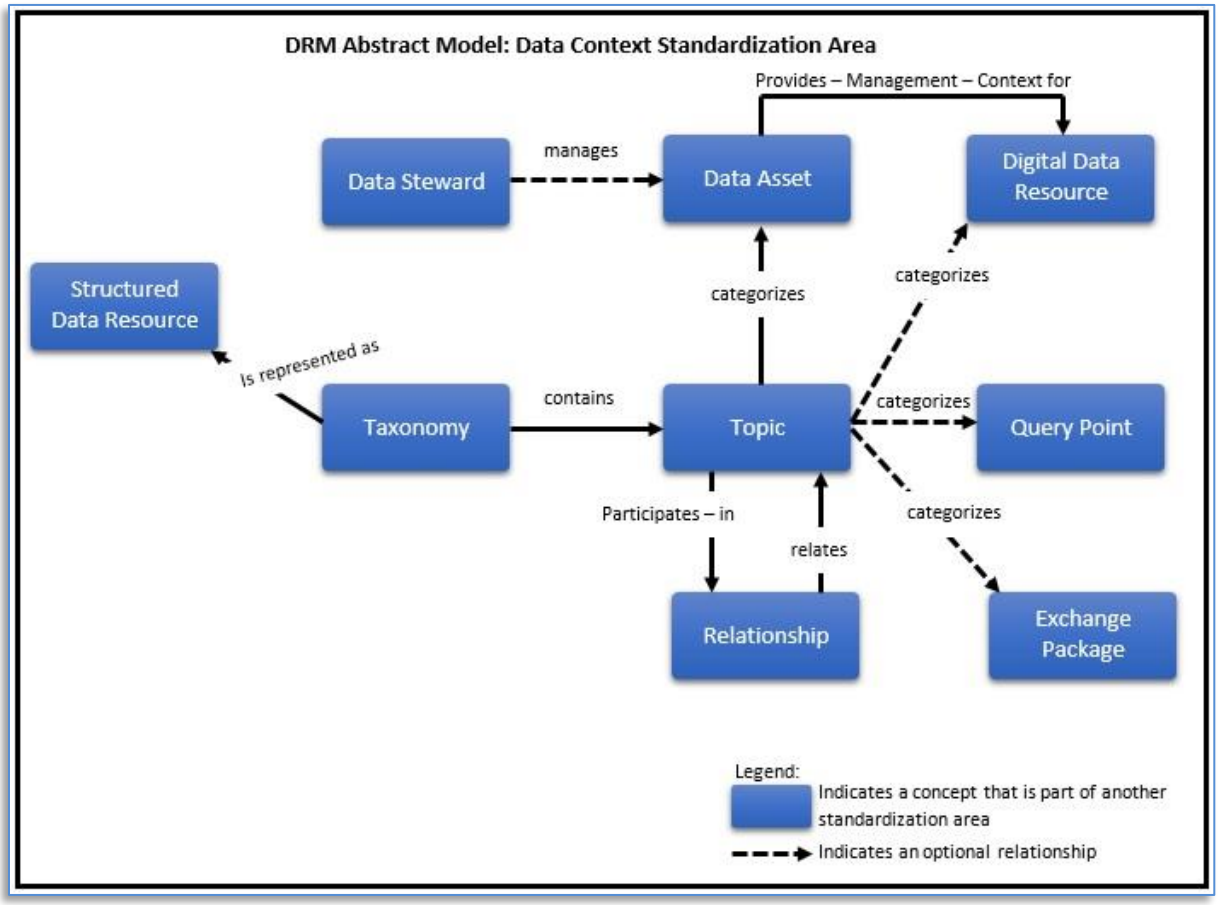


FIGURE 5.4: ABSTRACT MODEL OF DATA CONTEXT

Data Sharing Abstract Model

Data sharing is the use of information by one or more consumers that is produced by a source other than the consumer. Data sharing has two stakeholders: the data supplier/producer and the data consumer. The data supplier/producer should always be one but there could be one or more data consumers. The consumers of data produced by a Government department may be other divisions within the same department, other departments within Government and external stakeholders such as citizens, businesses, NGOs etc.

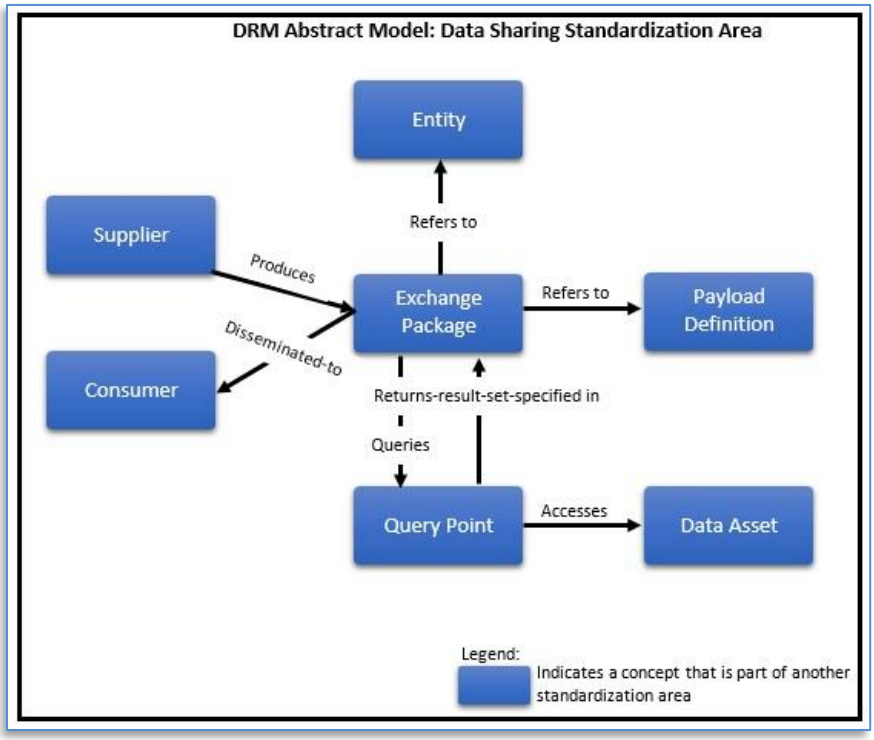


FIGURE 5.5: ABSTRACT MODEL OF DATA SHARING

Data sharing covers primarily two types of data sharing:

Data Exchange – These are invariably recurring transactions between two systems

Data Access – Data access refers to sharing of data, invariably with people through querying of data assets.

The data architect may use the data sharing section to organize and share information about what data is being shared, with whom and how.

5.5. Metadata and Data Standards

Data Standards are accepted ways of representation, format, definition, structuring, tagging, transmission, manipulation, and use of data. Data Standards enable reliable recording of information and are fundamental to efficient sharing and exchange of information. They provide the rules for structuring information. Metadata takes its importance once the Data Standards are in place. Metadata i.e. data about data defines and describes data or information. It is used to manage data, information and knowledge. Metadata is the structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource.

An integrated service in a typical e-Governance system would involve multiple domains, and deal with its various entities. Each of these entities is defined with the attributes called data elements. It is very important to define each of the data elements as an independent unit and provide it with a contextual definition. For achieving interoperability among domain applications, standardization of commonly accepted and context-based data definitions and metadata of various data elements becomes vital.

Table 5.1 below provides the list of various publications related to Policies and Standards on Data and the location from where the related documentation can be accessed.

Name of Publication	Purpose of the Publication	Published By	Published At
eGov Standards	Provide a platform for sharing of ideas, knowledge and draft documents among the members of various committees involved in Standards formulation process	Ministry of Electronics & Information Technology and Ministry of Communications & Information Technology, Government of India	http://egovstandards.gov.in
Local Government Directory	To make available Standard location codes with a mechanism for dynamic update of create / split / merger of villages/ blocks / districts / states and local governments (panchayats and municipalities)	Ministry of Panchayati Raj, Government of India under e-Panchayat Mission Mode Project (e-Panchayat MMP)	http://lgdirectory.gov.in
National Data Sharing and Accessibility Policy (NDSAP) – 2012	To make data available to public for access, for enabling rational debate, better decision-making and use in meeting civil society needs	Ministry of Science & Technology (Department of Science & Technology), Government of India	https://data.gov.in http://dst.gov.in
Open Data Element Framework (O-DEF),	To define Object-oriented classification of data elements	The Open Group	www.opengroup.org/bookstore

TABLE 5.1: PUBLICATIONS ON DATA STANDARDS AND DATA POLICIES

Some of the standards which have been notified in http://egovstandards.gov.in are listed below:

- Metadata and Data Standards – Demographic
- Digital Preservation Metadata and Schema
- Localization and Language Technology Standards
- Metadata and Data Standards for Rural Drinking Water and Sanitation
- Technical Standards for IFEG
- Standards and Specifications for e-Authentication
- Data Security Standards

Data Security

Data is a critical asset of the government and many data collected by the government as part of its operational processes require different levels of security and privacy to be maintained. The Information Technology Act as well as the Aadhaar Act stipulate processes to be followed with respect to data of citizens. In addition, there may be other data elements which need to be protected for various reasons including those of national security.

The nature of an attribute of a data entity determines the type of security practices to be followed at different levels in which the data is handled such as at the time of data capture, at the time of data transportation over the network, data storage, data sharing and data display in public or private domain. The security needs of each data attribute should be analyzed in all respects and the implementation strategy worked out based on the guidelines provided by Security Reference Model.

Special Technology Requirements

Sometimes certain data attributes may have special technical requirements. For e.g., in order to capture bio-metric data, a biometric device would be required; similarly, in order to capture Lat-Long, a mobile, DGPS (Differential GPS) or Electronic Total Station (ETS - GPS) device could be used based on the specific requirement in terms of accuracy etc. Such special requirements may be at the time of data capture, transportation over the network (NICNET, SWAN or Public network), storage (geographical restriction for e.g. Data center should be in India), viewing (bar code reader, card reader) etc. Such requirements should be identified and recorded so that using the guidelines provided in TRM, the technology architecture can be prepared.

5.6. Data Governance

Data Governance

The DRM defines how to arrive at the data architecture through Data Description, Data Context and Data Sharing. The question now arises as to how we can ***ensure*** that all departments describe their data architecture in this manner. In addition, there are many cross-cutting issues which need to be addressed so that the Government gets a complete, correct and unambiguous view of the data from across different departments and is able to take meaningful policy decisions. This is where Data Governance comes into picture.

Data Governance is a set of policies, processes and controls that ensure that key data is managed effectively throughout the Government/Enterprise. The Data Management Book of Knowledge (DMBOK) defines Data Governance as *the exercise of authority, control and shared decision making (planning, monitoring and enforcement) over the management of data assets*. Data Governance primarily deals with *ensuring that data is managed properly* as opposed to *managing the Data*. It is comparable with the function of auditing of financial assets. While accounting manages the financial assets, auditing ensures that it is managed as per defined policies and procedures. Similarly, while data management directly relates to managing data assets, data governance deals with laying down policies and procedures for data management and exercising control to ensure that the laid down policies and procedures are properly followed. This automatically implies that there should be a clear separation of responsibilities between the people who do data governance and the people who manage data.

Aspects of Data Governance

Data Governance covers all of the aspects of data as given in the DRM such as unambiguous data description, Data Stewardship and mechanisms for data sharing. In addition, it also covers certain cross-cutting themes such as Data Standardization & Master Data Management, and Metadata Repository. Each of these is described below:

a. **Data Standardization and Master Data Management** – Master Data refers to those commonly required data which are agreed upon and shared across the Government/Enterprise. It may be a reference data such as a list of values to be used for a data element such as sectors in Government. It may also be a master data that is a generated once and used by many applications such as the BPL Survey data. Master Data Management is critical to ensure that all applications use standard set of data and thus are able to interoperate with one another in a meaningful manner. It would be the responsibility of the Data Stewards to ensure that they don't maintain their own list of values or manage a copy of their own. Use of a standard definition and code for master data entities is absolutely necessary in order to enable interoperability among different eGovernance applications. The following table lists some of the master data entities which are likely to be used by almost all applications. Some of these master data entities are available as downloadable files while some are accessible as online services:

Sr. No.	Name of the Core Data Entity	Details of its availability
1.	Revenue Entities such as States, Districts, Divisions, Sub-districts, Sub-divisions, villages etc	Available as downloadable files in JSON as well as XML formats from Local Government Directory (http://lgdirectory.gov.in) Also available as online services from Local Government Directory (LGD) LGD has been recognized as the standard directory by the Cabinet Secretariat, Government of India for providing unique codes to revenue entities, panchayats, urban local governments and traditional local bodies
2.	Panchayats such as District Panchayat, Block/Intermediate Panchayat and Gram Panchayat	Available as downloadable files in JSON as well as XML formats from Local Government Directory (http://lgdirectory.gov.in) Also available as online services from Local Government Directory (LGD)
3.	Urban Local Bodies such as municipalities, Corporations, Cantonment boards etc.	Available as downloadable files in JSON as well as XML formats from Local Government Directory (http://lgdirectory.gov.in) Also available as online services from Local Government Directory (LGD)
4.	Blocks	Available as downloadable files in JSON as well as XML formats from Local Government Directory (http://lgdirectory.gov.in) Also available as online services from Local Government Directory (LGD)
5.	Traditional Local Bodies such as Autonomous District Councils, Village Development Councils etc	Available as downloadable files in JSON as well as XML formats from Local Government Directory (http://lgdirectory.gov.in) Also available as online services from Local Government Directory (LGD)
6.	Scheme/Programme	A scheme or a Programme of the Central or State Government. Currently there is no online directory which provides a standard list of schemes and unique codes for them. However, Direct Benefit Transfer Mission has taken the initiative to provide unique codes to schemes. DBT Mission may be asked to publish this as an online directory and make the list available as services. **As regards State Government schemes/programmes, each State Government should identify a nodal department which would give unique codes to schemes of the State Government.**

Sr. No.	Name of the Core Data Entity	Details of its availability
7.	Sectors and Sub-sectors	Every State Government has a set of sectors in which various activities are undertaken. Examples include health, education etc. **The sectors and sub-sectors should be identified and unique codes given to each of them.**
8.	PIN Code	PIN Code is given by the Department of posts, Government of India across the country. The list of pin codes along with the area covered by them (in terms of revenue entities as available in LGD) should be made available
9.	IFSC Code	The list of IFSC codes for RTGS can be obtained from http://rbidocs.rbi.org.in/rdocs/RTGS/DOCs/RTGEB0815.XLSX The list of IFSC codes for NEFT can be obtained from http://rbidocs.rbi.org.in/rdocs/content/docs/68774.xls
10.	Country Code	ISO 3166 is the International Standard for country codes. It can be accessed from the URL https://www.iso.org/obp/ui/#search/code/

TABLE 5.2: INDICATIVE LIST OF MASTER DATA ENTITIES

In addition to the above, Ministry of Electronics & Information Technology, Government of India has also put in place a mechanism to arrive at standards for various types of data. The details can be accessed from http://egovstandards.gov.in. The above table is an indicative list and is applicable to government organizations. In addition, there is a need to identify and adopt domain-specific data standards by the implementing organization.

b. **Metadata and Metadata Repository** – Metadata, usually defined as data about data, relates to the data definition given by the data steward. A metadata repository is a repository which holds the metadata relating to all entities used by the Government. A metadata repository is also sometimes referred to us a data dictionary. However, - In general, the term Data Dictionary is generally implemented as part of a DBMS and includes tables which give complete information about the database such as the tables, their properties, columns and their properties, view implemented, privileges and roles granted to users etc. Such a data dictionary is designed as part of the DBMS itself and is called an active data dictionary. An active data dictionary is used by the DBAs and developers to define and/or make changes to the database which then gets reflected in the database automatically. However, the data dictionary is invariably not available to the external users who wish to have information about the data as the database access is restricted to the DBAs/owners/developers only.

In view of the enterprise-wide requirement, in the context of Enterprise Architecture, a data dictionary takes on a new connotation and may be defined as a centralized **metadata repository** of information about various data entities and their data elements such as meaning, relationships to other data, origin, usage, format etc. As a metadata repository, it would generally be stored separately from the database. Any changes that are made to the data (in the database) will have to be reflected separately in the repository. Updation of the metadata repository should be defined as part of the overall Data Governance process. Such a data dictionary is generally called a passive data dictionary. **Every State should maintain a centralized metadata repository which can be viewed by all departments. Each department should be given privileges to update the data entities related to their domain while certain generic data entities may be managed by one nodal department** (which administers the metadata repository).

In addition to state-level metadata repository, a **national level repository** consisting of metadata related to national level data entities should also be maintained. Access to view the data definitions should be made available to all departments of all States. The data definition itself would be updated by the data trustee department as part of the Data Governance process.

Goals of a Data Governance Programme

The first step towards building an effective Data Governance Programme would be to clearly define the goals of the Programme. The goals should be compelling enough for the Government to see value in sustaining the programme. The following could be some of the goals of establishing a Data Governance Programme:

a. Enable effective policy decision-making through the use of quality data
b. Reduce or eliminate problems in integrating systems so that the Government is able to get an integrated view of its various programmes
c. Eliminate duplication of efforts in collecting the same data and promote use of the *Golden record*
d. Ensure accountability of data
e. Ensure and promote standardization of Master Data

The mark of a successful data governance programme would be that the programme is no longer needed as the policies and procedures have become integral to the day-to-day activities of data management.

Critical Success Factors

Critical Success Factors for ensuring a successful data governance programme include the following:

1. The need for data governance should be clearly understood by the Government
2. Government departments invariably do not own up the data and treat data and content management as the responsibility of the IT unit associated with the department. This should change.
3. Change management is a very important game changer of Data Governance. Cultural shift that is required within government should be taken into account and addressed appropriately. For e.g., almost every government department maintains its own list of districts. If standardization is adopted, it should be followed and enforced.
4. Data Governance is a continuous activity. It needs to be sustained till it practically becomes part of the overall government data management

It is very important to communicate the benefits of data governance to the top management in terms of concrete value to the government.

5.7. Empowering Government with Analytics

Data analytics is the process of deriving insights from datasets through the use of queries and data aggregation procedures. It may use simple tools to complex statistical algorithms to arrive at the insights. The focus of Data Analytics lies in inference, which is the process of deriving conclusions about the information the datasets may contain, invariably through the use of specialized systems and software.

Big Data refers to huge volumes of data which cannot be effectively processed using the traditional DBMS and tools. Database systems such as MongoDB, NoSQL etc. are invariably used to manage such data. Hadoop, MapReduce, Apache Hive, Apache Sparkopen are some of the tools available for processing Big Data.

The attributes and challenges of big data have been described in terms of "three Vs": volume, velocity, and variety. Volume is big data's primary attribute, as terabytes or even petabytes of it are generated by organizations in the course of its operations, while also complying with Government regulations. Velocity is the speed data is generated, delivered, and processed. Variety is that data comes in all forms: structured (traditional databases like SQL); semi-structured (with tags and markers but without formal structure like a database); and unstructured (unorganized data with no business intelligence behind it). The concept of big data has evolved to imply not only a vast amount of the data but also the process through which organizations derive value from it.

Data Visualization is an important aspect of data analytics. Data visualization enables a user to quickly detect patterns, trends and correlations which may go undetected in text-based data. It makes complex data more accessible, understandable and usable via statistical graphics, plots and information graphics.

Data analytic tools combined with excellent visualization tools provide a powerful platform to derive insights into the data.

Data Analytics in Government

There is no doubt that Government collects a large volume of data about the citizens, programmes, etc. Earlier, it was difficult to use this data to analyze and drive the future policies. But with the advent of Information and Communication Technologies, more and more processes of the government are becoming e-enabled which in turn is opening new opportunities for the Government to improve its performance. More and more governments across the globe are investing in Big Data analytics capabilities to improve government services and overall government functioning.

So far, government departments have been relying on reports to aid them in decision making. But analytics take the process of policy formulation and decision making to a whole new level by offering deep insights not only on past performance but also use it to predict the future behavior and trends.

With effective data governance, data across departments can be combined to get a unified view of the overall impact of the government.

5.8. DRM and Other Reference Models of IndEA

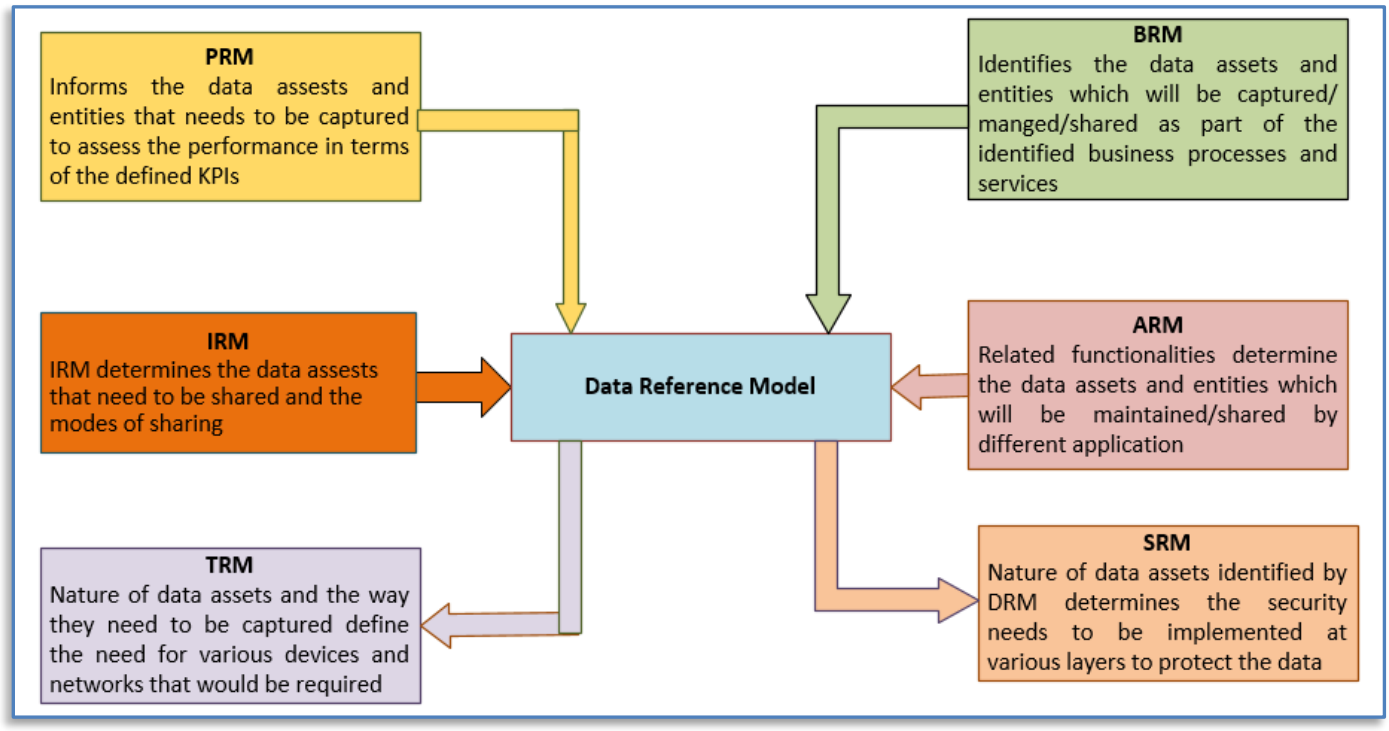


FIGURE 5.6: DRM AND OTHER REFERENCE MODELS

DRM and SRM:

The nature of an attribute of a data entity determines the type of security practices to be followed at different levels in which the data is handled such as at the time of data capture, at the time of data transportation over the network, data storage, data sharing and data display in public or private domain.

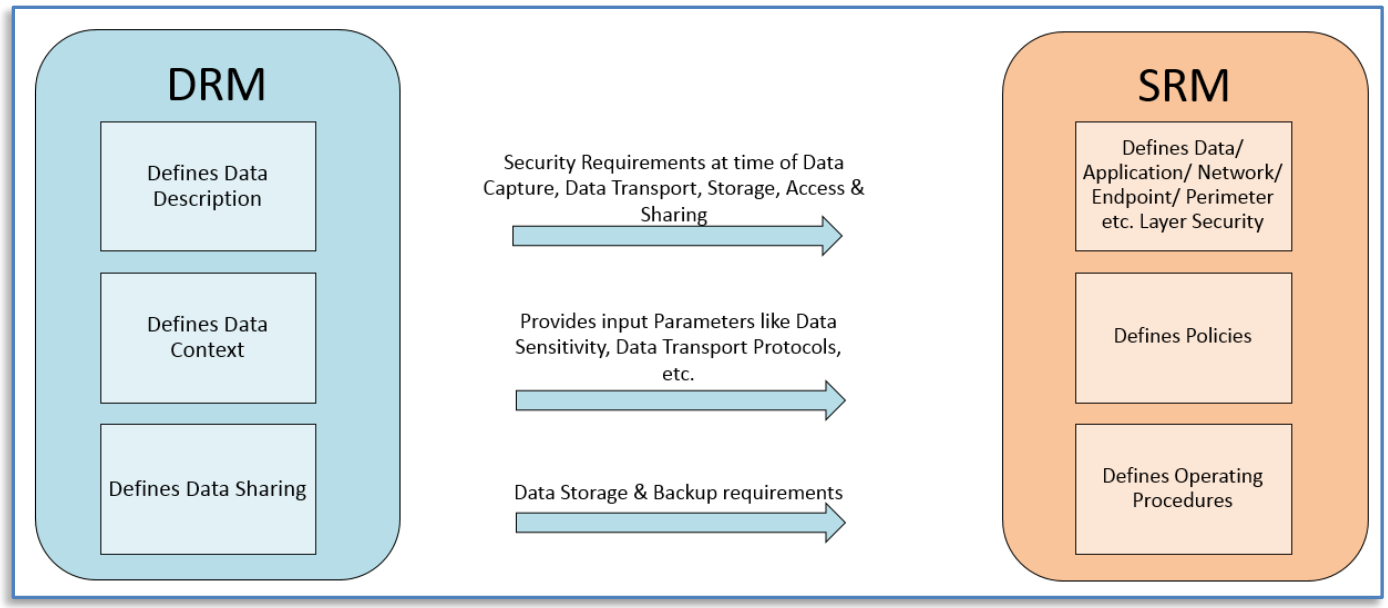


FIGURE 5.7: RELATIONSHIP BETWEEN DRM AND SRM

5.9. Developing Enterprise Data Architecture from DRM

The data requirements are always driven by the business architecture needs which in turn are driven by the vision of the department aligned with the vision of the Government. The initial step in designing the Data Architecture involves identifying data elements required and commonly agreed way to describe the data. The department(s) must adhere to the DRM principles mentioned in this chapter. Current data architecture should consist of identifying the core applications and systems and subject them to reverse engineering to identify the underlying data entities. In defining the target architecture, the DRM should be used to build meta-data standards, data definition, data sharing and data context. Data architecture analysis should also categorize certain common data across the government. These include data pertaining to people, businesses, land, things. They are candidates to be become "data hubs". Please refer to the chapter on '**Implementation Approach**' and '**IndEA Adoption Guide**' for further details.

6. Application Reference Model

Governments can provide better services to stakeholders by automating their *Services*. The Application Reference Model provides the foundation to automate these *Services*, which are identified as a part of the Business Reference Model. It enables the government to achieve its objective of better collaboration and data-sharing between & within departments thereby providing effective business services to its stakeholders.

IndEA promotes the adoption of **Federated Enterprise Architecture**. In a State Government, there are a set of data elements and processes which are common across all departments. Similarly, there are sets of data elements and processes which are department specific. The adoption of **Hybrid Pattern** of Federated Enterprise Architecture enables the State Governments to define Core/ Common/Group and Department Specific Data Elements, Process and Applications. The State Government also specifies data and integration standards, policies and guidelines which must be adhered by all applications. This ensures seamless interoperability amongst applications across departments. The grouping of applications enables sharing and re-use of applications which in-turn, provides cost-efficiency to the State Government. The Hybrid Pattern also provides individual departments with the option to procure/ develop applications which meet their department specific needs.

ARM encourages state governments to align their application landscape to '**IndiaStack**[2]'. IndiaStack is a set of APIs that allows governments, businesses, startups and developers to utilize a unique digital Infrastructure to solve India's hard problems in moving towards a towards presence-less, paperless, and cashless service delivery. IndiaStack has four layers viz. Presenceless Layer (through use of Aadhaar), Paperless Layer (through eSign and Digital Locker), Cashless Layer (through use of UPI) and Consent Layer. The application landscape of state governments must avail the APIs provided by IndiaStack for authentication, verification, payments, identity protection, and elimination of paper.

The IndEA ARM also provides guidelines on the Application Architecture Standards, use of Open APIs, Microservices Architecture and Open Source Software. It also specifies the Secure Coding Standards for Application Development.

Application Reference Model (ARM) *provides the framework for grouping similar applications to maximize re-use. To this end, a concentric layered ARM Meta-model is prescribed for IndEA. The inner-most layer of the 4 layers of ARM is the IndEA Core Platform, which provides the most generic services in a domain-agnostic, application-agnostic and technology-agnostic manner. The three layers around the IndEA Core relate to Common Applications, Group Applications and Domain-specific Applications.*

[2] https://indiastack.org

6.1. ARM Objectives

The Objectives of ARM are:

a. Acting as the bridge between the BRM and the TRM, by translating the services identified by BRM into applications and components to be implemented by using the TRM;
b. Mapping the commonality of functions of various domains and identifying the applications and components for re-use across Government or parts of Government;
c. Enabling government to provide effective and integrated services to its stakeholders through collaboration between & within departments;
d. Defining building blocks required to develop high-level Application Architecture;
e. Suggesting appropriate methods for software development.

6.2. ARM Concepts & Definitions

Concepts:

a. **Core Applications:** The Core Applications are the applications with domain-agnostic functionalities required by all the departments, and as such, maintained centrally and shared by all the departments.
b. **Common Applications:** The Common Applications are domain-agnostic but government-specific functionalities required and used by all departments. These are also built and maintained centrally.
c. **Group Applications:** Group Applications are the applications with functionalities required by several (but not all) departments, with marked similarity in their domain functions.
d. **Department Applications:** Department Specific Applications have functionality that is specific to a department.
e. **Brownfield Applications** are the software applications already functioning in the enterprise and providing services. They may be fit to be migrated to the target Enterprise Architecture with or without enhancements or need to be retired as they can't be so migrated despite significant effort.
f. **Greenfield Applications** are the software applications developed afresh to provide services not existing in the legacy system, so as to fulfill the entire portfolio of services envisioned in the Target Business Architecture.

Definitions:

a. **Work Products:** Artifacts produced during the Enterprise Architecture project
b. **Interoperability** is the ability of a system or a product to work with other systems or products without special effort on the part of the customer.
c. **Service-Oriented Architecture (SOA)** is a style of software design where services are provided to the other components by application components, through a communication protocol over a network, in a manner that is independent of vendor, product or technologies.
d. **Service or Business Service** in the context of the public-sector environment is the act of fulfilment of the request made by a citizen, business or employee, by following a set of defined processes and workflows.
e. **Web Service** (also used conterminously as *Service* in the literature on system architecture) is a software functionality that provides a mechanism to enable access to one or more capabilities of the system, where the access is provided to the *consumer of the service* using a prescribed interface and is exercised consistent with constraints and policies as specified by the *provider of the service* through a service description.

f. **Application Program Interface or API** is a *code* that allows two software programs to communicate with each other and consists of two aspects – the **specification** (that describes how information is exchanged between programs, done in the form of a request for processing and a return of the necessary data) and a **software interface** written to that specification and published for use.

6.3. ARM Principles

Principle ARM 1: Ease of Use
Applications are easy to use, with the underlying technologies being transparent to the users.

Principle ARM 2: Sharing & Reusability
All commonly used Applications are abstracted to be built once and deployed across the Whole-of-Government through reuse and sharing. Sharing & Reusability shall be subject to conformance with the principles of Security & Privacy.

Principle ARM 3: Technology Independence
Application Design is open standards-based and technology-independent.

Principle ARM 4: Application Security
Applications are secure by design and developed using secure coding standards and practices.

6.4. ARM Schematic

The ARM provides building blocks to design Applications/ Modules/ Sub-Modules/ Functions. It provides templates for various '*Work Products*' which are fundamental to developing Application Architecture. ARM is depicted in **Figure 6.1**.

The State's Enterprise Architecture will comprise of existing applications that have to be upgraded/ maintained/ phased-out along with applications that have to be additionally developed. ARM provides a structure to group all such applications based on their Type/ Capability, etc. and to categorize them based on their Priority/ Service Category, etc. The Applications are selected and prioritized based on the **'*Business Services*'** that need to be automated to meet requirements set by the BRM.

Applications can be deployed in multiple methods based on the Application Type, Category, etc. ARM provides building blocks to capture the deployment parameters. These parameters are utilized by the Technology Reference Model to further design the Technology Architecture.

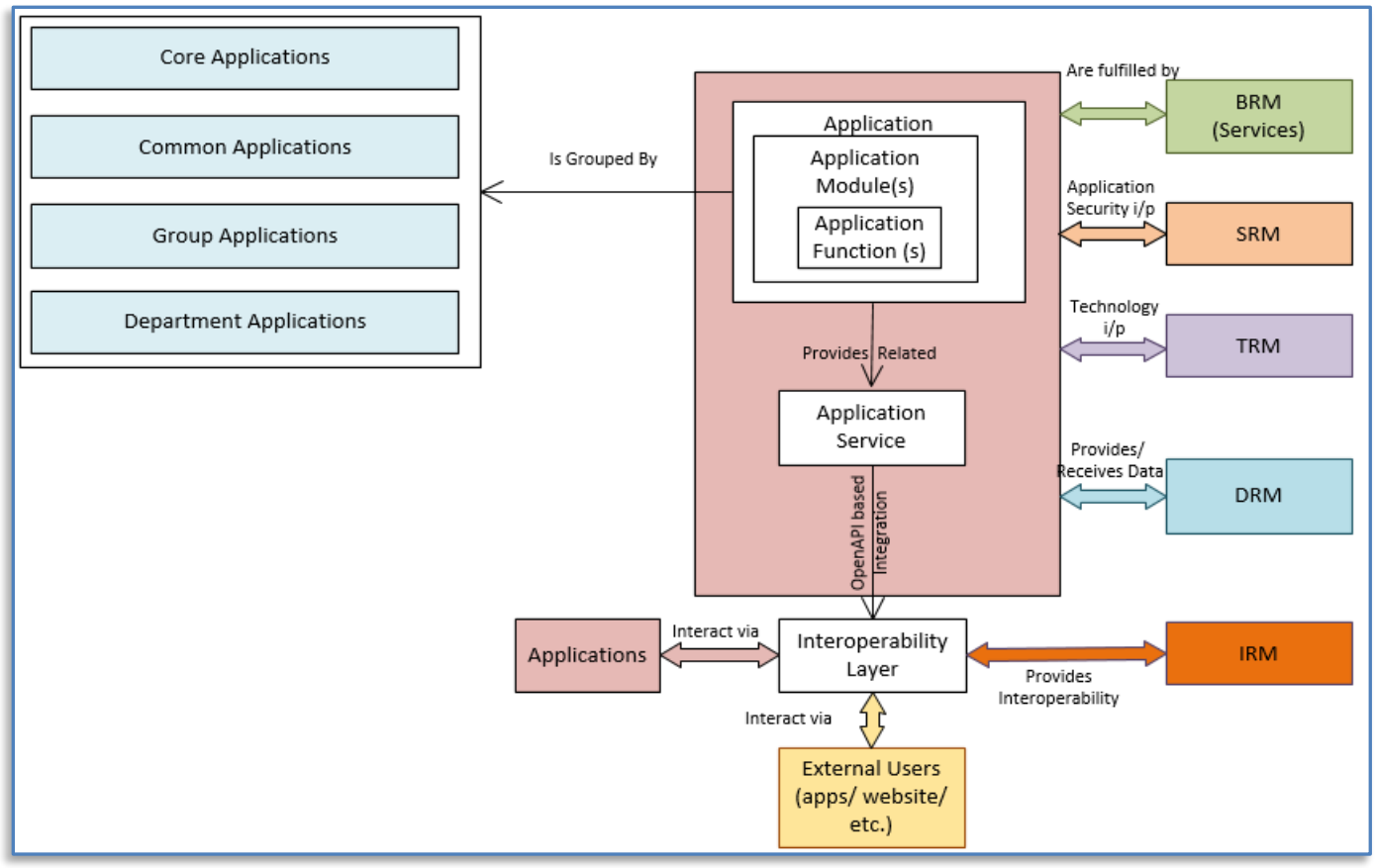


FIGURE 6.1: APPLICATION REFERENCE MODEL

ARM Explained

The Components of ARM are explained below:

a. Application

It represents the Applications that are existing (Brownfield) and/or to be developed (Greenfield) by the State Government. Applications contain Modules/ Sub-Modules/ Functions, Input & Output Data Sources and Interfaces. Figure 6.2 shows the template for Application Description.

Application Code	Department	Application Name	Application Function	Application Description
3.02	Education	School Education	Student Management.	This module provides services to enroll students, register their attendance, tracking their performance and providing them facilities and benefits like course material and scholarships.

FIGURE 6.2: TEMPLATE FOR APPLICATION DESCRIPTION

b. Application Type

The Application Type is a method of grouping of applications based on their use in and across departments as depicted in the **Figure 6.3**. The Application Types are:

- Core Applications
- Common Applications
- Group Applications
- Department Applications

Cross-Cutting Applications are designed to deliver a single service or a set of related services in an orchestrated manner by multiple departments in response to a single request.

The following explanation is offered on the Application Meta-model of ARM, depicted in **Figure 6.3**.

a. The ARM Meta-model is a concentric 4-layered structure. The 4 layers are represented by the 4 types of applications mentioned above. The Core Applications lie at the center surrounded by the other 3 types of applications.
b. The concentric layers are logical in nature. The deployments may be distributed physically and may be implemented in any sequence.
c. All the applications inter-operate to the extent needed, mostly through the Middleware/ ESB or the API Gateway, both forming part of the Core Layer.
d. It is desirable that the Core Applications are designed and implemented together and in the first phase of the IndEA initiative, for better performance and for providing the maximum value to all other layers.
e. The core platform consists of 7 services - a service delivery portal, an app store, a messaging gateway, , an ESB Middleware, an API gateway, Identity & Access Management tool and the India Stack"
f. The actual applications comprising each layer are those drawn from the IndEA Business Landscape described in **Section 4.8**. Primary the meta-model is represented from the perspective of a State Government, but can be easily customized to a GOI Ministry or a PSU, by selecting the full set of Applications (Greenfield and Brownfield) and placing them in the respective layers, depending on the type of each application.
g. Altogether **42 Applications** have been included in the ARM meta-model and shown in **Figure 6.3**. Out of these, 7 are in the Core Layer/ Platform, 15 in the Common Layer, 9 in the Group Layer and 11 in the Department-specific Layer.
h. Together, these 4 layers represent the Application landscape of IndEA, which in turn can interact with External Applications outside the IndEA Portfolio. These interoperability requirements and methods are specified in the **Integration Reference Model** of IndEA.

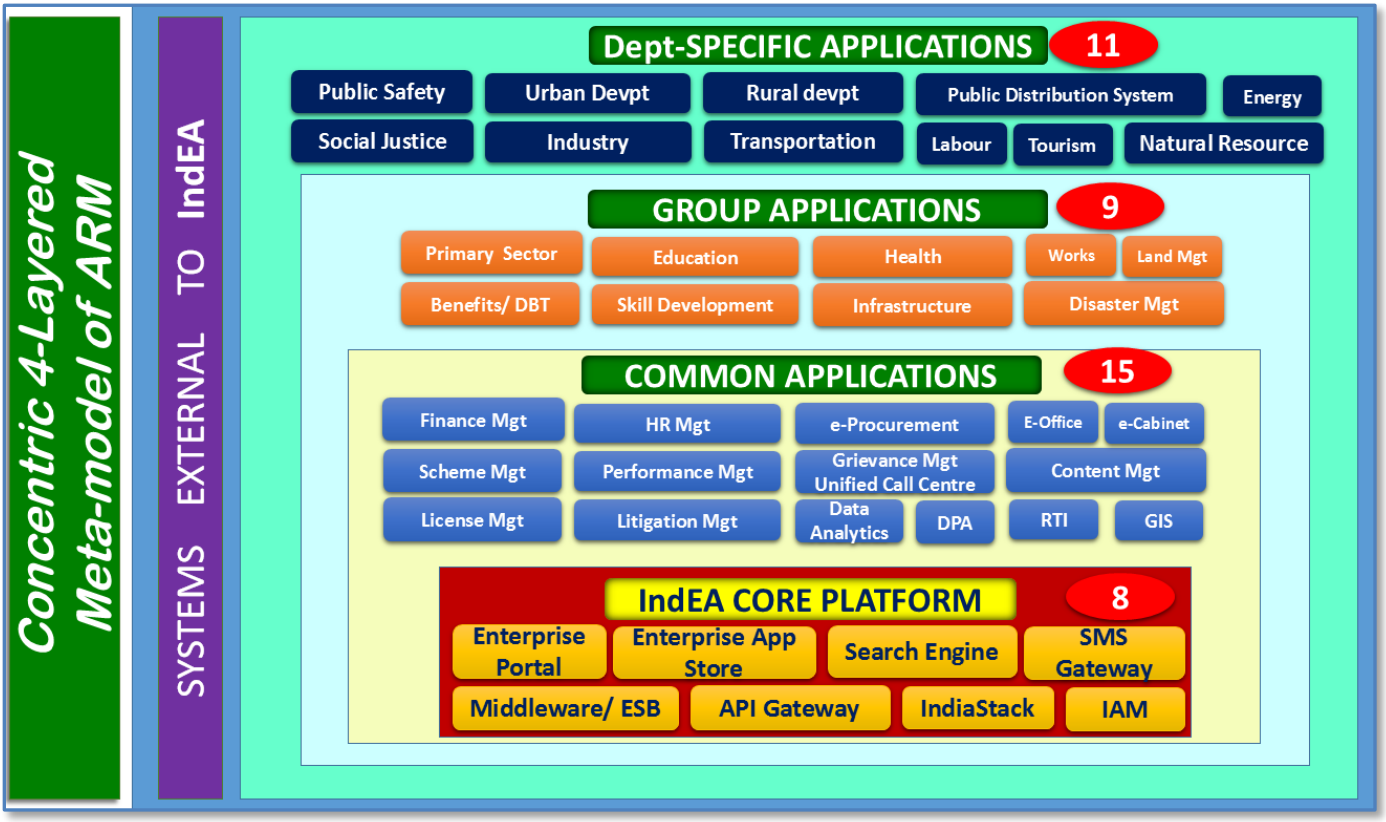


FIGURE 6.3: INDEA APPLICATION PORTFOLIO

c. Application Function

Application function is the specific capability that the application provides to fulfill Application Service. Each Application is composed of one or more Modules & Sub-Modules. Each Module/ Sub-Module can provide one or more Functions. Business Services are fulfilled using one or more Functions.

d. Application Service

Applications fulfill business services by providing individual or composite SOA services. These SOA Services have three components viz. Contract, Interface & Implementation. The difference between Business Service and Web service has been brought out in the definitions section.

e. Interoperability Layer

Designing Interoperation is an integral part of Application Architecture Development. All applications in the Enterprise Application Architecture shall be SOA complaint. The integration between applications shall be via the Enterprise Service Bus (ESB) or through the API Gateway. The ESB supports various features including Mediation, Adaptors, Transport Protocols, Security Management, and System Admin Features. The protocols supported include SOAP, ReST and HTTP(S). APIs designed must be compliant with ***Open-API Specifications.*** Please refer to https://www.openapis.org/ for Open-API specifications. The major components / functionalities of the Interoperability layer are depicted in the **Figure 6.4**:

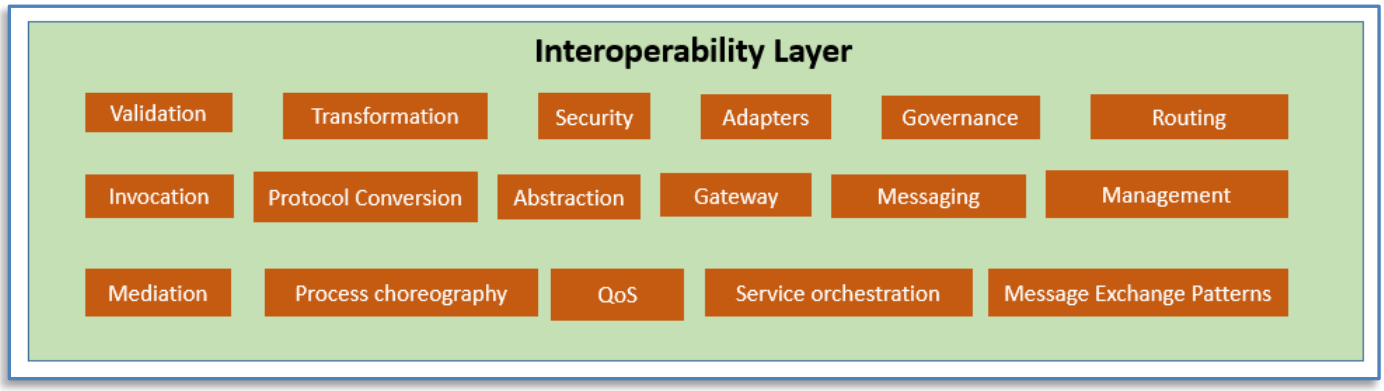


FIGURE 6.4: COMPONENTS OF INTEROPERABILITY LAYER

Integration Reference Model (IRM) is described later in this document, provides additional guidance on Enterprise Integration at various levels.

f. Application Portfolio

The Application Portfolio is the consolidation of all the applications in the organization that effectively provide Business Services. It provides a unified view of all the applications that are present across different departments in the state government. It catalogues the Application's Services, Modules, Sub-Modules & functions. It contains a Meta-Model for Logical Application Components and Physical Application Components. **Figure 6.5** depicts Sample Application Portfolio catalogue.

App. No	Application Name	Application Department	Application Users	Application Function	Application Type	Application Modules	Input Parameters	Output Parameters	Hosting
3.02	School Education	Education	Education Department Parents Teachers Students	Student Enrollment, Fees, Monitoring academic progress.	Line of Business	• Enrollment • Curriculum • Fees & Charges • Examination • Analytics, etc.	(Indicative) • Student Profile • Fees & Charges • Exam Time Table	(Indicative) • Student enrollment ratio/ percentage/ growth %. • Exam Outcome	Cloud

FIGURE 6.5: SAMPLE APPLICATION PORTFOLIO CATALOGUE

The Applications in a State Government's portfolio can be grouped into ***Core Applications***, ***Common Applications, Group Applications*** and ***Department Specific Applications*** (Indicative Applications only. Not exhaustive list). ***The applications are mapped to the Group and Capabilities based on the Services that they fulfill as depicted it Figure 6.6.*** The **Core Applications** are mandated by the State Government to be implemented by all the departments on an **as-is** basis. There is no deviation in the implementation of these applications from the guidelines provided by the state. The **Common Applications** have functionality which is used by all departments, **Group Applications** are used by many (but not all) departments and **Department Specific Applications** have functionality that is department specific. Each Department/ agency implements these applications to meet their

business requirements. All applications are implemented in accordance with the **IndEA Application Architecture Principles**.

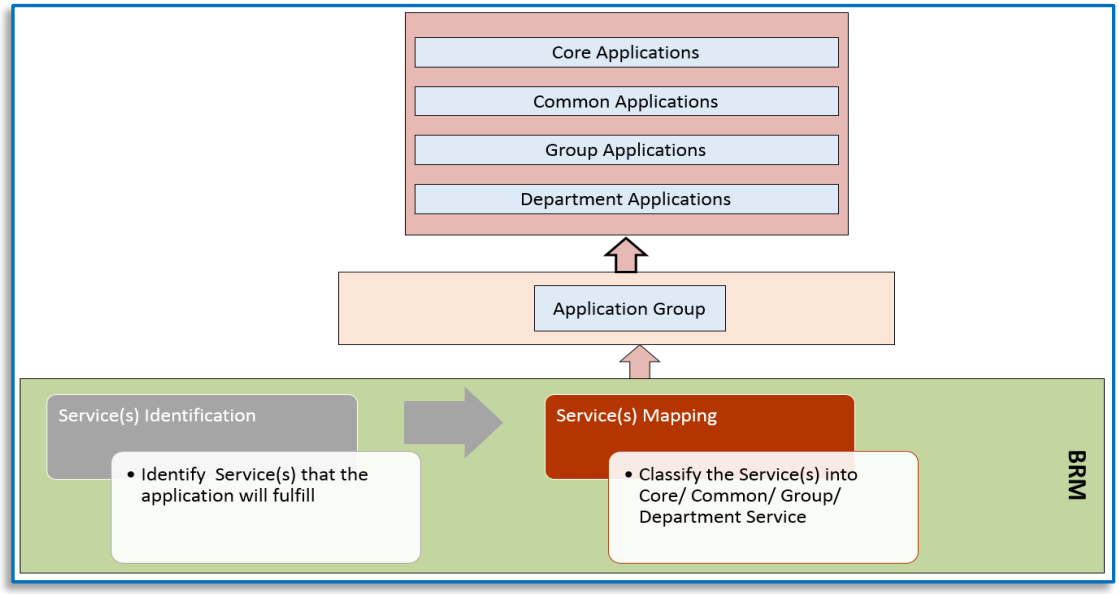


FIGURE 6.6: APPLICATION MAPPING

Application Number Encoding:

Application	Encoding
Application Number	XX<1-99>
Type	Core: 1; Common: 2; Group: 3; Department: 4.
Application Code	<Type>.<Application Number>

TABLE 6.1: APPLICATION NUMBER ENCODING

g. Core Applications

The indicative Core Applications are mentioned below:

Application Code	Application Name	Application Function	Application Module
1.01	Enterprise Portal	Enterprise Portal aggregates all services and makes them available to the Stake-holders.	1. Aggregation of All Services provided by the State Government
1.02	Enterprise App Store	Enterprise Application Development Store and App Usage	1. Developer Registration 2. App Management 3. API Management 4. User Registration 5. App Download
1.03	SMS Gateway	SMS Gateway	1. SMS Gateway

Application Code	Application Name	Application Function	Application Module
1.04	Middleware/ ESB	Supports Interoperability amongst applications.	1. Integration via Middleware. (For details, please refer to IRM Chapter of this document).
1.05	IndiaStack	Facilitates authentication, verification, payments, identity protection, etc.	Provides APIs for: 1. Authentication 2. Document Storage and Verification 3. Payments to and by the Government and 4. Authentication using electronic signature.
1.06	Identity And Access Management System	Identity And Access Management System	1. Access Control Management 2. User Profile Management 3. Policy Management 4. System Administration 5. Authentication & Security Management
1.07	API Gateway	Supports Interoperability amongst applications.	1. Integration via API Gateway. (For details, please refer to IRM Chapter of this document).
1.08	Search Engine	Enables searching structured/ semi-structured/ un-structured documents.	Citizens accessing government portal for services, information, etc. have to search through a large amount of Structured, Semi-structured and Unstructured data. This data has to be aggregated, indexed, etc. In order to ensure that it is easily searchable and readily available to all stake-holders. Various government agencies also access this data for day-to-day processes & to generate analytical reports. The system must also ensure that only authorized personnel are granted access to sensitive data. The Search Engine shall ensure that relevant information is readily available to authorized users. The search engine should enable the stakeholders to perform various types of searches like Boolean, Prefix, Range, Faceting, Full-Text, NOSQL, etc. The Search Engine must support features like

Application Code	Application Name	Application Function	Application Module
			Crawling, Indexing, Query Engine, Matching, Best Bets, etc. The Search Engine must be Secure, Upgradable, Cloud Deployable and must have High-availability & Ease of Migration.

TABLE 6.2: INDICATIVE LIST OF CORE APPLICATIONS

h. Common Applications

The indicative Common Applications are mentioned below:

Application Code	Application Name	Application Function
2.01	Finance Management	It is used for managing the Finances of the state government. The following functions are supported by Finance Management Application (Indicative List): 1. Budgeting & Planning 2. Accounts Payable 3. Accounts Receivable 4. General Ledger 5. Financial Audit 6. Expense Management 7. Limits Management 8. Project Finance Management 9. Funds Approval Workflow 10. Reconciliation Management.
2.02	Human Resource Management System	The HRMS manages all the activities pertaining management of employees viz. Onboarding, Payroll, Attendance, etc. The following functions are supported by HRMS Application (Indicative List): 1. Onboarding employees 2. Payroll 3. Attendance Management 4. Holiday Calendar Maintenance 5. Increments & Salary Revision 6. Appraisal 7. Employee Management 8. Retirement/ Retrenchment 9. Pension Management 10. Contract Employee Management
2.03	e-Procurement	The following functions are supported by e-Procurement Application (Indicative List): 1. Tender Release & Management 2. Addendum/ Errata Management 3. Tender Schedule Management 4. Procurement Process Management

Application Code	Application Name	Application Function
		5. Tender Closure/ Withdrawal 6. Bid Evaluation. 7. Contract management 8. e-Payments
2.04	e-Office	e-Office is aimed at increasing the usage of work flow and rule based file routing, quick search and retrieval of files and office orders, digital signatures for authentication, forms and reporting components.
2.05	e-Cabinet	e-Cabinet Application provides functions relating to (Indicative List): 1. Meeting Scheduling and Management 2. Meeting Agenda Management 3. User Profile Management 4. Content Management
2.06	Scheme Management	Scheme Management Application provides functions relating to (Indicative List): 1. Management of all the Schemes implemented by the Government 2. Dashboards 3. Monitoring & evaluation 4. Feedback 5. Grievance Redressal
2.07	Performance Management	This system enables creating Project Case Details for all the projects undertaken by the State Government. It is a G2G Service and enables government to monitor performance of its projects/ schemes. It translates the goals of the PRM into actual practice, through the use of KPIs
2.08	Grievance Management/ Unified Call Center (UCC)	Grievance Management / UCC serves as a common call center with a single toll-free number to avail various Grievance Management Services for all departments. Some of the features of the Grievance Management system are: 1. User Management 2. Grievance Management Workflow 3. Case Management 4. Document Management 5. Analytics & Reporting 6. Call in 7. Call out 8. User/ beneficiary surveys & feedback
2.09	Content Management	The feature of Content Management system are (Indicative List): 1. Document Life-cycle Management 2. Catalogue Management 3. Search functionality

Application Code	Application Name	Application Function
2.10	License Management System	License Management System is used by various departments to issues & manage licenses. The features of License Management System are (Indicative List): 1. License Management workflow 2. Document Management 3. License Repository 4. License Issuance, Monitoring, Renewal, Suspension & Cancelation
2.11	Litigation Management	The features of Litigation Management System are (Indicative List): 1. Case Management 2. Contract Management 3. Document/ Content Management 4. Calendar & Scheduling 5. Fees & Charges 6. Alerts & Notification on important cases
2.12	Right To Information (RTI)	Integration with RTI-RAMIS
2.13	GIS	GIS Based Systems enable geo-coding, creating maps, etc.
2.14	Data Analytics	Data Analytics provides various analytics based solutions to enable departments to make informed decisions.
2.15	Digital Process Automation	Digital Process Automation assists in automating business processes by providing features like process modelling, Business rules management, document support, low-code support, API support, IoT support, etc.

TABLE 6.3: INDICATIVE LIST OF COMMON APPLICATIONS

i. Group Applications

The indicative Group Applications are mentioned below:

Note:

1. *The Application Functions are illustrative*
2. *The portfolio of the Applications is drawn from the perspective of a typical State Government in India. It can act as the model for drawing up suitable portfolios of Group Applications for the Central Government, a Large Local Government Body or a PSU.*

Application Code	Application Name	Application Function
3.01	Primary Sector (Agriculture/ Sericulture/	The functions supported by Primary Sector application include (indicative list): 1. Extension & Advisory Services

Application Code	Application Name	Application Function
	Horticulture/Animal Husbandry)	2. Input Management 3. Loans & Subsidies Management 4. Insurance (Crop & Livestock) 5. Farm Management Services 6. Supply Chain Management 7. Veterinary Services 8. Warehousing & Marketing 9. Planning
3.02	Education	The functions supported by Education Sector application include (indicative list): 1. Admission Management 2. Faculty Management 3. e-Learning 4. Exam Management 5. Scholarship Management 6. Placement Management 7. Affiliation & Accreditation 8. Management 9. Grants Management 10. Hostel Management 11. Infrastructure Management
3.03	Health	The functions supported by Health Sector application include (indicative list): 1. Public Health Services including: a. Registration of Births & Deaths b. Mother & Child Health (MCH) c. Disease Surveillance d. Control of Non-communicable Diseases e. Nutrition f. IEC 2. Medical Services including a. EMR/ EHR b. Hospital Management (Primary, Secondary and Tertiary Healthcare) c. Emergency care d. Facilities Management e. Telehealth 3. Medical Education including a. Medical Colleges b. Nursing Colleges/ Schools

Application Code	Application Name	Application Function
		c. Pharmacy Colleges d. Medical Research 4. Support Services including a. Health Insurance b. Drugs Control Administration c. Drugs Supply Chain Management d. Diagnostics
3.04	Works	The functions supported by Works application include (indicative list): 1. Works Management 2. Funds Management 3. Management of construction projects 4. Asset Management
3.05	Land Management	The functions supported by Land Management application include (indicative list): 1. Management of Land Records 2. Land Survey & Sub-division 3. Registration of deeds 4. Management of Government/ Community Lands
3.06	Benefits/ DBT	The functions supported by Direct Benefits Transfer application include (indicative list): 1. Scheme Management 2. User Profile Creation and Management 3. Funds Transfer 4. Management of Distribution of Non-cash benefits (e.g. mid-day meals)
3.07	Skills Development	The functions supported by Skills Development application include (indicative list): 1. Skill Requirement Management 2. Program Management 3. Student & Faculty Management 4. Certification Management
3.08	Infrastructure	The functions supported by Infrastructure application include (indicative list): 1. Project Management 2. Project Financing 3. Advisory Services
3.09	Disaster Management	The functions supported by Disaster Management application include (indicative list): 1. Integrated Disaster Management System 2. Command and Control Centre 3. Resources Management 4. Communications Management

Application Code	Application Name	Application Function
		5. Emergency Procurements 6. Logistics & Supply Chain Management 7. Social Media & Crowd Sourcing 8. Damage Assessment 9. Relief 10. Rehabilitation

TABLE 6.4: INDICATIVE LIST OF GROUP APPLICATIONS

j. Department Applications

Indicative department applications are mentioned below

1. *The portfolio of the Departments is drawn from the perspective of a typical State Government in India. It can act as the model for drawing up suitable portfolios of departments for the Central Government, a Large Local Government Body or a PSU.*
2. *Application Functions are not described here.*

Application Code	Application Name
4.01-4.11	1. Public Safety 2. Urban Development 3. Rural Development 4. Public Distribution System 5. Energy 6. Social Justice 7. Industry Development 8. Transportation 9. Labor & Employment 10. Tourism 11. Natural Resources Management

TABLE 6.5: INDICATIVE LIST OF DEPARTMENT APPLICATIONS

6.5. Application Architecture Meta-Model

A government has multiple departments and each department has multiple processes. It is therefore imperative that the government has a visibility on all its processes and is able to modify them easily with minimum disruption of services. Various services shall invoke multiple applications. The orchestration for each of these services needs to be handled effectively. The government will have a mix of legacy applications (pre-SOA) and SOA compliant applications. The legacy applications have to be made SOA compliant. To enable the State Government to analyze the applications from the perspective of SOA, a model comprising the Logical Layers of Enterprise Application Architecture is provided in the **Figure 6.7** and explained in what follows.

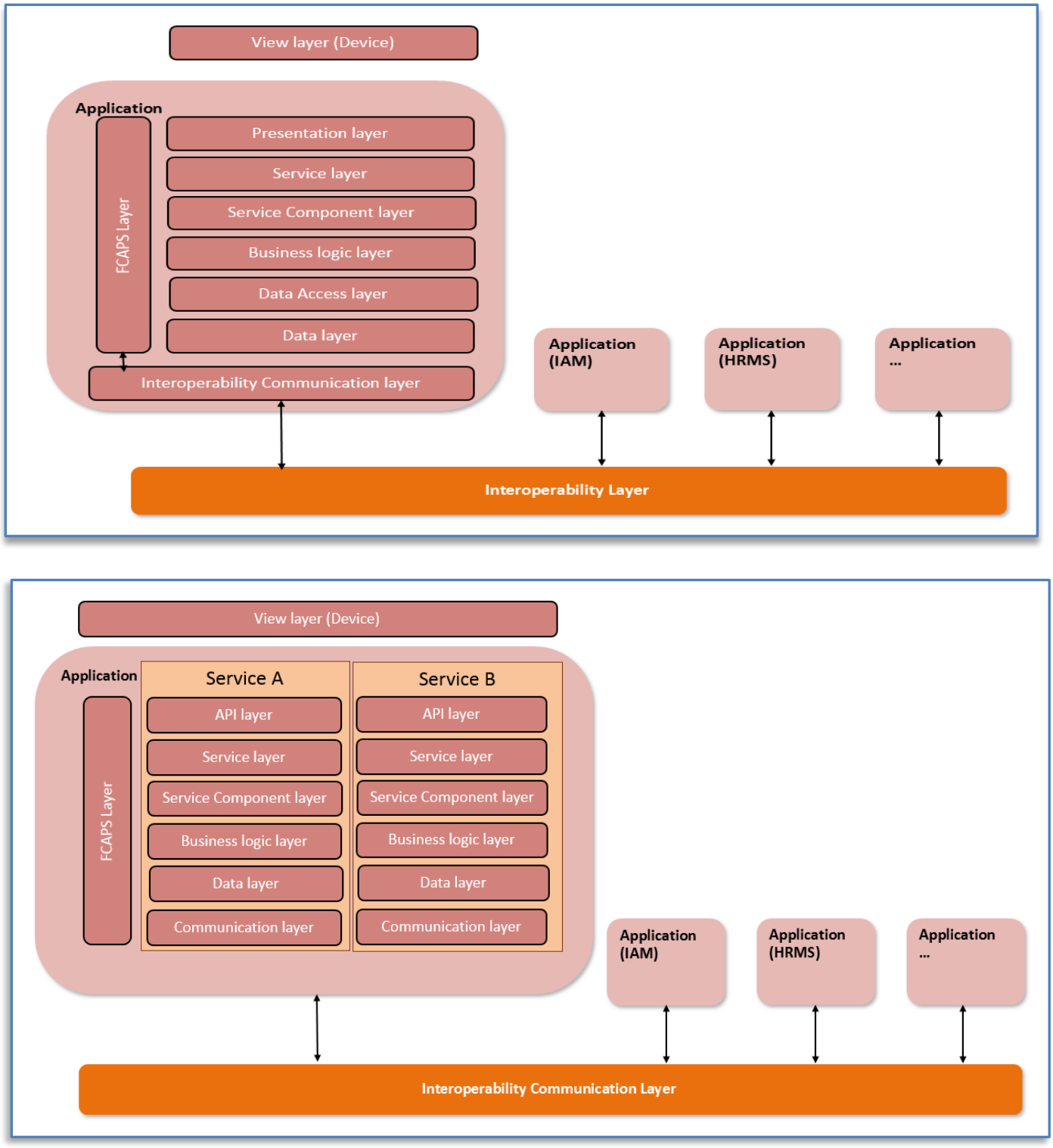


FIGURE 6.7: LOGICAL LAYERS OF ENTERPRISE APPLICATION ARCHITECTURE (SOA & MSA)

View Layer: This layer comprises of thin client, mobile applications, etc. used by the end-user to access the applications.

Presentation Layer: This layer receives inputs from the View Layer and invokes respective services. It is responsible for delivery and formatting of information. It receives the presentation data from application components and returns it to View layer.

Service Layer: This layer comprises of all the Services that are defined in the SOA. The Services can be Individual Service or Composite Service. The Service Layer contains Contracts which binds the Provider and Consumer of the Service.

Component Layer: This layer contains software components, each of which provides the implementation or "realization" for services and their operations. The layer also contains the Functional and Technical Components that facilitate a Service Component to realize one or more services.

Business Logic Layer: This layer enables modelling and designing business processes. A single Service might require interaction of various departments to fulfill the Service. This layer enables mapping the business process and simulating the process. On successful simulation, the process can be deployed in real-time. It also provides for easy change of business processes and its percolation across various departments.

Data Access Layer: This layer provides data from the Data Layer to Business Logic Layer.

Data Layer: This layer comprises of the Applications Database.

Interoperability Communication Layer: All integrations shall be effected through this layer. This layer facilitates effective Mediation Services, provides Adapters, Transport protocols, Service Management, Security features, etc. Translation Logic required for integration is built in this layer.

Application: Applications comprises of both, SOA compliant and legacy applications.

FCAPS Layer: This is the management layer responsible for managing the application component. FCAPS is the term introduced by Telecom industry for management of telecom networks. It is an acronym that stands for Fault, Configuration, Accounting, Performance and Security functions. This layer supports interface for management applications to effectively and efficiently manage the performance of the application.

6.6. Application Architecture Standards

The Enterprise Application Architecture must ensure interoperability of all the applications in the system along with seamless upgradation/ migration and addition of new applications to the system. The Enterprise Application Architecture must adhere to:

- Interoperability Framework for e-Governance (IFEG): http://egovstandards.gov.in/sites/default/files/Interoperability%20Framework%20For%20e-Governance%20(IFEG)%20Ver.1.0.pdf
- Technical Standards for Interoperability Framework for E-Governance in India http://egovstandards.gov.in/sites/default/files/Technical%20Standards%20for%20IFEG%20Ver1.0.pdf
- Software Development & Re-Engineering Guidelines for Cloud Ready Applications http://meity.gov.in/sites/upload_files/dit/files/Application_Development_Re-Engineering_Guidelines.pdf

6.6.1. Application Architecture Guidelines and Best Practices

Some of the important points that application architects must consider while designing the Application Architecture are mentioned below. These are in the nature of guidelines and best practices:

a. Open Source Software

Government of India has notified the guidance for adoption of Open Source Software by Government Organizations. In accordance with the same, the organizations shall endeavor to adopt Open Source Software in all e-Governance systems as a preferred option in comparison to Closed Source Software (CSS).

The Open Source Software shall have the following characteristics:

- The source code shall be available for the community / adopter / end-user to study and modify the software and to redistribute copies of either the original or modified software.
- Source code shall be free from any royalty.

All applications must comply by the "Policy on Adoption of Open Source Software for Government of India". For Further details, please refer to: http://meity.gov.in/sites/upload_files/dit/files/policy_on_adoption_of_oss.pdf

b. Open Application Programming Interfaces (APIs)

The Application Architecture may use Open APIs to enable quick and transparent integration with other e-Governance applications and systems implemented by various Government organizations, thereby providing access to data & services and promoting citizen/ developer participation for the benefit of the community.

All applications must comply the "Policy on Open Application Programming Interfaces (APIs) for Government of India". For Further details, please refer to:

http://meity.gov.in/sites/upload_files/dit/files/Open_APIs_19May2015.pdf

For OpenAPI specifications, please refer to https://www.openapis.org/

Specific OEM products may only be used when necessary to achieve scale, performance and reliability. Every such OEM component/service/product/framework/Managed Service Provider pre-existing product or work must be wrapped in a vendor neutral API so that at any time the OEM product can be replaced without affecting rest of the system. In addition, there must be at least 2 independent OEM products available using same standard/API before it can be used to ensure system is not locked in to single vendor implementation.

c. Service Discoverability

While productizing the existing application or designing a new application for hosting, it is important that accidental creation of redundant services or implementation of redundant logic is avoided. Service discoverability makes this happen by ensuring that metadata attached to a service and describes overall purpose of the service and its functionality, which makes the services easily discoverable. A repository of re-usable business logic components is to be maintained and made available.

d. Platform & Database Agnostic

Applications shall be forward and backward compatible. They shall be deployable on any technology platform and shall be able to communicate with any data store

e. Application design for occasionally connected systems

For the small percentage of functionality that requires "occasionally connected/offline" operations, applications may be designed to use a local persistent store/cache just for the purposes of offline capability and later synchronize with the host application as and when connectivity is restored. As connectivity becomes ubiquitous, less of such offline capabilities are needed.

f. Microservices

Micro Service Architecture (MSA) allows creation of Services which are loosely coupled, have different programming language base, scalable, quicker delivery time, etc. However, addition of every new Micro Service in the system will consume system resources, require integration with other Microservices and potentially increase system latency. Larger number of Microservices will also increase time required to Test and maintain the services. Therefore, MSA should be adopted after conducting due diligence on its likely impact on the overall performance of the system.

Government services are to be exposed via suitable interfaces that are technology implementation and vendor agnostic. One of the approaches is to follow the Open API specifications (https://openapis.org) and must comply with the "Policy on Open Application Programming Interfaces (APIs) for Government of India". For Further details, please refer to: http://meity.gov.in/sites/upload_files/dit/files/Open_APIs_19May2015.pdf

MSA Implementation Example: Government eMarketPlace (GeM)

The Micro Services architecture is emerging as an agile architecture style for modern day systems, it is applied in Government e MarketPlace(GeM) since its business functionality can be broken into smaller and lightweight independent business sub domains and services. Business domain of GeM is divided into four sub domains- 1) Product Catalogue and Direct Procurement, 2) Bid facilitated Procurement, 3) Order Placement and Payment and 4) Analytics; and they are mapped onto four Micro Services. Each Micro Service is a miniature application, having its own Domain, own codebase and persistence mechanisms (Database). This is called as Polyglot, where each team has freedom to choose any tool and technology. Each Micro Service has limited, focused business scope, a very few operations and simple message format.

REST Architecture style is used to build its design. It is simple messaging style which uses HTTP request-response, based on resource API style, where, every functionality is represented with a resource (URI) and operations are carried out on top of those resources. Traditional Monolithic applications use complex binary formats, SOA (Web services-based applications) uses text messages based on the complex message SOAP format and schemas (xsd). But, Micro Services-based applications, use simple and light weight text-based JSON message formats on top of HTTP resource API style.

If business capability is implemented as a service, its service contract has to be defined and published. In traditional monolithic applications, it is never defined. In SOA, Web services model, WSDL is used as a service contract, it is very complex and strongly coupled to SOAP. Micro Service uses REST API definition language, RAML to define the service contracts, which is very light weight.

In order to implement the business functionality, of GeM or any system, services need to communicate with each other. In SOA implementations, the inter-service communication is executed with an Enterprise Service Bus (ESB) and most of the business logic, e.g. message routing, transformation, and orchestration resides in the

intermediate layer, so it becomes thick and complex. However, Microservices architecture eliminates the ESB and move the 'smart-ness' or business logic to the services known as 'Smart Endpoints'. Another option is to use a lightweight message bus or gateway with minimal routing capabilities and with no business logic implemented on gateway. This is known as API gateway Architectural design pattern and it is implemented in GeM.

Key Benefits of MSA include Continuous delivery and deployment, Vertical & Horizontal Scalability, Performance, etc.

Limitations of MSA:

Micro Services Architecture (MSA) allows strong modular development of services as opposed to the monolithic development as is done in service oriented architecture (SOA). MSA emphasizes on loosely coupled development of services making it more suitable for scalable development. It is suitable for faster development when the teams are large and isolated, when modules have the requirement of different programming language or technology base. The architecture undoubtedly has certain advantages such as faster delivery, fault isolation, easy to understand, etc. However, it comes with certain challenges. MSA is not suitable for distributed development. The loosely coupled development may have impact on the performance of the application, maintaining consistency in integrated system may be more challenging. Deployment of microservices can also be more challenging as every module needs to be separately deployed as oppose to a single WAR or EAR of monolithic architecture. MSA solution may not be cost effective on cloud as it may not be able to leverage the complete VM. Hence, like other various architecture MSA should be chosen with its suitability for a particular application.

g. Secure Coding Practices

All applications in the Enterprise Application Architecture must adhere to Standard Secure Coding Practices. For example, while designing and implementing access management, session management, password protection, data protection, Error handling and log management, etc. Indicative standards for Secure Coding are available in **ISO/IEC TS 17961:2013** (Information technology -- Programming languages, their environments and system software interfaces -- C secure coding rules).

h. Non-Functional Requirements of Applications

All the Applications in the Enterprise Architecture must meet the following non-functional requirements (indicative list):

Sr. No.	Requirement	Description
1	Scalability	The application should be able scale elastically to handle the increase or decrease in workload. • All applications must be able to handle volume of **X%** Y-o-Y growth for the life of the application. • The Application must support load balancing and routing. • The Application must support horizontal and vertical scaling of Servers, compute, storage, network, etc. • Graceful failure: The application must not have any Single-point of failure. There must be a graceful degradation of services in case of any failure.

Sr. No.	Requirement	Description
2	Performance	The Application must comply by Service Response Time as required by the Application and stipulated in the SLAs.
3	Security	All applications in the Enterprise Application Architecture must adhere to Standard Secure Coding Practices as stipulated by GIGW Standards and other Standards Body.
4	Usability	The applications must comply with ISO 9241-210:2010 Standards (Ergonomics of human-system interaction), GIGW Standards and other standards as stipulated by the state government.
5	Quality	The applications must comply by ISO/IEC 25010:2011 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models, GIGW standards and other stipulated standards.
6	Availability	All Applications must support the Availability SLAs as mentioned for each application. The system must meet the stipulated RTOs and RPOs.
7	Recovery	The applications must comply by the Recovery Point Objective and Recovery Time Objective as stipulated in the DC & DR requirements.
8	Error Handling & Resolution	The applications must efficient error handling. It must also provide detailed logs to enable efficient de-bugging and issue resolution. A repository of 'Known Issues' must be made available to the System Administrator.
9	Documentation	All Software documentation including but not limited to Requirement Gathering, BRS, FRS, Gap Analysis, Design, Testing Use Cases, User Guides, etc. must be maintained with proper Version Control and Access Rights. Software Traceability Matrix must be maintained.
10	Support for Differently-Abled Users	All applications must support accessibility by Differently-Abled Users and adhere to GIGW Standards.
11	Change Control	The must be a Change Control Board which must approve and monitor the changes that are done to the software. All Change Request documents must be approved before implementation and Unit Testing and System Integration Testing must be done post-implementation.

TABLE 6.6: NON-FUNCTIONAL REQUIREMENTS OF APPLICATIONS

6.7. Rationalization of the existing Application Portfolio

Rationalization of the existing Application Portfolio enables Governments to optimize their efforts in designing and implementing Enterprise Architecture. The existing applications must comply with the target application architecture and must be evaluated on the following parameters:

a. Conformance to IndEA Principles
b. criticality of the application in the business landscape
c. Volume of Services and number of End-Users of the application
d. Uniqueness of the functionality of the application
e. Performance of the application
f. Conformance to Open Standards
g. Conformance to Meta Data and Data Standards
h. Application's adherence to security standards

Based on the above assessment, all existing applications which are required in Target Architecture may be categorized into:

A. Application which are compliant with the above criteria and can be used 'As-Is'.
B. Applications to be enhanced and made compliant
C. Applications which cannot be enhanced and have to be retired

6.8. ARM and Other Reference Models of IndEA

The Enterprise Architecture provides a layered structure to group Performance, Business, Application, Data, Security and Technology Architectures. It enables design of interoperability amongst different layers in the Architecture. The interaction of ARM with other Reference Models is depicted in **Figure 6.8** below:

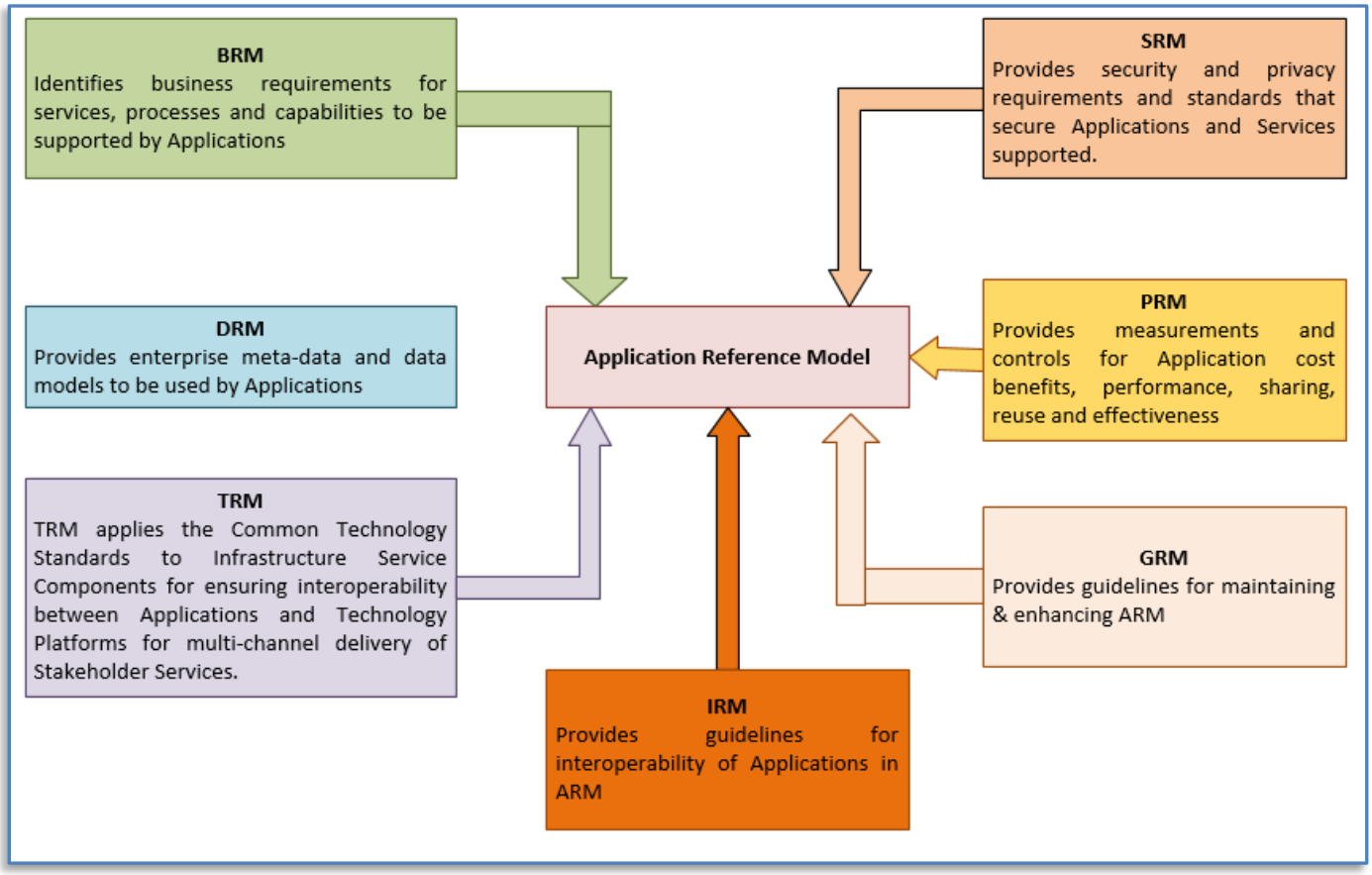


FIGURE 6.8: ARM AND OTHER RMS

ARM and DRM:

The Data required by the Applications to fulfill the Business service is modeled using DRM. The Data required as Input by the applications can be either generated as Manual Input OR be obtained through integration with another application/ data source. The output data is stored in a data store (Database/ Data warehouse, etc.). The

DRM provides the syntax and semantics of the Data elements which are consumed by ARM. All applications in the Application Architecture must adhere to the data standards stipulated in the DRM.

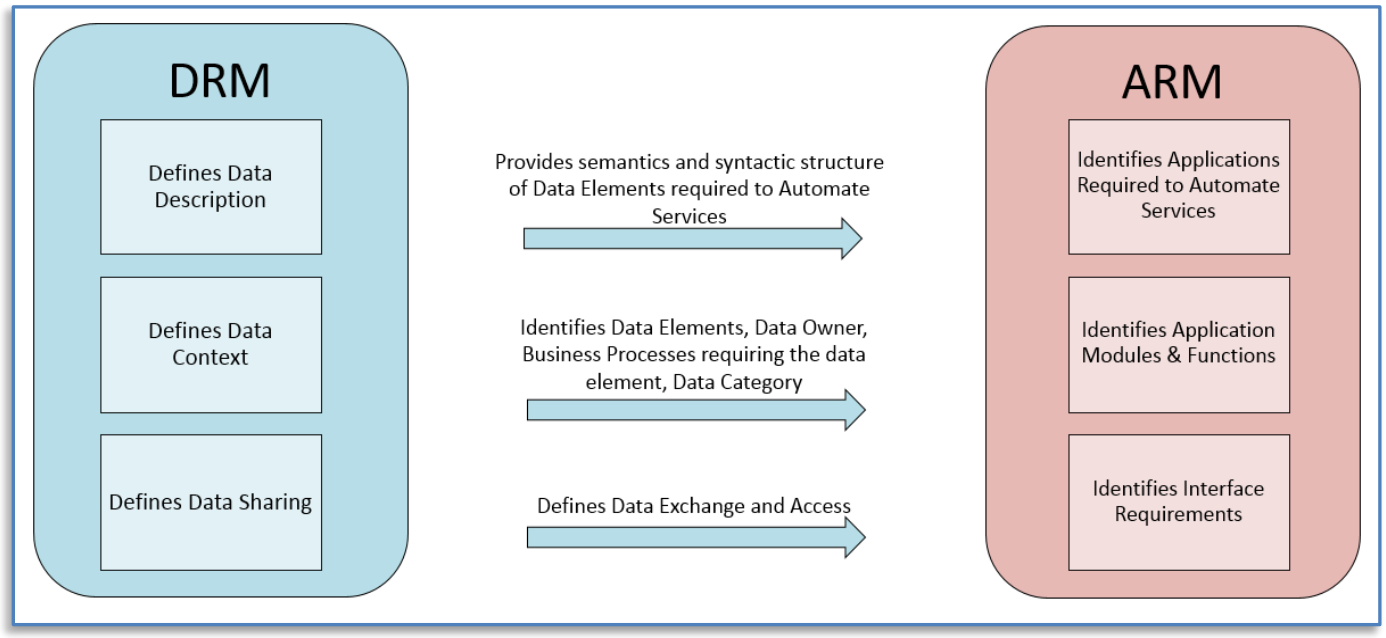


FIGURE 6.9: RELATIONSHIP BETWEEN DRM AND ARM

ARM and IRM:

The Integration Reference Model provides the guidelines for integrating applications in the Enterprise Architecture. It ensures interoperability of all applications in the EA. It identifies different integration methods for different application types.

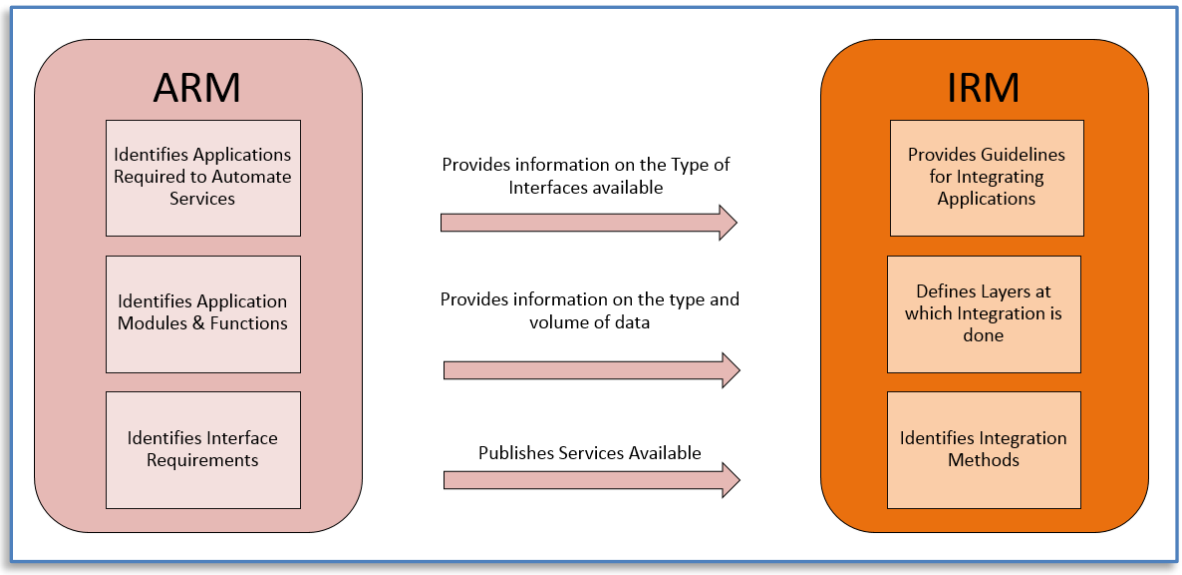


FIGURE 6.10: RELATIONSHIP BETWEEN ARM AND IRM

6.9. Preparing for AI in Government with Enterprise Architecture

Artificial Intelligence (AI) in government involves the design, development and adoption of cognitive computing and machine learning to improve the operations of government entities, with the goal of improving governance. Use of AI in government is not without challenges and impediments. However, adoption and use of architecture based approach, provides a solid way to deal with these challenges and impediments. This enables in elevating the readiness in government entities to use AI. The table below lists the main challenges and impediments and how they are addressed by IndEA:

Sr. No.	Challenges to AI Adoption	Role of Enterprise Architecture in Addressing Challenges
1	Legacy IT Infrastructure	The adoption of TRM addresses the issue of legacy IT infrastructure, and drives modernization. With the TRM, infrastructure standardization is easier and the associated technology governance ensures that moving forward, the issue of "legacy" is minimized. This is essential for AI adoption.
2	Limited IT Interoperability	The IRM is specifically provided to address issues of interoperability. The IRM takes a holistic perspective to integration – primarily targeting application, data, and technology layers. They form the crux of enhancing IT interoperability.
3	Lack of Data Driven Approaches / Solutions	The DRM is provided to enable the adoption of data driven approaches and solutions. One of the key aspects of AI is to analyse data and uncover underlying patterns, to gain insight and inform decision making. For data to be usable, it needs to be analysable. The DRM advocates how data is described, contextualized and shared in a standardized manner.

4	Inadequate Enterprise Security	The SRM addresses aspects of security in an integrated manner. It takes a multi-tier approach starting from data (the asset to be secured) to private and public cloud infrastructure. The security controls are provided for guidance.
5	Risk Aversion	The risk aspect is covered within the SRM. The IndEA provides access to methods to quantify and measure risk. The primary reason for risk aversion is inability to understand the risks and therefore, coming up with mitigating strategies. Proper use of AI generally leads to discovery of unexpected findings.
6	Limited Capacity to Make System Level Changes	Enterprise architecture as an approach is to encourage adoption of system level changes. A good and effective architecture provides insight, oversight and foresight, the essential components of systemic changes. EA discourages piecemeal thinking and solutions, as they lead to sub-optimal outcomes.
7	Limited Credibility of IT Departments	An effective and mature EA elevates the credibility of IT Departments. Use of reference models enable adoption of standards, which is imperative to scaling up. EA gives the IT departments a baseline to be proactive into strategic issues, rather than being in a perpetual operational fire-fighting mode. EA improves communication and enhances governance.
8	Inadequate Participation by Business Domain Experts	AI succeeds only if adequate time and resources are spent on "training" the computers. This requires business domain experts to be part of any AI journey. The use of EA, specially through the PRM and BRM helps in creating performance objectives and indicators closely linked to the business operations, requiring involvement of business domain experts.

TABLE 6.7: AI ADOPTION

To summarize, adoption of enterprise architecture (based on IndEA) prepares government entities for an AI based approach. Collectively, the eight reference models interjected within the underlying TOGAF ADM (in Part 2) are designed to address the challenges to AI adoption. An effective architecture is an essential pre-requisite to delivering AI in Government.

6.10. Developing Enterprise Application Architecture from ARM

Enterprise Application Architecture facilitates collaboration amongst all state departments and different business functions within the departments. Emphasis must be laid on re-usability and sharing of applications to gain cost-advantage. The current application architecture is analyzed and application catalogue is prepared. Applications are grouped by their 'Type' and 'Capability'. Target Application Architecture is developed based on Current Business Architecture and Gap Analysis. If required, Transient Application Architectures may be developed. For details on developing Enterprise Application Architecture from ARM, please refer to the chapter on 'Implementation Approach' and 'IndEA Adoption Guide – A Method Based Approach' for further details.

7. Technology Reference Model

The Technology Reference Model enables the development of an interoperable and cost effective Technology Architecture Central, State and Local Governments and their agencies for an efficient and effective service delivery.

Technology Reference Model (TRM) *depicts the layout of the technology foundation of ICT-based systems to be designed for delivery of identified business services. TRM lists all the components of the technology system on an end-to-end basis, including IT Infrastructure, Applications, Access Devices, Communication Systems and Service Delivery modes. TRM defines the currently applicable open standards for all the solution building blocks and components and identifies the Open Source Products for each technology component.*

7.1. TRM Objectives

The objectives of Technology Reference Model (TRM) are to:

a. Create a framework for designing the Target Technology Architecture for the enterprise
b. Depict the logical and physical components of the Technology Architecture to support the Arm and the Architecture Vision
c. Identify and describe the functionality of the Architecture Building Blocks, essentially required to implement the Enterprise Technology Architecture
d. Enable the preparation of an Architecture Definition Document
e. Identify and list the Open Standards and Specifications of the components required for deployment of the Technology Architecture
f. Identify the Open Source Products wherever prudent and applicable
g. Provide a method for mapping the stakeholders' concerns to the Architectural Building Blocks and technology components
h. Define methods to ensure that the Technology Architecture has the essential attributes of Performance, Maintainability, Availability and Security.

7.2. Definitions

a. **Service Outlets:** The access devices through which electronic services are delivered to stakeholders. Example are mobile, tablets, laptops, kiosks, digital signage.
b. **Virtualization:** Creation of a virtual version of a device or resource, such as a server, storage device, network or even an operating system where the framework divides the resource into one or more execution environments. **Open Standards:** The standards/protocols that are publically available for inspection and application/system development. These standards are used by the community of vendors and system integrators for making their products and services interoperable.
c. **Open Formats:** The data/message formats and standards which are widely accepted by the community of vendors and system integrators for making the products and services interoperable with the smooth flow of data from one application/system to another.

d. **Interoperability:** It defines the ability of one application/system to communicate with another application/system upon requirement. This is achieved by adhering to common standards and protocols while the application/system components are designed and built.
e. **Enterprise Service Bus:** The inter-application communication happens though messages through a common channel called enterprise service bus. The applications are connected to the above bus via adaptors and data messages are transferred via connectors for making applications technology agnostic. It also does the message queuing, routing, publish/subscribe and event based activities via dedicated APIs.
f. **Open API:** The API refers to Application Program Interface or Application Platform Interface. It provides a secure and authenticated (digitally signed) channel for external applications or services to access an embedded service or functionality of another application. Open API refers to the sharing of data between different platforms.
g. **Microservices:** Applications built for a single or a few coherent fine-grained services which could be developed using lightweight protocols and rolled out by a team size of less than 10 people.
h. **ROA:** A new paradigm in application development where designing and developing software as resources. The Resource Oriented Architecture (ROA) uses popular RESTful (Representational State Transfer) APIs using HTTP verbs such as GET, POST, PUT and DELETE for enabling microservices.
i. **SOA:** It's paradigm architectural style in software development where the application is built in terms of aggregation of services at the atomic levels, discoverable and accessible through standard protocols. This ensures the reusability of the services, and creates a lesser impact on other services when the data, view or logic of a service needs to be altered.
j. **Internet Objects:** The applications or devices which are accessed over the web by another application elsewhere for accessing an embedded service or functionality. Alternatively, for the above purpose the device or external applications may use the web to access a service or program in another application. IoT (Internet of Things) works on the above method.

7.3. TRM Principles

Principle TRM 1: Technology Independent Architecture
Enterprise Architectures are developed in a technology-neutral manner so as to avoid captivity to a specific product or implementation method.

Principle TRM 2: Future-proof Architecture
Enterprise Architectures are suitably designed and developed so as to be future-proof, not requiring frequent revisions with the advent of every new technology.

Principle TRM 3: Open Standards
Open Standards are adopted in the design and implementation of all greenfield systems. Legacy systems are incentivized to migrate to open standards, where required.

Principle TRM 4: Shared Infrastructure
IT Infrastructure is shared to ensure optimal utilization and effective maintenance.

Principle TRM 5: Cloud First
Cloud infrastructure is chosen by default for deployment of applications and on-site option is resorted to only with strong justification.

Principle TRM 5: Mobile First
Mobile channels are mandatory for delivery of all services, among all delivery channels.

Principle TRM 6: Availability
The information systems along with the applications and services are available 24 x 7.

7.4. TRM Schematic

TRM gives a consistent and common vocabulary for description of interoperability requirements between diverse systems, support for commonality across systems, consistent use of standards, and comprehensive identification of information exchange and interface requirements. It ensures that the agencies of the central and state governments benefit from economies of scale by identifying and reusing the best solutions and technologies that support their departmental missions, functions, services and target architecture.

TRM focuses not only on the products but also on the interfaces between applications/platforms and between the platforms/communication infrastructures which connects applications to the users. The above approach underscores that the infrastructure applications have a robust platform to run and execute their services by adopting a common technology standard. TRM provides the traceability of IT investment by continually measuring and evaluating the technologies and standards. By aligning governmental capital investments to the TRM ensures inter-department discovery, collaboration, and interoperability.

The proposed TRM envisions deployment of cloud native applications, delivery platforms, network components, and access devices. The above components could be open source or proprietary products. As per GoI policy, the open source products shall be given preference wherever applicable and prudent. For interoperability, all proprietary products or devices used shall follow open standards and the data communications shall follow open formats.

For improving the efficacy of application architecture and deployment and for creating a third party ecosystem consisting of startups, the Open API Gateway is a must. It allows a component based architecture with APIs, that could be shared with other components and the third party ecosystem for accessing the services embedded in component structure. The arrival of third party applications and service providers and their access to governmental big data will transform the governance though several value added services to the stakeholders. The conceptual map of the proposed TRM is illustrated in the diagram below:

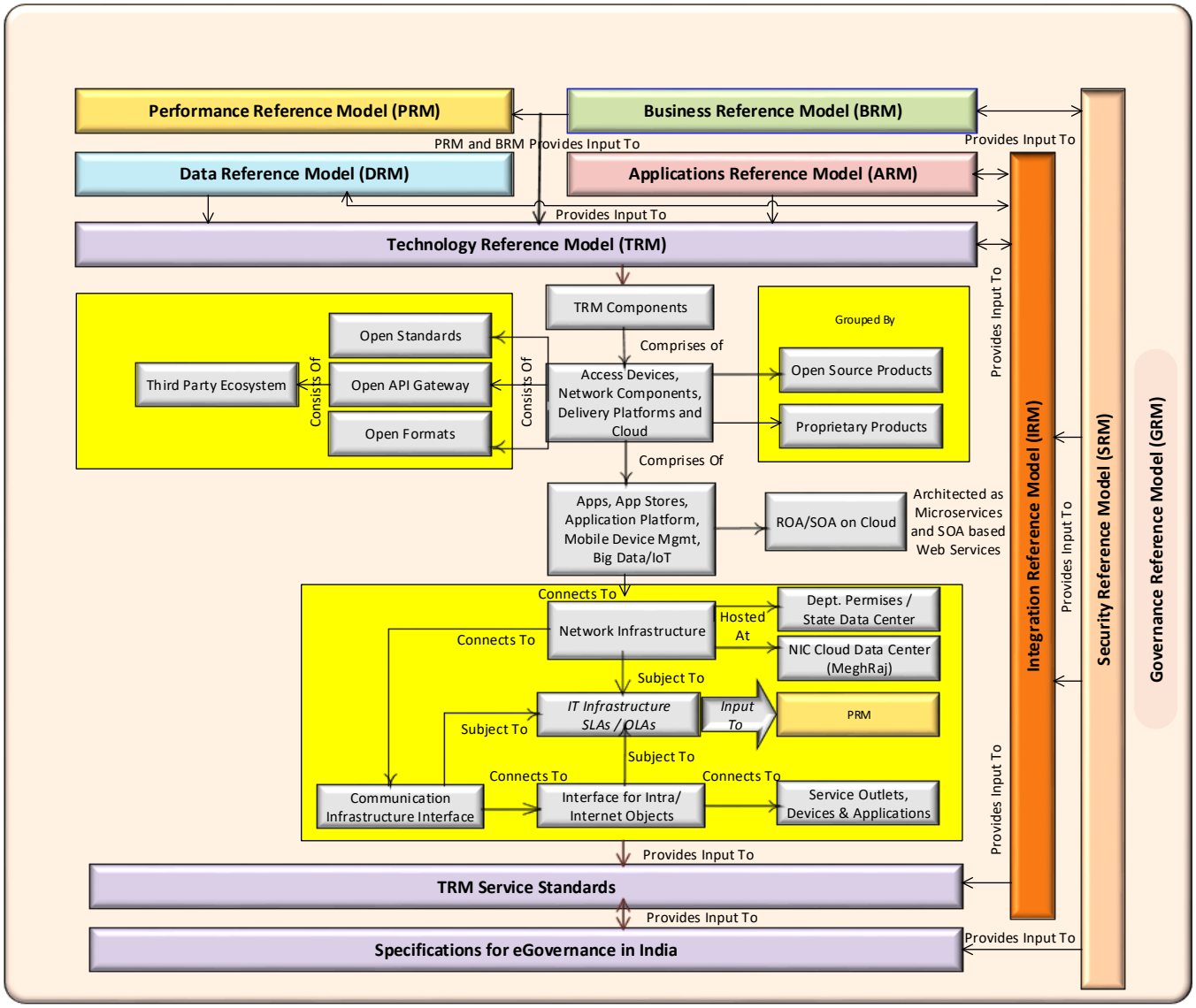


FIGURE 7.1: TRM CONCEPTUAL MAP

The services delivered through Open API Gateway for third party service providers or applications or other stakeholders shall be either RESTful Microservices or SOA based services. In order to ensure scalability the departmental services needs to be virtualized and deployed on cloud. All existing monolithic applications needs to be excavated for implementing a hybrid of RESTful/SOA based cloud native application architecture. These augur well for virtualization of departmental services on cloud and it's on demand delivery. The existing monolithic applications at departmental premises or state data center or NIC cloud, may be given a façade for integration, adapter for exchanging protocols and translators for data exchange for reorienting them to the Micro/SOA Services architecture.

The IT delivery infrastructure consisting of platforms and applications, and the communication infrastructure consisting of network and security components operates based on agreed SLAs and OLAs for ensuring the high availability of services. The measures of performance of the above infrastructure component are monitored via network monitoring systems and the indicators are shared to Performance Reference Model. The technology standards for the above components need to be established and maintained for their interoperability requirements, and the smooth delivery of virtualized on demand services from the cloud to external service outlets, devices and other third party applications.

Therefore, the Enterprise Technology Architecture resulting from the Technology Reference Model shall address the design issues, constraints, opportunities and challenges and give possible solution options for its implementation.

7.5. Technology Architecture Trends

The top technology trends point to the sweeping changes in the applications and technology landscape. It's the technological innovation that drives economic and business cycles - as per Schumpeter the famous economist http://www.economist.com/node/186628 . Therefore, if the TRM has to relevant for the 21st century, it has to adopt to disruptive digital technologies and modern application development practices. Adoption of these new age technologies will help to maximize the governance capabilities of the states and the central government.

The conceptual map of Technology Reference Model gives the big picture of the e-Governance technology facets. However, to assist departments and digital platform architects to create interoperable platforms and systems for digital transformation using Social Media, Mobile, Analytics, Cloud, Big Data and IoT requires application and technology architecture models. The basic architecture models are provided in Open Group Standard - Technology Base Reference Models for Open Platform 3.0™. The latest technology trends for Cloud, Open API are given below:

7.5.1. Open API-Based Architecture

The TRM functional diagram for Virtualization of Departmental Services using Open API Gateway on Cloud is illustrated in the diagram below:

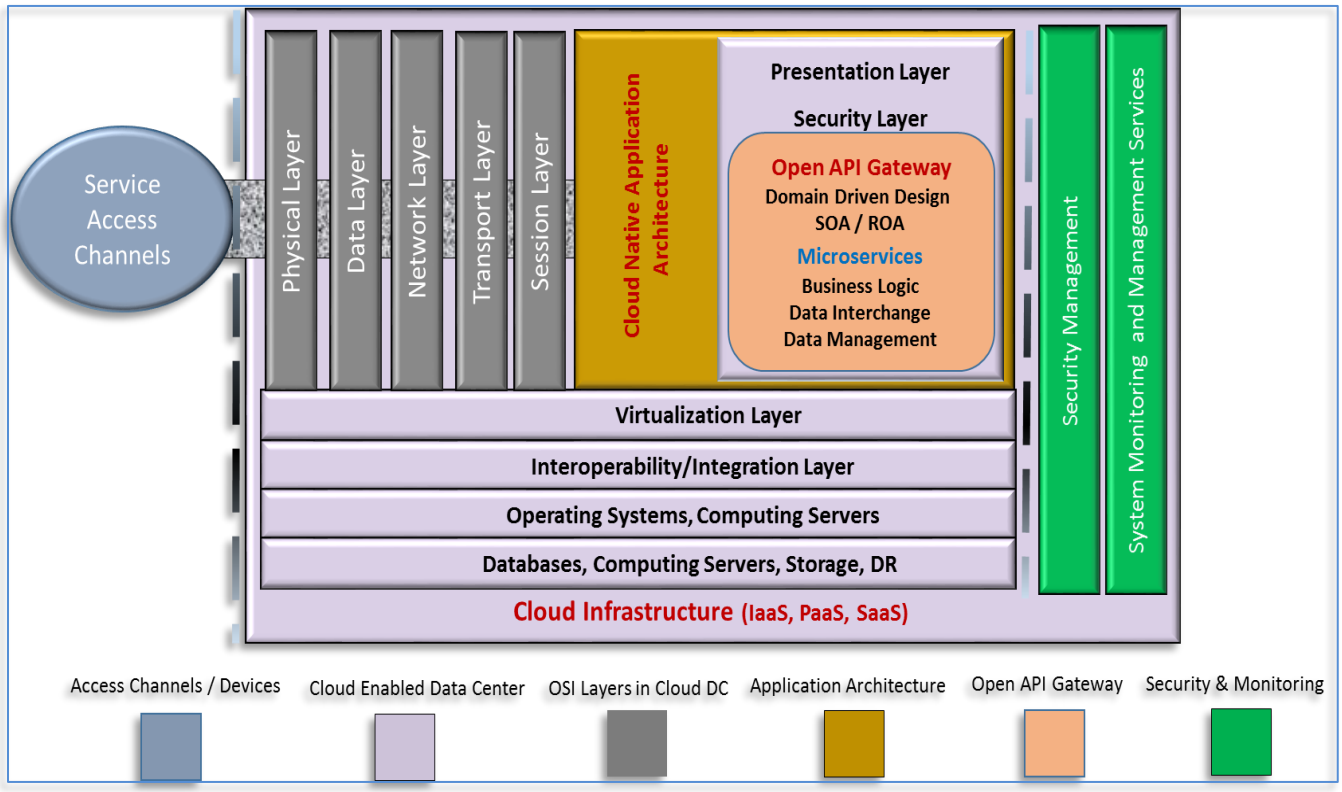


FIGURE 7.2: TRM FUNCTIONAL REPRESENTATION - FOR CLOUD, OPEN-API AND MICROSERVICES

For example, the GST Technology Architecture follows the Open API design considerations as described below:

a) The system is designed to expose four sets of distinct APIs for the consumption of G2C, G2B, G2G and one for internal use to manage the entire system in terms of hot fixes, deployments, configurations, monitoring and security services. These APIs shall be centrally configurable based on the change in government policies and business rules. The APIs may be RESTful, XML-based, and stateless services wherever microservices are defined, and it should be SOA based for integrated services (non-microservices). This creates two categories of APIs i.e. RESTful and SOA based.

b) The use of open APIs addresses loose coupling of components allowing independency of each other and having a service provider neutral layer for allowing use of one or more providers and replacement of a system component with another without affecting other parts of the system. The data access must be always through APIs, no application will access data directly from the storage layer or data access layer. For every internal data access also (access between various modules) there will be APIs and no direct access will be there.

c) While developing the APIs, it should be ensured that the API end points shall be behind the application's presentation and security layer and it should be consumed via secured VPN (HTTPS protocol) for increased application security. The OAuth 2.0, OpenID and LDAP directory services should be enabled for Open API

Gateway to enable application access through secure servers. The encapsulation of access control, auditing, confidentiality (encryption), and integrity (digital signatures) is possible via common APIs.

d) As the system will be API driven, the APIs built both by internal and external authorities should go through performance and security measures to increase reliability. For increased security, partitioning, encryption and hashing should be done at the application level and it should not be proprietary features of the databases used. The security and privacy of data needs to be protected using strong PKI national standards for encryption, use of Hardware Security Module appliances, physical security, access control, network security, stringent audit mechanism, and through measures such as data partitioning and data encryption wherever applicable.

e) For linear scaling of a parallel and distributed system, the system shall be architected to work in parallel within and across machines with appropriate data and system partitioning. The containerization of applications has to be done for easy deployment of applications just in time and the container environment variables has to be configured via OS. The data partitioning or sharding ensures the scalability of the system at data access level by using RDBMS, Hadoop, NoSQL data stores and distributed file systems running under the SAN using fiber based communication protocols.

f) The envisaged cloud system shall be built as platform with open APIs with an open scale out architecture using commodity hardware from established OEMs. The cloud system architecture should support horizontal scaling when required, thus allowing to make incremental capital investments when required. The system should support lights out scenarios by allowing non-intrusive monitoring of solution components for better manageability and proactive maintenance. Whenever options are available, open source frameworks/components shall be used instead of proprietary frameworks/components to avoid vendor lock in and high sustenance costs.

g) The API driven approach allows test automation for automated regression testing, continuous re-factoring and tuning within an implementation, and better component level versioning and lifecycle management.

h) The Technology Standards for Application Layer, Infrastructure Components and Cloud Computing Stack are given in Annexures (III - V) Technology Standards for Application Layers, Technology Standards for Infrastructure Components, TRM Service Standard – Cloud Computing Stack respectively.

7.6. Technology Architecture Standards

The TRM has to provide guidelines and open standards and open formats for the technology solution building blocks that can be widely referenced and used by the government departments and agencies involved in e-Governance services. The use of open standards and open formats for the development/procurement of solution building blocks increases the interoperability of solution building blocks in multiple deployment environments.

7.6.1. Application Component Standards

For seamless service delivery to stakeholders, the open technology standards for application layers needs to be defined. The application layers has to support common standards for application level and service level interoperability. The commonly used Application Layers while designing departmental solutions is illustrated in the diagram below. The technology standards for the Application Layers are given in **Annexure (III) -** Technology Standards for Application Layers.

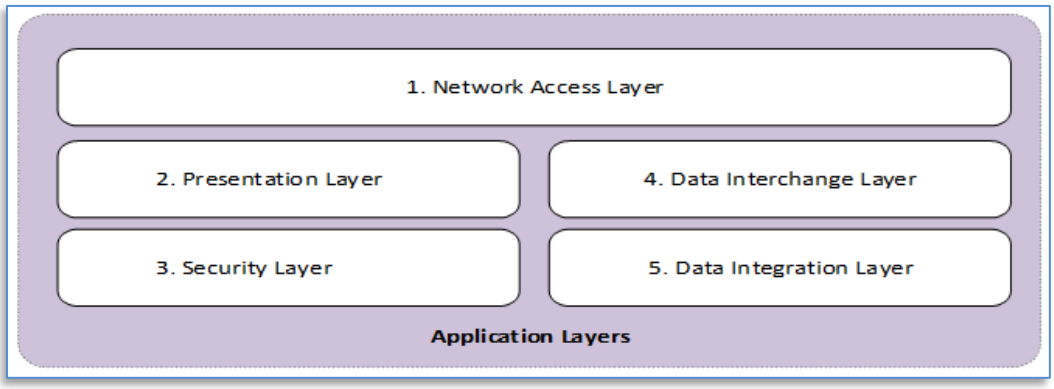


FIGURE 7.3: TRM APPLICATION LAYERS

7.6.2. Infrastructure Component Standards

The infrastructure components required for virtualization of services and its on demand delivery using a cloud model is categorized into Access Devices, Network Infrastructure, Delivery Platforms, and the Cloud Computing Stack. The aforementioned infrastructure components for a cloud centered e-Governance journey using Open Standards and Formats is indicated in the diagram below:

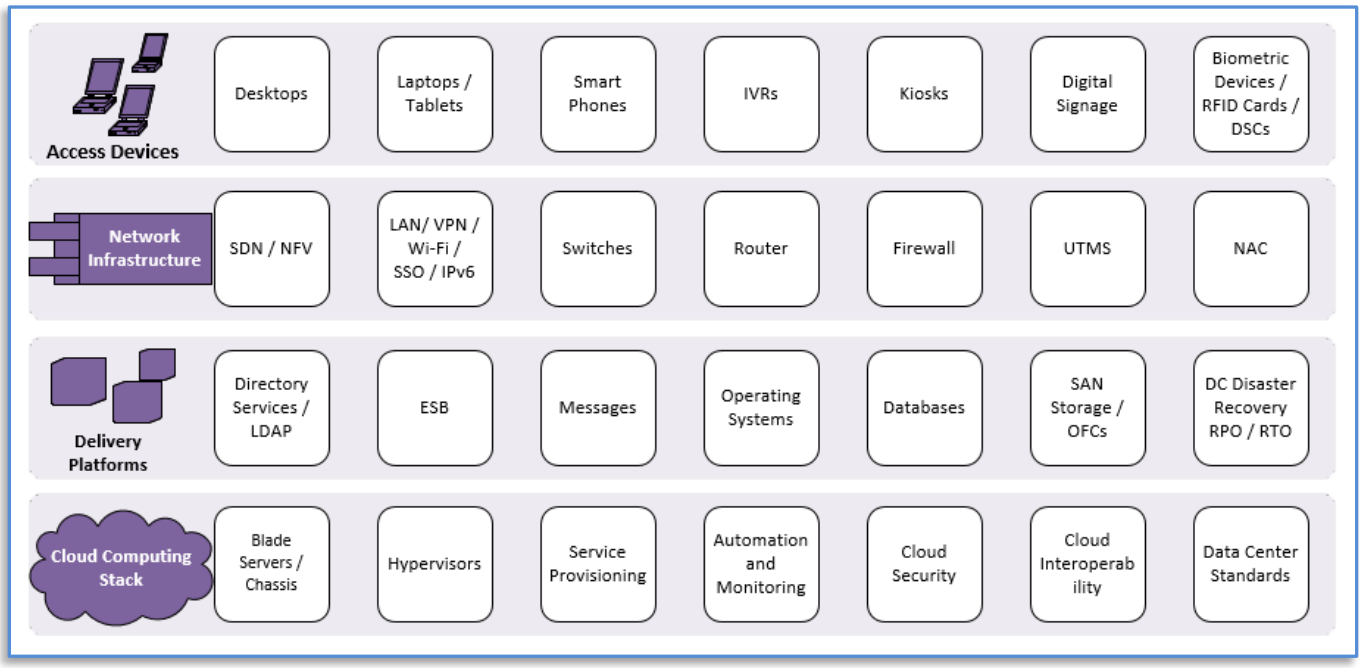


FIGURE 7.4: TRM SOLUTION BUILDING BLOCKS

The open technology standards for the solution building blocks and equivalent open source products wherever available is given in the **Annexure (IV) -**Technology Standards for Infrastructure Components . The open source solutions may be used wherever prudent.

7.6.3. Technology Options for Multiple Service Delivery Scenarios

India being a geographically dispersed country with a huge population with different ranges of tech savviness cannot be juxtaposed with a one size fits all solution criteria. Therefore, the choice of technology has to cater based on geography, age (digitally savvy or not) and tech-economic profile (people with smart phones and ordinary phones; people connect to internet and not). Accordingly, the technology choice for different scenarios is illustrated below:

Sr. No.	Scenario	Technology Options	Specification
1	For poor people who doesn't own any smart phones and live in remote rural areas were internet signal strength is weak.	1. Interactive Voice Response (IVR) 2. SMS based Services 3. USSD (Unstructured Supplementary Service Data) based Services	1. IVR uses a touch-tone telephone to interact with a backend predefined database to acquire information from or enter data into the database based on user choices between 1 to 9. Using modems, the analog signals from phone is converted to digital data in the application. The database could be any RDBMS, preferable an open source one like MySQL. 2. In case of the SMS based Services, the User sends a structured SMS query to a given mobile number, and the conversation can continue between the backend application server and the user through interactive queries. The SMS replies are received by the GSM operator and passed (via modem) to the SMS gateway which transfers the SMS to the backend application database using SMS Gateway APIs. The data can then be processed by the server side application which may be preferably written in a platform independent language like JAVA, PHP or Python 3. USSD messages create real-time connection between the GSM SIM phone and the application server enabled for the same. The application server hides the USSD protocol from the user, hence the user needs to input predefined text/alphanumeric values in the defined format to avail the menu/location based information or transaction services. The application frontend could be JavaScript and the core application may be developed in Java ME. For USSD, there is no established

Sr. No.	Scenario	Technology Options	Specification
			communication standard, the application developer can prescribe the standard. *The USSD data handling is network dependent, and it is not easy to get all the telecom service providers to agree on a standard prescribed by the developer. Hence, SMS based services is preferable when compared to USSD based services.*
2	Remote Rural areas with limited internet signal strength, and people uses smart phones.	1. Lightweight Mobile Apps which works both in online/offline mode 2. JSON/XML 3. RESTful / SOA architecture based API for backend application and database architecture (Refer sections 7.5.2 and 7.5.3)	1. The mobile apps size shall be restricted to a maximum of 5MB. The mobile app shall be developed using HTML5, Ajax, CSS3 and Responsive Web Design. The App shall have light webpage headers, footers and frames by default, so that only the transactional data needs to be exchanged with the application server, for increased performance. The App shall have a local ACID-compliant database preferably an open source one like SQLite for caching the data for publish/subscribe activities. For data transfer between the App and the application server JSON shall be used.
3	Geographical areas with good internet strength and high population density	1. Kiosks 2. Digital Signage	1. Kiosk is a touch screen that displays information upon taping the screen. It can work on WAP and web based application protocols. 2. The Digital signage use technologies such as LCD, LED and Projection to display content such as digital images, video, streaming media, and information. The Digital Signage uses HTML5 and Unity3D for interactive content. The Synchronized Multimedia Integration Language (SMIL) is used to improve standardization and interoperability of the digital signage. The JPEG images and MPEG4 videos remains the popular digital content formats for the digital signage. Connecting digital signage with mobile apps (via Bluetooth) will help

Sr. No.	Scenario	Technology Options	Specification
			the visually impaired citizens not only to get voice based instructions, but also for navigational purposes in campuses or offices.
4	For applications with high volume transactions	1. Java, Python, PHP, Apache / NGINX, JBoss, Linux 2. JSON/XML 3. RESTful / SOA architecture based API for backend application and database architecture (Refer sections 7.5.2 and 7.5.3)	1. For high volume structured transactions the programming languages could be preferably platform independent ones like Java, Python and PHP. 2. The application stack may preferably be open source like Apache / NGINX for webserver, JBoss for application server and Linux as the operating system. 3. For structured transactions RDBMS shall be used to maintain ACID compliancy.
5	For applications with high volume multimedia data	1. CMS, Apache / NGINX, NoSQL, JBoss, Linux 2. JSON/XML 3. RESTful / SOA based API for application and database architecture (Refer sections 7.5.2 and 7.5.3)	1. Use a readymade Content Management System (CMS) preferably an open source one like Drupal 8, Joomla, WordPress etc. This will cut down development time and increase performance. 2. The webserver may preferably be open source like Apache / NGINX. 3. The use of NoSQL facilitates large unstructured data processing capability to the application. 4. The application server could be preferably open source like JBoss on a Linux server.

TABLE 7.1: TECHNOLOGY OPTIONS FOR MULTIPLE SERVICE DELIVERY SCENARIOS

7.7. TRM and Other Reference Models

The Enterprise Architecture provides a layered structure to group Performance, Business, Application, Data, Security and Technology Architectures. It enables design of interoperability amongst different layers in the Architecture. The interaction of ARM with other Reference Models is depicted in the diagram below:

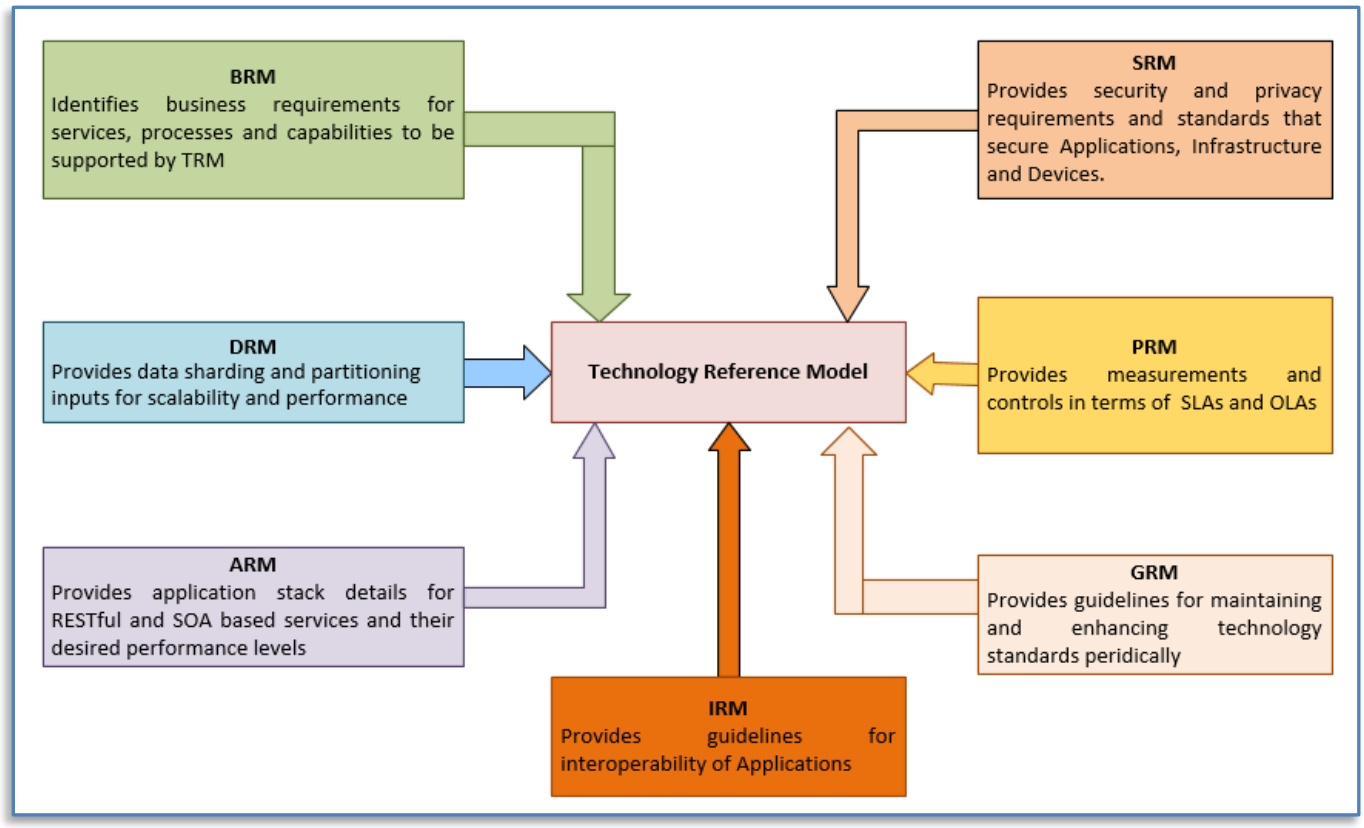


FIGURE 7.5: TRM AND OTHER REFERENCE MODELS

TRM and ARM:

Applications in ARM provides the specifications in terms of interface devices, infrastructure requirements, data type/ volume, etc. to TRM. ARM has to adopt the open standards and formats as defined in the TRM. ARM will provide the SOA and RESTful Microservices performance levels to the TRM for adopting suitable technology stack.

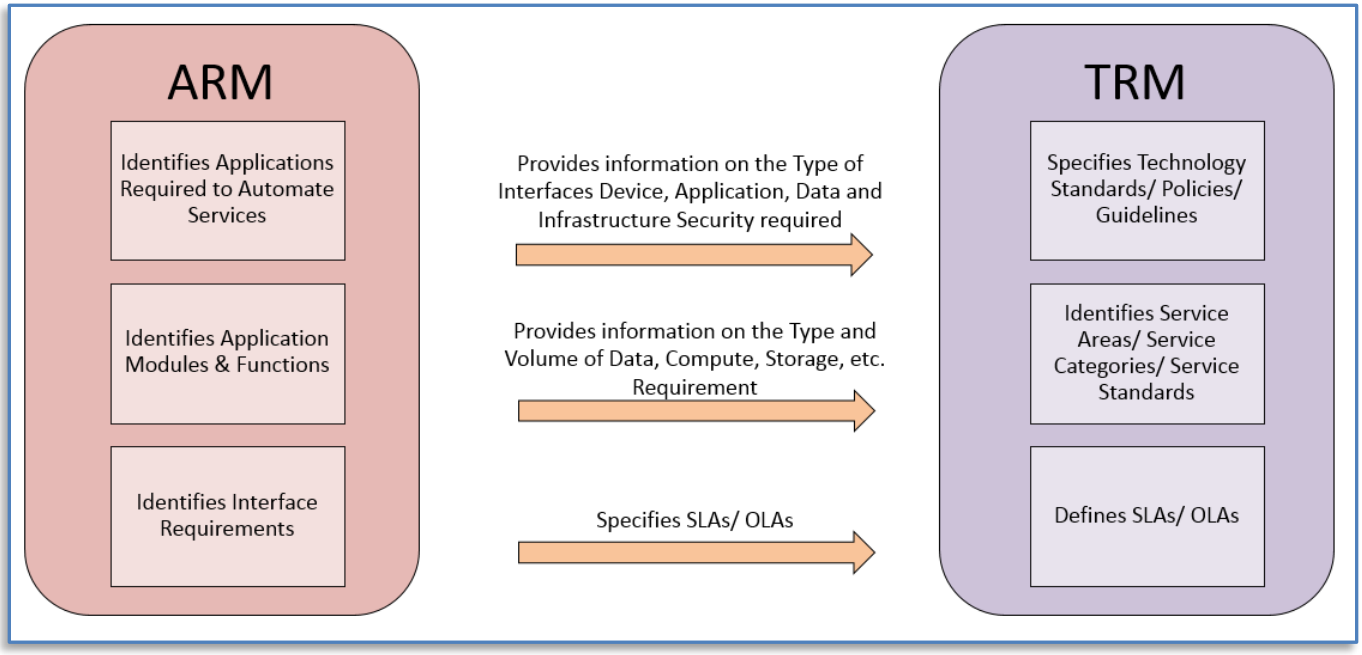


FIGURE 7.6: RELATIONSHIP BETWEEN TRM AND ARM

7.8. Developing Enterprise Technology Architecture from TRM

The TRM needs to transition from a reference model to a technology architecture for its practical usage.

a. Use Domain Driven Design Techniques and bounded contexts, and develop the Services catalogue as per section 7.5.3 for RESTful Microservices and Integrated Services SOA.
b. Use guidelines for building Open API Gateway in sections 7.5.2 and 7.6.3 for technology options for multiple scenarios.
c. Identify Software and Hardware components used in the layers of the architectural patterns diagram given in Figure 7.2
d. For each of the above components, identify the open standards, and use open source products wherever prudent and applicable with reference to annexures as given below.
e. Refer the service standard tables for Application Layer standards in **Annexure (III)-** Technology Standards for Application Layers, for Infrastructure Components in **Annexure (IV) -** Technology Standards for Infrastructure Components, and for deployment and interoperability standards for cloud computing in **Annexure (V)-** TRM Service Standard – Cloud Computing Stack.
f. For further details on developing Enterprise Application Architecture from TRM, please refer to the chapter on 'Implementation Approach' and 'IndEA Adoption Guide – A Method Based Approach'.

8. Integration Reference Model

A critical aspect of Enterprise Architecture in Governments is their ability to make government administrations at different layers to collaborate and work together in order to provide public services in an integrated seamless manner. When multiple government entities are involved there is a need for coordination and governance by the relevant authorities with a mandate for planning, designing, provisioning, and operating public services. This makes integration architecture covering all the viewpoints (performance, business, data, application, technology, security) an absolute imperative to realize the vision of **ONE Government**.

8.1. IRM Objectives

Enterprise Integration is the most important step in achieving the vision of **ONE Government**. The other reference models described in this part cover aspects that are important building blocks to the overall architecture, while the integration perspective is the glue that keeps them together and relevant. With its goal of connecting the dots, the integration architecture is the layer that enables provisioning of seamless citizen experience when interacting with the government in its various institutions and agencies. In the context of India, this is even more relevant as the structure involves governments at central, state and local levels, with varying degrees of administrative controls and procedures. The IRM aims to:

i. Guide government entities at various levels to conceptualize, design and deliver public services that are *cashless*, *paperless* and *faceless* in a seamless manner, independent of the internal administrative structures and operations of the government;

ii. Highlight the various layers that contribute to holistic integration, elaborate relationships between them thereby fostering cross-organizational and cross-sectoral interoperability; and

iii. Elaborate the realization of integration in the application layer by presenting and comparing the various technical strategies to implement integration.

8.2. IRM Concepts and Definitions

Concepts:

a. **Performance Integration:** Outcome based performance metrics aggregating multiple input measures in a way that represents the results being targeted, coming in from one or multiple underlying business processes and activities, realized through the PRM.
b. **Business Integration:** End-to-end services that are personalized, choice-based and available via multiple channels in an orchestrated manner by coordinated business processes in different government organizations working in concert to enable synchronized internal operations, realized through the BRM.
c. **Data Integration:** Exchange of data between parties involving both government and other organizations in a way that ensures privacy and security, enabled by a standard method for describing data, common taxonomy and sharing, covering both semantic and syntactic aspects, realized through the DRM.
d. **Application Integration:** Linking of applications and systems between disparate organizational entities operating in harmony for realization of end-to-end services, manifesting synchronized processes and data, resulting in application portfolio optimization and shared capabilities, realized through the ARM.

e. **Security Integration:** Ensuring that information that enable delivery of services are made available to the right person, at the right time, in the right format, through the right channel, for the right purpose to achieve the right outcome, realized through the SRM.
f. **Technology Integration:** A common and shared platform of technical capabilities, used to identify the standards, specifications, and technologies that support and enable the delivery of service components and capabilities, realized through the TRM.
g. **Integration Governance:** A functional view of government entities organized around mission priorities, vertical and horizontal lines of business and business functions, that encourage collaboration and eliminates redundancies and overlaps, realized through the GRM.
h. **Hybrid Integration:** It is a concept used for the platform which can integrate Applications hosted on cloud with on-premise Applications. It provides the best fit solution to the Enterprise for seamless exchange of information between on-premise Legacy Applications and cloud based Applications.

Definitions:

a. **Managed File Transfer (MFT):** This is used to transfer the data from one system to another in a secure way.
b. **Service:** A Service is a logical representation of a repeatable business activity that has specified outcome.
c. **Integration Platform as a Service (iPaaS)[3]:** Integration Platform as a Service (iPaaS) is a suite of cloud services enabling development, execution and governance of integration flows connecting any combination of on premises and cloud-based processes, services, applications and data within individual or across multiple organizations.
d. **API:** API stands for Application Programming Interface, which is an Interface for software program or service that can be used by another software program to communicate to each other.
e. **REST API:** It is an Application programming interface which is based on representational state transfer technology. REST is a web service architectural style for communication.
f. **Business Process:** It is an activity or set of activities designed to achieve the some business goal.
g. **Swagger:** Swagger is an open specification to define REST APIs.

8.3. IRM Principles

1. **Principle 1: Openness and Transparency -** Government data is made open, barring exceptions, so that external parties can build services.
2. **Principle 2: Interoperability –** Interoperability is assured through adoption of open standards and open interfaces.
3. **Principle 3: Data Portability –** Data is easily transferable and usable across jurisdictions, applications and systems.
4. **Principle 4: Primacy of User Experience –** All service interactions are designed with citizens at the core, by providing integrated multi-channel service delivery.

[3] Source: http://www.gartner.com/it-glossary/information-platform-as-a-service-ipaas/

5. **Principle 5: Elimination of Digital Divide –** Digital public services are available to citizens and users belonging to all groups, and there are no differences and discrimination based on location (rural versus urban), access to technological infrastructure, and physical abilities.
6. **Principle 6: Multilingualism –** Services are delivered in language/s that are preferred by the consuming populations with the option of multi-lingual support, wherever feasible.

FIGURE 8.1: INTEGRATION DESIGN PRINCIPLES

8.4. IRM Schematic

The UN e-Government Survey 2016 identifies the need to take a holistic and integrated approach as a key factor in delivering public services in a seamless manner, across the whole-of-government, extending even to the overall ecosystem. Integration can be achieved at many levels, starting from integration within and between government entities (intra-government), integration with government entities across state and national boundaries (inter-government), integration with entities outside the government, i.e. the ecosystem (extra-government) and finally to a stage wherein integration becomes so ubiquitous, that government acts as a platform to design and deliver new innovative services. This staged approach to integration maturity is depicted in the **Figure 8.2** below.

The key point to note is that with increasing integration maturity, the underlying complexity increases exponentially. This is because public services have to factor in multiple levels of government, myriads of individual government entities, interactions with numerous external entities, all operating in a coordinated and orchestrated manner, towards a common overarching goal. This would mean that the Enterprise Integration in the context of Government would be significantly different from and more complex than in a typical business enterprise. **Enterprise Integration in the government landscape can't be achieved through a single technology or suite of products, but would require the deployment of a judicious combination of technologies and products available in the integration space**.

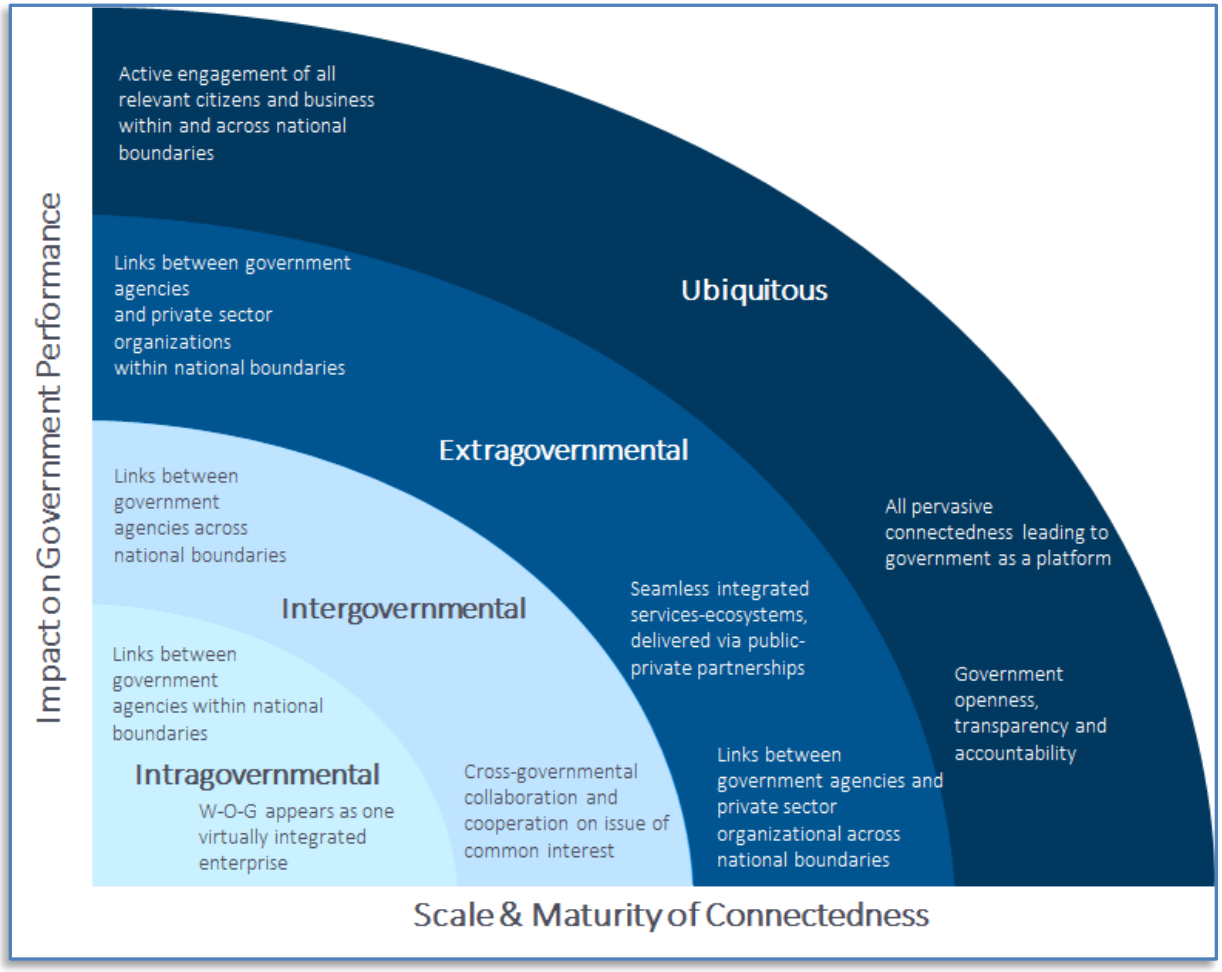


FIGURE 8.2: STAGED APPROACH TO INTEGRATION MATURITY

The IRM promotes the notion of **Integrated by Design** as its core theme, and **Figure 8.2** fosters the following:

- **Seamless service experience** based on an orchestration function, aimed to eliminate the complexity for the end-user;
- **A 'no wrong-door' service delivery** policy realized through front, middle and backend integration to provide alternative options via multiple delivery channels;
- **Reuse of business, data and technology services** to achieve consistency and economies of scale;
- **Secure-by-design** realized through a balance of preventive and corrective controls.

Figure 8.3 depicts the layers of integration in a conceptual model, while **Figure 8.4** shows the Enterprise Integration Reference Model, in concert with the various other RMs forming part of the IndEA Framework.

Integration of any kind is driven by the **mission priorities** that are translated to actionable goals and performance indicators. These set the overall direction for the organizations. The results and outcomes require aggregation of data from various sources (services and underlying business processes) and generating a set of

analytics. The goals and performance indicators are converted to a portfolio of services enabled by underlying business processes, which are consumed by users (citizens and businesses). These services can range from being department specific to spanning the entire ecosystem. Realization of cross-domain, cross-sectoral services require data interchange, common data standards and communication protocols.

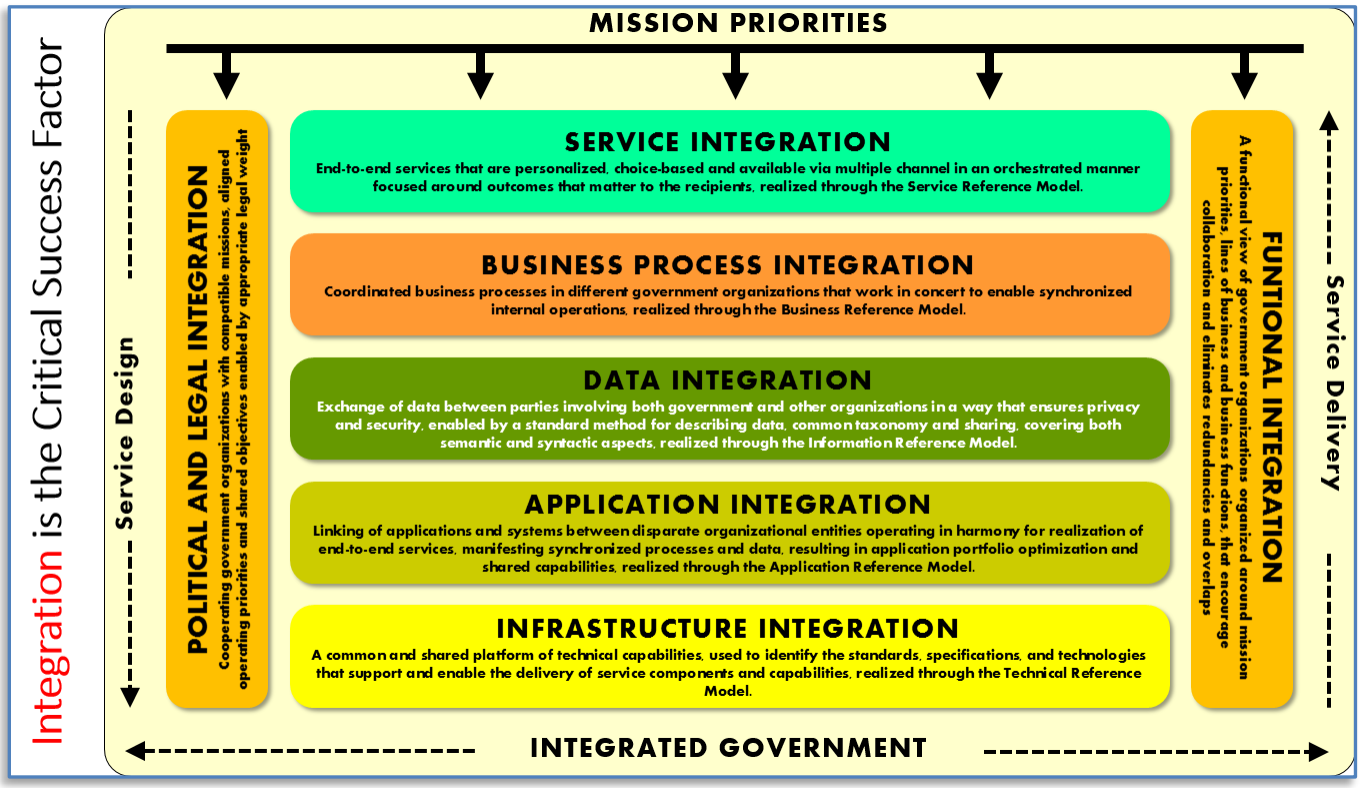


FIGURE 8.3: INTEGRATION REFERENCE MODEL (IRM) – CONCEPTUAL VIEW

Digitization of services needs applications and systems to interact with one another with certain standard protocols. This is enabled by **data integration**, guided by **business integration** and driven by **performance integration**.

Integration governance is a critical success factor as it addresses key issues like the following:

i. In case of a shared public service requiring involvement of multiple entities, who is accountable for its performance?

ii. In case of reuse of capabilities and components, what are the economic factors that need to be factored in?

iii. In case of loss of information, especially when involving external parties, where does the jurisdiction of the government extend to?

iv. Are the various government entities ready and able to share information, in an acceptable form?

v. What institutional arrangements, organizational structures, roles and responsibilities, policies and agreements are required to make the integrated government work?

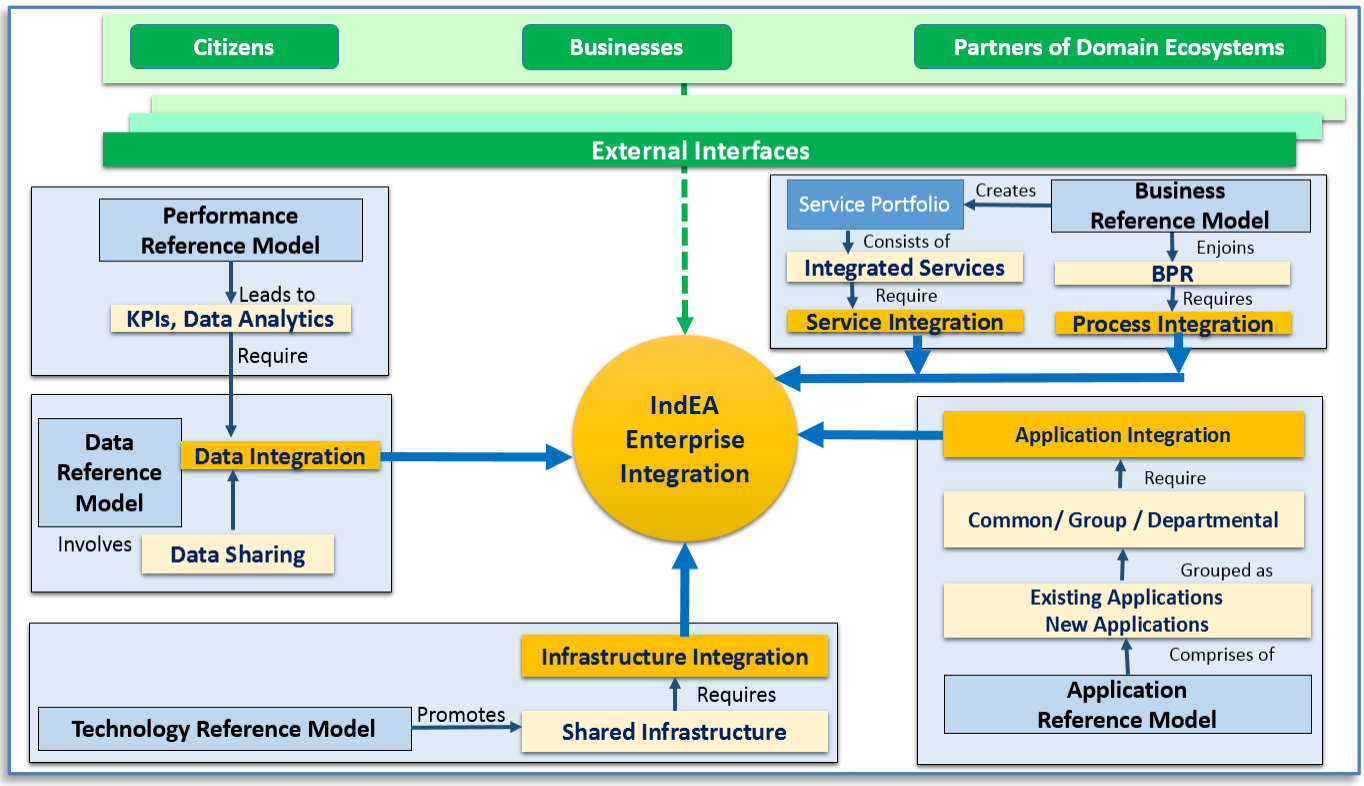


FIGURE 8.4: INTEGRATION REFERENCE MODEL (IRM) – LOGICAL VIEW

8.5. Enterprise Integration & Application Integration

The difference between EIA and EAI is more than semantic. EIA is a holistic *architecture* that takes into consideration the multiple dimensions of an enterprise represented in Figure 8.3. EAI, on the other hand, is a *technology* that addresses the sub-set of integrating a set of applications, which form a *sub-set* of the enterprise system. Having said that, it is necessary to mention that Application Integration forms, by far, the most important component in an implementation of EIA. Given this situation, the Application Integration Reference Model, which is an important sub-model of IRM, is dealt with in some detail in the subsequent sections.

Government IT Landscape:

Governments aspire to provide seamless service to all its stakeholders within a shortest time possible and in a cost-effective manner. The stakeholders can be individual citizens, business organizations, government departments, government employees, etc. These services are provided via various government departments their business functions. The number of departments in a state-government can vary from 30-70 departments. Most of these departments have automated their services to some extent resulting in development of silo applications. These applications have been developed over a period of time with then prevailing technologies. As a result of this, the application landscape is heterogeneous with limited integration. The key challenges of Government IT Landscape are:

1. Large number of stakeholders across different categories (individuals, businesses, etc.)
2. Presence of large number of applications developed by departments in silos and on different technologies.
3. Huge variation in the number of transactions for each service across different services.
4. Multiple access points for the services (Web Applications/ Mobile Applications/ Service Centers/ IVR, etc.)
5. Data security and confidentiality is a primary concern.
6. Remote parts of the country do not have access to internet and process related data has to be collected off-line which is subsequently uploaded.
7. Data dictionary is not defined for all the data elements leading to inconsistency.

Enterprise Application Integration:

Addressing these key challenges in the IT landscape of the government mandates the requirement of seamless integration of its applications to ensure interoperability and effective sharing of data. The key objectives of Enterprise Application Integration are:

1. Seamless integration of applications to deliver services effectively.
2. Scalability to address growth in service volumes.
3. Security of data exchanged and of the backend systems.
4. Ability to interface with different types of end-point devices, applications and data formats.
5. Support for multi-channel service delivery.

Approach to Enterprise Application Integration:

The Enterprise Integration Strategy is a strategically important and complex issue. There is no single and straight forward answer to the question whether to follow the ESB route or the API Gateway route. A large number of mutually conflicting factors impact the decision-making process in this aspect. **Table 8.1** gives a list of the major factors along with the preferred approach in respect of each of those factors.

In the context of the IndEA Framework, which is meant to be used by a Governments / Government Agencies, with well-functioning legacy systems, and with large aspirations for providing innovative services in a rapid manner, **it is necessary to adopt a dual approach namely, positioning the infrastructure for both the architectural styles, so as to cater to the widely varying requirements in the public sector landscape.**

Sr. No	Factors	ESB	API Gateway
BUSINESS CONSIDERATIONS			
1	Number of Business Domains & Business Processes to be integrated	Large	Low
2.	Number and size of Brownfield (legacy) applications, which need to be migrated to target architecture	Large	Small
3	Frequency with which business processes are modified	Less frequent	Frequent
4	Complexity of Business processes and business logic	Complex	Medium/ Low

5	Outreach / Number and Type of external interfaces	Low/ Fixed	Large number and great diversity of ecosystem needs
6	Desired Speed of Development	Slow/Medium	Fast
7	In-house technical capabilities	Weak	Strong
8	Model & Strength of Architecture Governance and IT Governance	Federated/ Medium	Centralized/ Strong
TECHNOLOGY CONSIDERATIONS			
1	Type of integration interactions (real time, synchronous, asynchronous)	Asynchronous, Not real-time	Synchronous, real-time
2	Number of services to be exposed externally	Large	Small/ Medium
3	Degree of Integration with IoT devices	Low	High
4	Deployment Strategy (cloud based / on-premise applications)	On-premise	Cloud
5	Protocol diversity in the existing / planned portfolio of applications	Large	Low/ Medium
6	Multiple layer of integration (Service/ Process/ Data/ Application levels)	Multiple Layers	Data / Application
7	Multiplicity of end-user access points (Web applications/ Mobile Applications/ Service Centers, etc.)	Low	Large

TABLE 8.1: ESB V/S API GATEWAY INTEGRATION FACTORS

Application Integration Platform acts as an Integration tool to connect various Systems and disparate Applications of the Government Departments. The State government has multiple departments and each department has multiple processes. There are some Applications used by the Departments/Agencies are running in siloes. Application Integration layer will connect these disparate applications. This will help to achieve seamless availability of Inter-departmental data, consistency of data, transparency etc.

The proposed Integration Reference Model (**Figure 8.5**) is of Hybrid Integration Platform so that it can integrate cloud applications and On-premise applications easily.

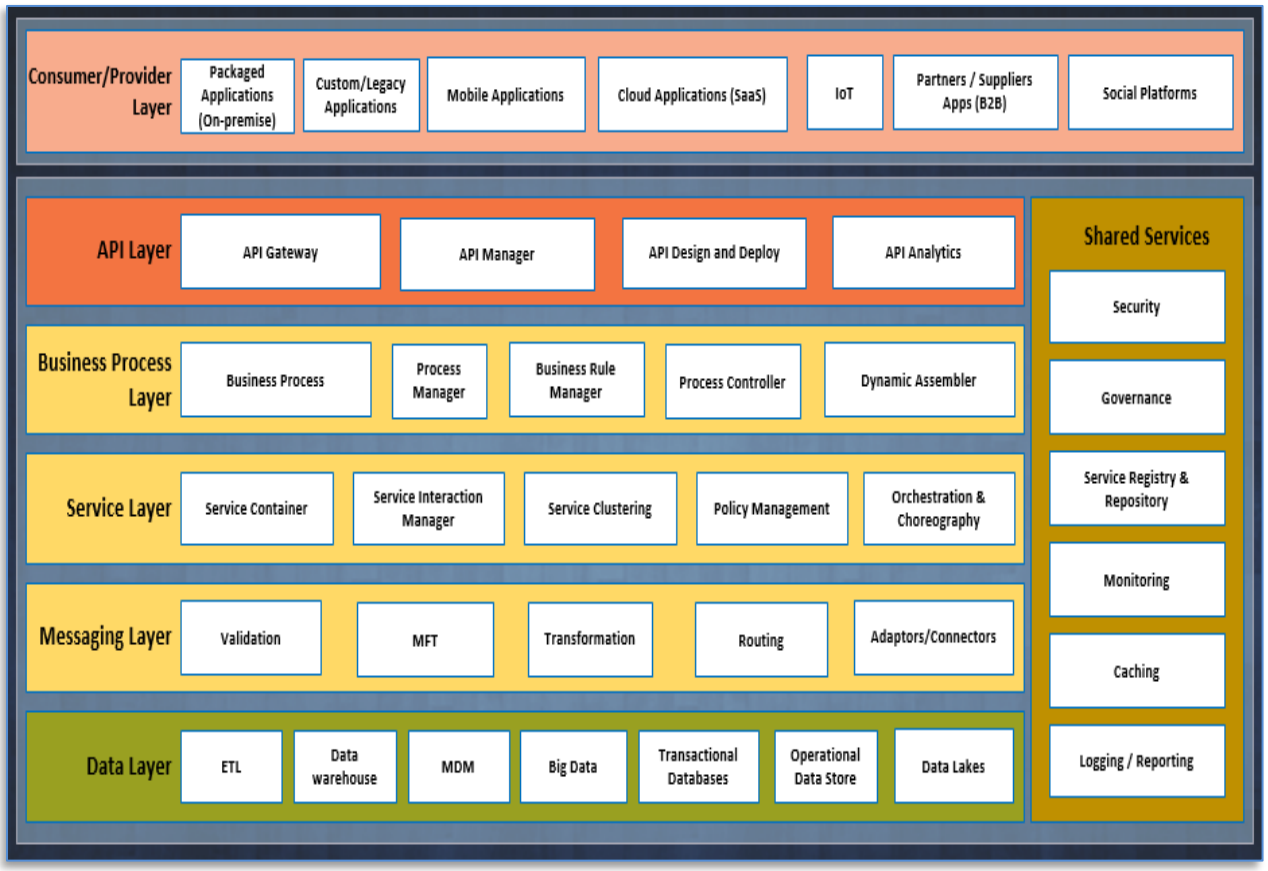


FIGURE 8.5: REFERENCE ARCHITECTURE FOR ENTERPRISE APPLICATION INTEGRATION

The model comprises of:

- **Consumer Layer/Provider Layer**: This is the entry point for all external consumers/providers. This can be any On-Premise Applications, Mobile Applications, IoT Devices, Partners/Suppliers' Applications or social platforms.
- **API Layer:** This layer comprises of API Gateway, API Manager, API Designer and API Analytics. This layer take care of API creation, API Management, Authentication & Authorization, API Analytics etc.
- **SOA/ ESB Layer:** This layer is comprises of Business Process Layer, Service Layer and Messaging Layer.
    - **Business Process Layer** covers process representation and composition, and provides building blocks for aggregating loosely-coupled services as a sequencing process aligned with business goals. Business processes represent the backbone of the flow of a business.
    - **Services Layer** consists of all the services defined within the SOA. Service clustering, Policy Management, Orchestration and Choreography will be done at this layer.
    - **Messaging Layer** takes care of transformation, routing, validation etc.
- **Data Layer:** This layer provide data level integration as well as access to all kind of data stores like Data warehouse, Big Data, Transactional databases, Operational data stores etc.
- **Shared Services layer** is cross cutting all these layers.

8.6. Integration of Legacy Applications

Legacy System/Application is an older version of the Application. The system can be out of date and may not supported by vendor. The main purpose of the keeping the Legacy applications is their data and the heavy cost to re-design or migrate the application. Nevertheless, the Legacy applications cannot be put in silos. They need to be integrated with other required systems/applications. The objective of Legacy application integration is to take advantage of information/data lying with the Applications.

Below steps provides the high level guidelines to integrate Legacy Applications:

- Analyze the existing Legacy Applications
- Design the Architecture following integration principles
- Choose the tools/technology to integrate the disparate applications
- Define the Interfaces.
- Complete the Implementation

8.7. IRM and Other Reference Models of IndEA

The overall Government Enterprise Architecture comprises of Business, Application, Data, Security, Performance and Technology Architectures. However, Integration Layer is one of important component of the Application Layer which ensures the information sharing between the disparate applications. At the same time, it gets input from other reference models. The interaction between IRM and other Reference Model is depicted below:

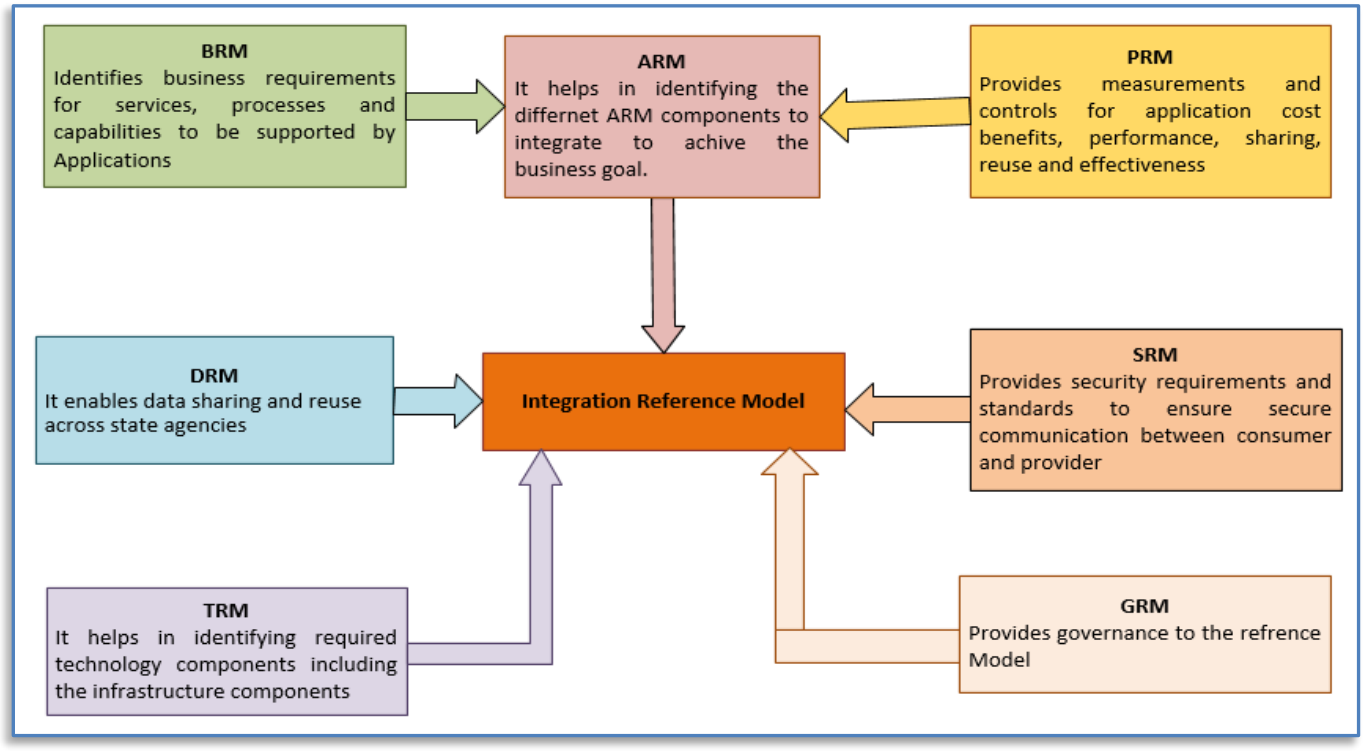


FIGURE 8.6: IRM AND OTHER REFERENCE MODELS

9. Security Reference Model

In the world of internet, governments are providing their services online accessible through web and mobile interfaces. This opens up an avenue for multiple threats to access the information, systems, and assets to be viewed and/or altered unauthorized to harm the services, applications or the organization. This poses a serious threat to e-Governance activity and points out to the importance of defining and implementing policies, processes, controls for information security.

Further, in this era of web and mobile world, online security is of prime importance and it should be considered even while conceptualizing any development. Security is not confined to a single level but needs to be addressed at business (defining security policies), infrastructure (appropriate configurations at network, data center, and hardware), application (Application deployment, OS hardening) and data (storage, access) levels. It is least costly and most effective to plan for and implement security-specific functions in the Target Architecture as early as possible in the EA development cycle to avoid costly retrofit or rework because the required building blocks for security were not added or used during systems development and deployment. The approach of the security architect considers not only the normal flow of the application, but also the abnormal flows, failure modes, and ways the systems and applications can be interrupted and fail. **Developing Enterprise Security Architecture concurrently with other Architectures is therefore of paramount importance.**

Security Reference Model (SRM) is a framework for developing a comprehensive and rigorous method of describing the current and future structure of the information security systems so that they align with the business strategies of the enterprise.

SRM specifies all the entities, policies and procedures, and their relationships. Integrity, privacy, confidentiality, and availability of information / IT systems are the key concerns addressed by SRM.

SRM adopts a **layered approach** for identifying and meeting the information security needs of the enterprise. The model identifies the security controls to be applied at **6 layers**, namely, the **Business Layer, Data Layer, Application Layer, Perimeter Layer, Network Layer and the End Point Layer**. SRM also touches upon the manner of designing **Security Policies** and **Standard Operating Procedures**.

9.1. SRM Objectives

The objectives of SRM are to:

a. Provide a structure, coherence and comprehensiveness to the design of security policies and security operations of the enterprise.
b. Enable a perfect alignment of the security strategies to the business strategies of the enterprise.
c. Ensure that all security models and implementations can be traced back to the business strategy and specific business requirements.
d. Enable the enterprise to undertake an assessment of security risks and threats to the information assets.
e. Provide a framework to identify Security Requirements of an enterprise at various levels and the approach to address them through appropriate systems and management.

9.2. SRM Concepts and Definitions

Concepts:

a. **Threat Modelling**[4]: Threat modeling is an approach for analyzing the security of an application. It is a structured approach that enables you to identify, quantify, and address the security risks associated with an application. Threat modeling is not an approach to reviewing code, but it does complement the security code review process. Threat Modeling also includes assessment of data being used in a way that can cause harm or damage to citizens and businesses by people within the government and outside, intentionally or unintentionally.

b. **Intrusion Detection System**[5]: Information systems used to identify that an intrusion has been attempted, is occurring, or has occurred.

c. **Intrusion Prevention System**[6]: Variant on intrusion detection systems that are specifically designed to provide an active response capability.

d. **Security Information and Event Management (SIEM)**: SIEM is an approach of security management that takes a holistic view of the organization's information technology security. SIEM systems provide quicker identification, analysis and recovery of security incidents.

Definitions:

a. **Authentication**: Authentication is the process of identifying user based on the credentials supplied by the user. The credentials are based on what the user knows or what the user possesses or what the user has.

b. **Authorization**: Authorization is the process of providing appropriate access permissions to the user. The user are authorized to access information only after appropriate authentication and as per the access permission rights.

c. **Data Loss Prevention:** DLP make sure that end users do not send sensitive or critical information outside the corporate network.

d. **Security Control:** Security controls are the measures to be taken to avoid, detect, control, counterattack or minimize the risk of information, physical infrastructure, computer systems or other assets compromise.

e. **Security Policy:** Security policy is a document that states how an organization or a company plans to protect its assets. The document addresses the constraints on behavior of the system users or administers, usage of infrastructure available.

f. **Security Procedures or SoP:** This is the manual that provides the steps to be followed at perimeter, network, and device layer to minimize the risk of security compromise.

g. **Security Event:** Security event is change in the daily operations related to network infrastructure or service that indicates the violation of security policy or security procedures. Security event may have significance on security of information, infrastructure, computer systems or other assets.

[4] Source: https://www.owasp.org/index.php/Application_Threat_Modeling
[5] Source: https://www.iso.org/obp/ui/#iso:std:56889:en
[6] Source: https://www.iso.org/obp/ui/#iso:std:56889:en

h. **Security Incident:** A security warning about a threat or violation that may have occurred and may be identified as an unauthorized access to a system.

i. **Vulnerability**: It is the weakness in the system, process or software that can be exploited to gain unauthorized access to information or assets. The unauthorized access to the system or assets of the organization may be misused.

j. **Threat:** Threat is a possible danger that can exploit to vulnerability of the system, infrastructure or application to cause harm to the organization or system functioning. Threats are usually classified as high, medium or low.

k. **Risk:** Risk is possibility of facing losses due to an event that probably may occur.

9.3. SRM Principles

Principle SRM 1: Data Integrity
Data is correct, consistent and un-tampered.

Principle SRM 2: Data Privacy and Confidentiality
Information is shared on a Need-To-Know basis and is collected/accessed/ modified only by authorized personnel.

Principle SRM 3: Secure by Design
Security has to be built into all stages and all aspects of architecture development. Security concerns extend to all the IT activities of the enterprise.

9.4. SRM Schematic

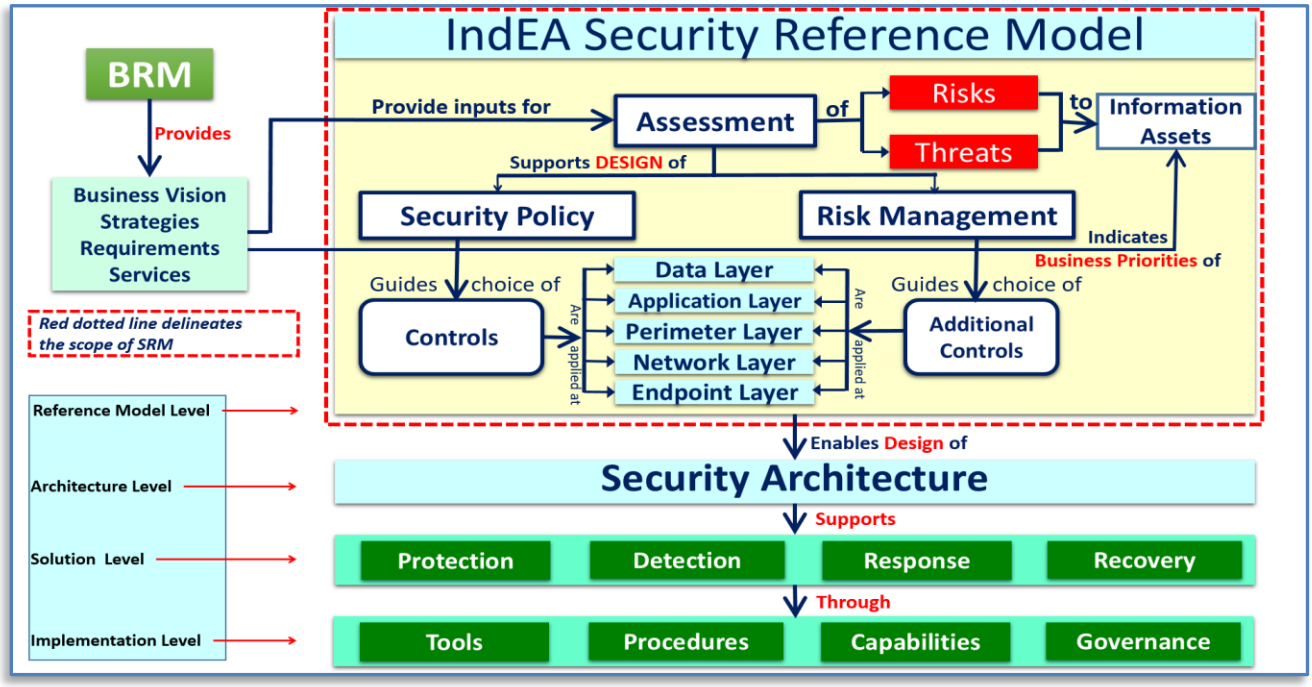


FIGURE 9.1: SECURITY REFERENCE MODEL

Figure 9.1 shows the Security Reference Model. The framework for selection of **Security Controls** is one of the most important aspects of SRM. The security controls are defined for each of the5 layers, namely Data, Application, Perimeter, Network and End-point. The security policies are defined basing on and in alignment with the business goals, given out by the BRM and the Business Architecture. A risk and threat assessment process guides the controls that are to be defined and implemented at each of the data, application, endpoint, peripheral and network layers.

The most important first step in defining the security policy is to **know what assets need protection**. Then the threats need to be identified as risks and to address these threats to protect the assets, secured procedures should be defined. Identification, analysis and management of the risk take place at the business layer and hence the outcome of the business layer is the policy document that should be converted to security controls at various layers. While designing any of the policies, all the IT, privacy, security, UIDAI acts should be taken into consideration. Continuous monitoring and analysis is also done at this layer. Various functionalities and the deliverables of this layer are covered in **Business Layer**.

Perimeter layer brings out the controls that are to be implemented on the infrastructure that is used to deploy the application or service along with its data. Perimeter can be the physical servers, applied zonal security such as DMZ, cloud infrastructure, perimeter devices in the data center. The objective for this layer is also to provide Standard operating procedures (SOP) related to data center. Regular monitoring and auditing is required of the physical assets. This layer also guarantees high availability and disaster recovery related controls are implemented at this layer. The details of this layer are covered ahead in **Perimeter Layer**.

The most important asset from a security perspective is data. Through peripheral layer we try to limit the unwanted access to the data from its storage location. However, when the data is transported between client and server or between two systems, the channel on which it is transported also should be ensured for security and privacy. The network layer of the architecture captures the security aspects from channel and network perspective. The network security also considers cyber security which is the biggest threat these days to the data privacy and security. Regular monitoring, auditing, SOP modification, policies related to the remote access become important aspect for this. The details of this layer are covered in **Network Layer**.

With the advent of mobiles services, applications are accessed through mobile devices and not only through the laptops, desktops or other systems. Security concerns for these devices are point of concern as the data leakage may take place here. Also with many biometric based authentication methods devices such as sensors capturing finger prints, IRIS is connected to the system to send these details to the service. Security at these end points is equally crucial and should follow the guidelines given for these end devices security. The controls related to anti-malwares, anti-virus software, compliance related to CIDR standards, access control mechanisms for device access are covered in this layer. The details of this layer are covered in **End Point Layer**.

Application layer contains the security controls related to the application deployment and its technology stack. Appropriate session management, best coding practice, use of secured channel for data transfer are some of the important controls that are to be implemented at this layer. Appropriate authentication mechanism based on the sensitivity of the application and authorizations are major features related to access control for application layer. The details of this layer are covered in **Application Layer.**

And finally, the most important is the data security that includes the security of the information stored in databases, spreadsheets, files etc. The storage, integrity, availability and access control are the important features related to the data layer. Security and privacy are the important aspects of enterprise security. The control to address the personal data security can be Identity management system, channel security, role based access control etc. The details of this layer are covered in **Data Layer**.

Figure 9.2 shows the layers of security architecture along with the different security functionalities covered in these layers.

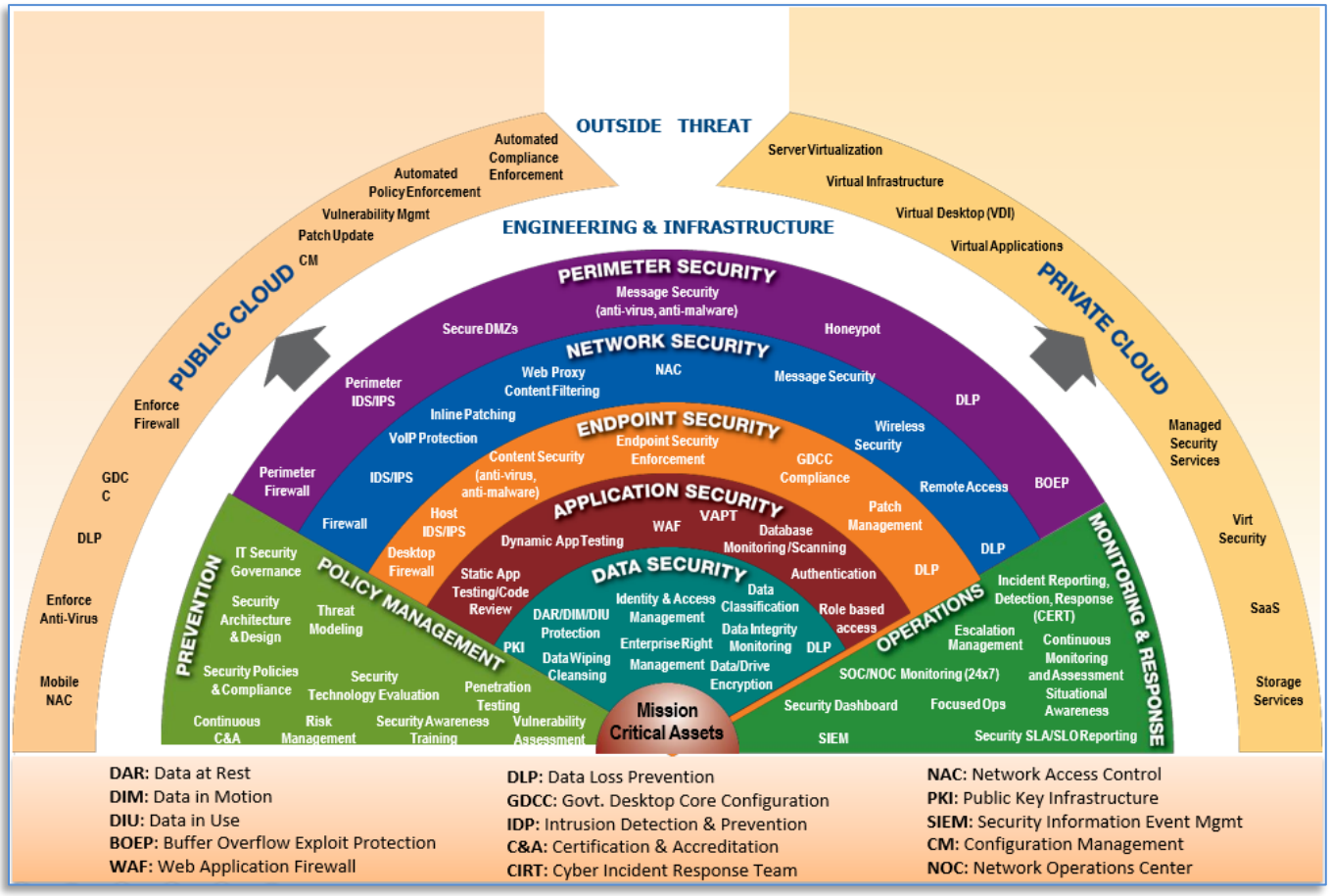


FIGURE 9.2: LAYERS OF SECURITY ARCHITECTURE[7]

9.4.1. Risk & Threat Management

Risk is possibility of facing losses due to an event that probably may occur. Risk has the following characteristics:

- Risk Factor – Something that may influence of occurrence of negative event

[7] Source: https://www.sto.nato.int/publications/.../STO-EN-IST-143/EN-IST-143-09.pdf

- Risk Event - Occurrence of a negative incidence that may result in loss of data, information or have a negative impact on system.
- Risk Reaction – It is the action to be taken when any negative event occurs.
- Risk Effect – Impact of the risk event on the system, organization or operations.

Risk identification can be done in two ways: through brain storming or through the existing checklist.

Top risks in software development are given in **Table 9.1** below:

Risk Factor	Preventive measures
Human error on part of staff	• Employ skilled best people; • Have a mechanism of appropriate rewards; • Have a process of peer reviews on regular basis; • Have capacity building programs to improve the skill set of the staff; • Build teams; • Adapt processes to available know-how
Unrealistic timelines or budget	• Choose approach of incremental development; • Adopt reuse of available software; • Modify the budget and schedule if necessary; • Do proper business case analysis
Use of incompatible standard or external components; or inexperience of standard software or external components selected	• Do the review of reference installations; • Do prototyping; • Do detailed compatibility analysis; • Have appropriate bench marking; • Review the suppliers; • Employ people with knowledge in the desired software or components; • Train the staff in the desired software or components
Problems with the tasks that are performed externally	• Have a regular audit schedule; • Form an internal team; • Parallel designing or prototyping should be done with different vendors

TABLE 9.1: TOP RISK FACTORS AND PREVENTATIVE MEASURES

Threat is a possible danger that can exploit to vulnerability of the system, infrastructure or application to cause harm to the organization or system functioning. Threats are usually classified as high, medium or low. General threats to IT systems and data include:

- Hardware and Software failure.
- Malware.
- Viruses.
- Spam, Scams and Phishing.
- Human error.

Risk management is the systematic process of identifying, analyzing and controlling risks. NIST 800-30 provides a guide for doing risk management. The purpose of risk management is to protect the system, assets, information and infrastructure from any kind of threat. A threat source can be internal or external and may have an impact on the overall functioning as well as business of the organization. In the current world, where cyberattacks are happening frequently, risk management becomes more crucial. While designing risk management plans and framework, one needs to consider needs of the organization, its objectives, context, operations, processes, products, services, assets, practices employed. Following are the steps involved in Risk & Threat Management:

Risk & Threat assessment:

Risk assessment is identifying patterns in the system that may lead to major vulnerability in the overall system. Objective of performing threat and risk assessment is to

- Identify the source of risk
- Risk impact analysis
- Cost associated with the risk
- Strategy which can be adopted to overcome the risk

Threat and risk assessment comprises of identification of threat and vulnerabilities. Then determine its likelihood and the impact of that risk on functioning of the system and / or on functioning of the organization. In order to do the risk assessment 9 basic steps should be followed:

STEP 1 – System Characterization

Identify boundaries of the IT systems along with its resources and information that constitute the system. This requires good understanding of system's processing and its environment. Hence first collect the information about hardware, software, system interfaces (internal and external communication), data, information, persons who are supporting IT system, system mission (includes processes performed), system and data criticality, data sensitivity. For an IT system under development, it is necessary to define key security rules and attributes planned for the future IT system. System design documents and the system security plan can provide useful information about the security of an IT system that is in development. To gather information about the system boundaries techniques like questionnaire, on site interviews, documents, etc. can be used.

STEP 2 – Threat Identification

Once the boundaries are identified, the task is to identify threat source. Threat source can be circumstances or events that can cause potential harm to the system. The source can be natural (floods, earthquake, tornado, avalanche, electrical storm, etc), human (events that are caused by human being intentionally or unintentionally such as cyberattacks, network attacks, insertion of malware, unauthorized access to the system) or environmental (long term power failure, chemicals, liquid leakage etc).

STEP 3 – Vulnerability Identification

Threats are usually associated with vulnerabilities. Below table shows a few vulnerabilities and threat pairs and action of threat.

Vulnerability	Threat	Threat Action

Terminated employees' system identifiers (ID) are not removed from the system	Terminated employees	Dialling into the company's network and accessing company proprietary data
Company firewall allows inbound telnet, and guest ID is enabled on XYZ server	Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the guest ID
The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system	Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities
Data center uses water sprinklers to suppress fire; tarpaulins to protect hardware and equipment from water damage are not in place	Fire, negligent persons	Water sprinklers being turned on in the data center.

TABLE 9.2: VULNERABILITY/ THREAT PAIR

To identify system vulnerabilities it is essential to identify the vulnerability sources, performing security testing through agencies like STQC or CERT-IN empaneled agencies, generating a security requirement list. In order to identify the vulnerability sources vulnerability analysis can be done, previous documents can be referred, audit reports, anomaly reports, security review reports, testing reports, vulnerability assessment and penetration testing (VAPT) reports can be used. It is recommended that security testing and certification like ISMS must be followed. Before deploying any system in the production environment its VAPT should be done.

STEP 4 – Control Analysis

After the identification of risks, threats and vulnerability, the goal is to design controls. The controls can be categorized as

- Preventive controls.
- Detective controls.

STEP 5 – Likelihood Determination

Likelihood rating is probability that a particular vulnerability may get exploited. The rating for likelihood is:

- High
- Medium
- Low

STEP 6 – Impact Analysis

The next step is to determine the adverse impact of the risk on the system and functionality of the organization. Impact analysis can be performed based on the sensitivity of the data and processes.

It should be seen that none of the SRM principals are compromised which means no loss of integrity, no loss of availability, no loss of confidentiality. Classify the magnitude of the impact into High, Medium or Low.

STEP 7 – Risk Determination

After knowing the threat and its impact, level of the risk should be assessed. A risk scale and risk matrix should be developed to measure risk. NIST 800-30 guidelines can be used to do this activity.

STEP 8 – Control Recommendations

Controls should be defined to mitigate or eliminate the identified risks. While recommending controls these factors should be taken into consideration- effectiveness of the recommended options, legislation and regulation, organization policy, operational impact, safety and reliability.

STEP 9 – Report Generation

The output of this risk assessment if a Risk assessment report that contains description of threats, vulnerabilities, measure of the risk, and recommendations on controls for different layers of SRM.
To avoid threats selection of proper secured technology for development is important. The details about the technology selection can be referred from TRM.

In order to reduce the risks that are brought out in the assessment report, senior management should try mitigation of the risk to minimize risks.

Risk (Vulnerability / Threat pair)	Risk Level	Recommended Controls	Action Priority	Selected planned controls	Required resource	Responsible team/ person	Start /end Date	Maintenance requirements / Comments

TABLE 9.3: TEMPLATE TO SAFEGUARD IMPLEMENTATION PLAN

The following standards have been referred for Risk Management:

- NIST 800-30 – It is a guide that defines for risk management for IT systems. The standard also provides the guidance in identification of threat and vulnerability identification. Details risk mitigation.
- ISO 27001 – Risk management was introduced in ISO 27001. The standard provides controls related to risk assessment and management.
- ISO 31000:2009 – It provides principles and generic guidelines on risk management.

Security Policy:

As shown in the security reference model, security needs to be addressed at multiple layers. A security policy should address all these concerns.

In order to implement the security policy various forms are required to be designed such as Security incident report. A possible template for a security policy document is given in **Annexure (VIII)**: Security Policy Document.
Security policy document is associated with all the layers of security reference model. Different controls at various layers are derived from the security policy document.

9.4.2. Business Layer

Based on the business requirements the state should develop policies and procedures to be followed to have the secured solutions. Risk assessment, stake holder identification, asset identification, requirement of every service and application, various standards and statutes followed by the state and at national level are required while designing security policies. At business layer management should do risk assessment followed by the impact

analysis of these risks to identify appropriate controls and define them in the security policy document. Risk and threat management given in the earlier subsections should be implemented.

Defining Policy

a. Develop the security policy to address threats and vulnerabilities.
b. Identify the resources to implement, monitor and update the security controls as per the defined policy.
c. Define the schedule regular testing and monitoring to maintain to ensure all time security.
d. Define the access controls at various levels such as data center, application, data, network, periphery layers.
e. Define authentication mechanisms at various levels as per the business requirements.
f. Ensure that the standards, acts, policies defined at the national and state level are incorporated in the document.
g. Define compliances related to the end point usage.
h. Define cryptographic standards to be followed along with the recommended key management policy.
i. The security policy document should be published and made available for ready reference for all the concerned.

Functionality at Business Layer

a. Security architecture and design
    i. A proper security architecture considering all the components as per the reference model should be in place and configurable design to meet the objectives of overall security of the enterprise.
b. IT security governance
    i. This comprises of formulation of guidance, structures, and processes for implementation of IT policy, risk, compliance, and audit functions.
c. Threat Modeling
    i. What are the threats and what can be its sources should be identified. In order to do threat modeling identification of assets and related vulnerabilities is crucial.
d. Risk assessment and management
    i. Assets should be first identified and then Inventory of assets should be maintained. Acceptable use of assets should be documented and ensured that it is implemented in every project.
    ii. Information should be classified as per its sensitivity and risk associated with the information such as data leak, privacy etc.
e. Vulnerability assessment and penetration testing
    i. Objective of carrying out the VAPT is an identification of vulnerabilities and possibilities of their exploitation. A policy should be defined by the departments to foresee the possible vulnerabilities and simulation of exploiting those vulnerabilities. VAPT is usually being discussed for exploiting the security of the application servers, network and the running application. However, it may also be seen for other layers as well such as possibility of spoofing in the installed biometric sensors which are being installed for the purpose of preventing the unauthorized access to the physical systems.
f. Security technology evaluation

i. Objective of security technology evaluation is to determine the degree of compliance with a stated security reference model, various controls, standards and specifications. For example Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security; Information Technology Security Evaluation Criteria by European Union for evaluating the enterprise security are being used extensively.

g. Continuous monitoring and analysis
   i. It is not only defining of the policies, standards or referring of the various international security standards but also to define the metrics which should be monitored and analyzed on a regular basis to achieve the required quality for security.

h. Security training to build awareness
   i. There is a need to develop a proper plan, policy to create the awareness, capacity building for achieving the desired security for an enterprise.

i. Incident detection and handling
   i. Purpose of incident detection and handling is to determine the possible attacks/threats to the overall system. Vulnerability at any level of the reference model can lead to the threat to the overall enterprise. There should be a mechanism to identify those vulnerability and the procedures to handle them. For example vulnerabilities related to network security, physical access to the systems, data access management etc.

j. Continuous certification and accreditation of policies
   i. The state should conduct the audit at regular intervals to verify the conformities. Agencies like STQC may be appointed for auditing
   ii. The objective of the audit should be made very clear to the auditors.
   iii. The report of the audit must be reviewed by the management for action and upgradation required.
   iv. Non-conformities identified during the audit should addressed and used for the corrective action as well as improvement in the policy.

k. Escalation management of security incidences
   i. All information security roles and responsibilities should be identified and allocated to the appropriate people.
   ii. Appropriate contacts with the relevant authorities should be maintained.
   iii. Maintaining a security dashboard

Business Layer Controls

Some basic controls related to the business layer are mentioned in this section. Some are also covered in **Annexure (VII) -** Controls at Security Layers. The list of controls defined in this document is not a complete list but a guideline. More controls should be defined at the state level based on identified requirements and threats to ensure the complete security. **Table 9.4** provides the list of essential controls at the business layer of the security model. For defining more controls the standards mentioned in 'Security Policy and standards' may be referred.

Objective: To limit the access to the information, data and facilities providing it.		
3.1.	Access Control Policy	• A policy should be established, documented and reviewed as per the business information security policy to provide access to information or assets available at the state/ organization/ department level. • The policy should define who can access what resources and what authentication mechanism should be used to provide the access. • Different multi-factor authentication mechanisms should be defined for accessing different information and information facilitating resources based on the sensitivity. • The principle of '**Least Privilege'** shall be followed, so as to give only the minimal permissions and authorizations to any user to enable him/ her to perform the specified functions.
3.2.	Strong password	• Policy should define what is an acceptable password. A strong password is recommended with minimum 8 characters, with at least one capital character, at least one numeric and at least one non-alphanumeric character.
3.3.	Professional/ company email id	• It should be mandated that for all the official work only the company / department email ID should be used. No government information is to be shared on personal email IDs. • The e-Mail policy of GoI contains such a stipulation.
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.		
3.4.	Incident reporting and handling	• A mechanism should be defined and made available to detect any security related incident. • A procedure should be well defined and documented giving steps to be taken for handling any incident.
3.5.	SIEM	• SIEM has two components, SIM (Security Information Management) and SEM (Security Event Management). It should provide real time analysis of the security alerts generated by network hardware and applications.[1] • A software information and event management system should be defined and documented for handling security related incidents.
3.6.	Learning from the security incidents	• Knowledge gained through analysis of the earlier incidents should reflect in the security policy document.
3.7.	Continuous Monitoring	• An institutional setup consisting of information security experts should be established for continuous monitoring that can help in detecting any security related incident. • The monitoring also includes the analysis of all actions and detection of the integrity getting compromised anywhere in the enterprise.
Objective: To ensure proper and effective use of cryptography to protect confidentiality, authenticity and/or integrity.		
3.8.	Policy for cryptographic	• The security policy should include the use of cryptographic controls to ensure confidentiality and authenticity of the user as well as systems.

	control usage and key management	• The security policy should document the secured use and storage of cryptographic keys. • The cryptographic keys should be changed at regular interval. The security policy should define the interval at which the keys are changed. The policy also should document the key generation mechanism to be used.
Objective: To ensure the integrity of the systems		
3.9.	Installation of software	• A secure procedure should be defined for installing software. • Rules governing installation of software should be defined and implemented. • Vulnerability Assessment and Penetration Testing (VAPT) should be mandated before installing any software in the production environment. Many of CERT-IN empaneled agencies do VAPT testing of applications. • Separate development, testing, staging and production environments should be recommended.

TABLE 9.4: CONTROLS TO BE DEFINED AT BUSINESS LAYER

SIEM:

Even after the risk analysis, identification of threats and providing controls, security breaches may happen. These are referred as security incidences. There should be a well-defined mechanism to detect such incidences and reporting of these. Such incidences are analyzed be professional bodies such as CERT-IN or if a state has state level CERT. The professional body after analysis of the incidence may publish advisory. The security policy should be modified as per the recommendations given in the advisory.

Updated security document should result in appropriate controls at various layers to prevent the re-occurrence of the incident.

Annexure (VII) - Controls at Security Layers provides many other controls that may be implemented at the business layer. In addition to these refer to the standards ISO/IEC 27001:13, Insider Threat security reference architecture, FEA – security model, Open Group standard- Open Trusted Technology Provider Standard (O-TTPS) version 1.1 for defining additional security controls.

9.4.3. Perimeter Layer

Access to any software is restricted first through the hardware where it is deployed. The environment in which the data and the application resides should be protected first. It is like having a lock to the house. Physical security is vital in order to protect the information and resources from unwanted access and intrusion. At state level the State Data Centres (SDC) provide the perimeter layer security. They should follow the design and policy given for SDC.

Functionality at Perimeter Layer

The main functionalities at the Perimeter layer are to identify the appropriate security for every asset, application / service and data. Based on the policies defined at the business layer regarding the access to various assets, the appropriate configurations at various levels should be done at this layer.

a. Secure DMZ – Design the network considering the sensitivity zones mentioned in 'Designing of Network'.
b. IDS/IDP – Intrusion detection and prevention at physical layer
c. Firewalls – to protect the infrastructure from unwanted or black listed intruders.
d. Message Security (anti-virus, anti-malware) – Appropriate anti-virus and anti-malwares should be identified and deployed. Policy regarding the same should be made to inform all the concerned.
e. Data Loss Prevention
f. Buffer Overflow Exploit Protection

Controls at Perimeter Layer

Table 9.5 gives some of the important controls that should be considered while designing the security at the data center. As per the policies and the requirement at state level additional controls should be defined and applied.

The controls mentioned in this section are more at generic level. They can be implemented by providing appropriate guidelines and defining SOP for Data centre access and usage. Safety measures can be applied at the entry door for the data centre, video surveillance through CCTV to monitor the access, defining emergency procedures etc. are to be detailed at the organization level.

Objective: Secure areas- To ensure that the information and the assets are not accessed, altered by unauthorized users through securing access to the physical infrastructure and the environment.		
6.1.	Physical Entry Controls	• Secure areas should be protected using appropriate controls. Not everyone should have access to the data centre. • A SOP should be defined for accesses to the data centre and different areas within the same. • A proper access control mechanism should be defined and implemented. • Multi-factor authentication is mandatory.
Objective: To ensure the protection of information and systems .		
6.2.	Security of network services	• Security mechanisms, service levels, and management requirements of all the network services should identified and included in the service level agreements.
6.3.	Avoid single point of failure	• In network paths between users and critical IT system resources, all the links, devices (networking and security) as well as the servers should be deployed in redundant configurations (also known as High Availability – HA).

TABLE 9.5: CONTROLS AT THE PERIMETER LAYER

Data centre may have physical servers or a cloud set-up. In the case of physical servers the controls related to access will be more crucial. The data privacy and security are more of a concern in the cloud set up.

Some of the important controls for physical servers and cloud set-up are also given in **Annexure (VII) -** Controls at Security Layers. Cloud related detailed controls can be found at NIST Cloud Computing Standards.

Cyber Intrusions and Security Controls

The rate of cyber-crimes has increased drastically as the usage of online applications through various channels is increased. Different techniques are applied to prevent the cyber-crimes which include the access control mechanism, providing only authorized access, putting restrictions on use of assets, applying different techniques to secure the data in storing or in transition, intrusion prevention systems etc. Still there remains the possibility of intrusion and it should be detected and then managed. For detecting such intrusions intrusion detection mechanisms are used at information level. Once the incident is occurred, it should be managed and the changes in the security controls should be done accordingly. Controls related to incident management are given below. Cyber security controls are required at perimeter, network as well as end-point layer.

Management of information security incidents and improvements		
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.		
6.1.	Responsibilities and Procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.
6.2.	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.
6.3.	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
6.4.	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
6.5.	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.
6.6.	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
6.7.	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

TABLE 9.6: CONTROLS RELATED TO CYBER INTRUSION

Audit

An internal audit should be conducted by the organization at regular intervals to monitor the security of the system and applications/ services. State/ organization should have well defined requirements and should conform to certain standard, and to ensure the conformance to various defined security policies and as preventive measure of prevalent security threats, a security audit should be performed.

a. Goal should be defined for the audit. For every audit criteria and scope should be well defined.
b. Organization should define a plan, frequency, method, and reporting structure for the audit. While designing the audit program importance of the process should be taken into consideration, results or reports of the previous audits should be considered.
c. While designing audit report the requirement of the management, its relevance to the management should be taken into consideration.
d. Various audit reports should be preserved for reference.
e. Selection of the auditors should be done impartially and the objective should be the prime concern of the audit.

Audit Considerations		
Objective: To minimize the impact of audit activities on the production environment.		
6.1.	Audit controls	Audit activities involving verification of systems in the production environment should be carefully planned to have minimum disturbance to the business or service.

TABLE 9.7: CONTROL RELATED TO AUDIT

While performing the security audit of services or infrastructure, the testing is performed on the production environment. Hence, it should be designed carefully that will not affect the services.

Recovery Strategy

Disaster recovery is an important aspect of information security. In the case of any natural or man-made threat, the earlier data should be made available.

Availability		
Objective: To ensure the availability		
6.1.	Availability of Information facilitating infrastructure	Information facilitating infrastructure redundancy sufficient to make the availability requirement of the application should be ensured.

TABLE 9.8: CONTROL RELATED TO DISASTER RECOVERY

Business requirement for the availability of the service/ application/ information system should be identified. In order to ensure the 24 X 7 availability a redundant infrastructure should be identified. This infrastructure should also be tested for failover mechanism.

9.4.4. Network Layer

Perimeter layer covered the storage aspect of the application, service or data. However, the data in transit needs to be secured through the network layer. Many functionalities at perimeter and the network layer are common.

Designing of Network

Network Security is critical for IT systems and their proper operations as most applications work in the networking environment and closely depend on network performance, reliability, and security. Improper network design can be very expensive i.e., loss of business, data loss, security breach, costs of network restoration, etc. Essential to network design is the security architecture that describes the network segmentation (i.e., security zones) and security layers (i.e., access control, intrusion prevention, content inspection, etc.).

Logical Network Segmentation

Network should be designed based on the trust level requirements of the application or the department or the service. While designing a network, first one should identify different trust level applications or systems.

a. Untrusted Zone (Internet / Outside Access) - It is the zone through which the organization/ department/ state connects to the outer world of internet through Internet Service Provider (ISP).
b. Low Trust (External) - The systems deployed in this zone should be tightly controlled and hardened to reduce the attack surface. External DMZ has systems that are exposed to internet for public access such as web servers, email gateways, FTP servers, web proxy servers, remote access servers.
c. Medium Trust (Enterprise/ Extranet) - The Enterprise zone is where end-user systems reside, including end-user workstations, printers, and VoIP Phones. Endpoint protection is a critical to limit the exposure of end-user systems to malware.

The Extranet zone connects with highly trusted third party business partners. Nonetheless, it is recommended that traffic between Enterprise and Extranet zones is monitored and filtered at the zone's perimeter to allow only approved traffic to enter and leave the zone. Systems in the Extranet zone will typically not abide by the organization's security policies. Therefore, it is important to perform a 3rd party risk assessment before establishing connectivity to understand their security posture and possibly strengthen perimeter defenses.

Functionality at Network Layer

Network layer ensures the channel security and has to implement the controls as per the security policy at the network layer.

a. Network Access Control (NAC) – Provide endpoint security technology, user or system authentication and security policy enforcement.
b. IDS/ IPS – IDS monitors a network or systems and identify malicious activity or policy violations while an IPS watches network traffic as the packets flow through it and identify suspicious activity, log information, attempt to block the activity, and then finally to report it.
c. Firewall - Prevent unauthorized internet users from accessing private networks connected to the Internet. Basically they do stateful packet inspection.
d. VoIP Protection - VoIP share the same infrastructure with traditional data network, therefore inherits all security problems from data network. VoIP does not have a dominant standard so far. Hence suitable measures should be taken for its protection.
e. Content Filtering - Screen and exclude from access or availability, Web pages or e-mail that are deemed objectionable.

f. Message Security - **Message security** uses the WS-**Security** specification to **secure messages**. i.e. ensure confidentiality, integrity, and authentication at the SOAP **message** level (instead of the transport level).
g. Wireless security – Prevent unauthorized access to network using wireless networks. Common protocols used are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).
h. Remote Access Security – Implement remote network ***access*** safely and easily to a wide range of users, and devices.
i. Data Loss Prevention – **DLP** make sure that end users do not send sensitive or critical information outside the corporate network. It also describes software / hardware products that help a network administrator control what **data** end users can transfer.

9.4.5. Endpoint Layer

Services or applications are accessed using laptops, desktops, mobile devices etc. In addition to these currently many biometric devices are used to capture fingerprints, IRIS of the users to authenticate them using Aadhaar. For digital certificates the crypto tokens are used. All these devices are referred as end point devices as these are used by the users. This section emphasizes on the end point device security.

Functionality at End Point Layer

End point devices should be protected from various threats. Below care should be taken to do so.

a. Desktop level firewall – Protect the integrity of the system from malicious software code, filter inbound and outbound traffic, and alerting the user to attempted intrusions. Should be enabled on every desktop in network.
b. IDS/IPS - HIDS monitors systems and identify malicious activity or policy violations while an IPS watches network traffic as the packets flow through it and identify suspicious activity, log information, attempt to block the activity, and then finally to report it.
c. Anti-virus and anti-malware – Every system should have latest and updated version of suitable anti-virus and anti-malware installed. It detect and destroy computer viruses , malware and other malicious software code.
d. Compliance with Govt. Desktop Core Configuration(GDCC) – Servers and Desktops in the network should comply to list of security settings recommended by GDCC.
e. Patch management – Security patches of various software should be regularly updated.
f. Data Loss Prevention - DLP make sure that end users do not send sensitive or critical information outside the business network. It also describe software / hardware products that help a network administrator control what data end users can transfer.

Controls at End Point Layer

Mobile Device		
Objective: To ensure the security use of mobile device.		
6.1.	Mobile device policy	There should be a policy defining the security measures for using mobile devices. The devices should be protected with anti-virus and anti-malwares.
Biometric Device		

Objective: To ensure data integrity and privacy in the use of biometric device .		
6.2.	Biometric device policy	Biometric database of Aadhaar is very frequently used to authenticate users for various activities. The devices that are used to capture the biometric information should be secured against the loss of data or illegal access to the biometric data. Aadhaar act should be followed while using these devices for Aadhaar based authentication.

TABLE 9.9: CONTROLS FOR ENDPOINT LAYER

9.4.6. Application Layer

The applications / services are deployed at state data center which is the production environment for the public access. To ensure the smooth running of the production set-up, maintaining a separate development, testing and staging environment is recommended.

a. The technology selection should be done to help providing better security along with the performance.

Every application should go through the vulnerability assessment and penetration testing before making it available in the production set up. VAPT is carried out by the CCA empaneled agencies. VAPT should be carried out on a regular interval and whenever any new patch or functionality is added or removed from the service / application.

Functionality at Application Layer

Below functionalities should be provided at the application layer to secure the service / application and its data:

a. Static testing and code review - Purpose of this type of testing is to identify the vulnerabilities without carrying out the actual execution of the code. Development or implementation team does this testing and provides the reports related to the same.
b. Dynamic application testing- Purpose of dynamic application testing is to determine the associated security vulnerabilities in the code by executing it. This helps to identify the security issues related to the complete production set-up including the exact version of the application and application stack.
c. Web application firewall: Firewalls at application level should be given consideration to prevent the attacks such as SQL injection, Cross Site Scripting (XSS), cross site request forgery etc.
d. Vulnerability assessment and penetration testing: Objective of carrying out the VAPT is an identification of vulnerabilities and possibilities of their exploitation. A policy should be defined by the departments to foresee the possible vulnerabilities and simulation of exploiting those vulnerabilities. Policy should address the guidelines VAPT at regular interval should be carried out to exploit the vulnerabilities associated with configuration changes at various levels, i.e. network, application server, database servers etc. Vulnerabilities assessment should also be carried out w.r.t possibility of execution of malware, viruses etc. and should be defined in the policy.
e. User Authentication: There should be a proper authentication mechanism being implemented in the applications for providing an access to the sensitive information to the users.
f. Database monitoring- Monitoring the application, database servers for their uptime, threats which are being observed
g. Role/ Rule based access: A proper authorization policy and rules should be defined to prevent the unauthorized access to the various areas of the application.

Controls at Application Layer

a. Applications should not be made public unless and until tested for security.
b. Regular audit should be conducted of application/service.
c. Avoid unwanted access.

User Authentication:

User should be authenticated with a strong authentication factor based on the sensitivity of the application / service as well as data. National level services like e-pramaan should be used for the purpose.

Application Access Control / User Access Management		
Objective: To ensure the authentic access to the systems and services / applications.		
8.1.	Registration and Deregistration	Only authorized users should be allowed to access systems and services. In order to identify the authorized users, a facility of registration and de-registration should be provided for every service. This will help enable the appropriate access rights.
8.2.	Access Provisioning	A formal access provisioning of the users should be implemented. It will assign or revoke the access rights for the users.
8.3.	Authentication Mechanism	Appropriate authentication mechanism such as password, OTP, Digital Certificate, PKI, Biometrics should be implemented for providing the access to the services. That access can be controlled based upon the data and service sensitivity and in accordance with the security policy of the state/organization/department.
8.4.	Secured Log-in process	Every service/ application can be accessed only through the secured log-in mechanism based on the chosen authentication mechanism as per the policy of state/organization/department.
8.5.	Password Management	Password management systems should be interactive and should ensure quality passwords. The password management systems should also be secured and should have a provision such that no password can be leaked.
8.6.	Access control to source code of the program	Access to program source code should be restricted.
8.7.	Management of Secret authentication information of the users	Secret authentication information of the users should be managed as per the state/organization or national policy. The information storage should comply with the acts related to storing secret information of the user.

TABLE 9.10: CONTROLS AT APPLICATION LAYER

Authorize:

Though the user is authenticated, she/he may not be authorized to access certain systems, data, information, services. Every information and information providing facility should be accessed only by its authorized users.

The access right usually are time bound and should be verified on a timely basis to avoid unauthorized access. The change in the business processes should immediately reflect into the authorization policy and implemented on priority to avoid unwanted access. For implementing authorization along with multi-factor authentication rule or role based access should be provided to the users.

Logging and Monitoring:

Objective: To record events to create the evidence.		
8.1.	Log creation	Events such as user activities, failures, exceptions, information security events, server, firewall, IT equipment transactions etc. should be recorded and maintained in the log format. System administrator, system operator activities also should be logged and protected.
8.2.	Protecting logged information	These log files are important evidences and should be maintained and also secured from hacking. Encryption mechanism can be used to protect log files from unauthorized access and tampering.
8.3.	Clock synchronization	The reference point for all the activities, events, logging is time and hence the clocks of all the relevant systems should be synchronized.

TABLE 9.11: SECURITY CONTROLS RELATED TO LOGGING AND MONITORING

API Security

It is possible to attack or leak the data in transit while calling the API and hence the API design is equally crucial when talking about security. The following care must be taken while designing API:

- Information required for routing or interpreting the contents of the packet should be part of header and should be appropriately tagged.
- The body of the packet should be encrypted and should not be easily accessible. User's personal identity information should be part of the body of the packet and not the header.
- Provide some default value for optional parameters/ tags.
- Only necessary information should be taken from the user and unnecessary information exchange should be avoided.
- Preferably no personal information should be shared as a part of response.
- API should be made available only on the secured channel.
- Access to API should be provided only to the authorized users.
- Whenever data is exchanged between two servers, it should be done only after proper white-listing of the IPs; requests should not accepted from any other IPs.
- Mobile apps which are open to public are particularly vulnerable. Sensitive or personally identifiable information should not be shared through such apps as the authenticity of the end user is questionable and also because mobile apps can be easily reverse engineered to retrieve the tokens etc. which are used to communicate with the server.
  Aadhaar APIs can be considered as a reference for designing secured APIs (Ref. https://uidai.gov.in/images/resource/aadhaar_authentication_api_2_5.pdf).

9.4.7. Data Layer

Data is the most crucial aspect of the security and should be protected in multiple ways.

- Classify the data as per its sensitivity level (Highly sensitive, medium sensitivity, not very sensitive). Appropriate methods should be chosen while storing the data in the data base, files, directories or any other mechanism. Based on the level of sensitivity the policy should be chosen for storing the data. Various mechanisms can be encryption, hashing, maintaining in clear text format. The storage location is also dependent on the sensitivity of the data.
- The access to any of the data should be provided through APIs or through proper authentication and authorization.
- The transport of data on various channels also should be ensured for security.

Functionality at Data Layer

a. Data needs to be secured when at rest, at motion i.e. in transit or in use – Every piece of data irrespective of its sensitiveness need to be secured against the threats of unauthorized access, data corruption or complete data loss Depending on the sensitivity and availability needs, methods should be applied to secure the data.
b. Identity and access management for data – The data should be accessible to only authorized persons, at appropriate time and only for the specified purpose.
c. Access Right Management – Access to data should be restricted by creating and applying a policy for every kind of data set. Data access policy will define the constraint for controlling the data access by its users. It will help in applying appropriate read, write controls over data elements.
d. Data Integrity monitoring – Data Integrity is as important as any other aspect of data security. If the correctness of data cannot be determined, it is almost same as data loss. In some cases having data with compromised integrity is more dangerous than having no data. Therefore mechanism needs to be applied to monitoring data integrity at various stages to enhance authenticity, reliability and availability of data.

The requirement results in the appropriate access control for data. Regular monitoring, logging, auditing of data is required. A backup plan should be prepared and implementation as per the plan should be ensured. A state data backup policy should be considered while defining the data back-up policy for the application or a service.

Data should be classified as per its sensitivity and the appropriate rights should be imposed for the modification of the data.

Controls at Data Layer

Backup:

Objective: To protect data against data loss.		
8.1.	Policy Creation	A backup policy should be created and documented to create the back-up of the data, information, system and software.
8.2.	Information Backup	Regular back up should be scheduled for applications, system, information and data as per the back-up policy. The back-up should be tested regularly to verify its integrity.

8.3.	Back up protection	Backups should also be maintained in the encrypted format to protect its integrity.

TABLE 9.12: CONTROLS RELATED TO DATA BACKUP

Personally identifiable information (PII)

Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

PII can be sensitive or non-sensitive. Non-sensitive PII is information that can be transmitted in an unencrypted form without resulting in harm to the individual. Non-sensitive PII can be easily gathered from public records, phone books, corporate directories and websites. Sensitive PII is information which, when disclosed, could result in harm to the individual whose privacy has been breached. Sensitive PII should therefore be encrypted in transit and when data is at rest. Such information includes biometric information, medical information, personally identifiable financial information (PIFI) and unique identifiers such as passport or Aadhaar numbers.

9.5. Security Standards

a. Security Reference Model (SRM) for IndEA is based on various security architecture standards. Insider Threat Security Reference Architecture (ITSRA), April 12 release of SEI providers the architecture proposed by SEI after studying about 700 cases related to the insider crimes. This reference architecture uses Federal Enterprise Architecture as well as NIST Enterprise Architecture Model.
b. ISO/IEC 27001:2013, ISO/IEC 27002 are referred for defining the control objectives and controls. These standards are followed in the organization for defining, implementing and monitoring information security at various levels. The standard elaborates on the controls at management, user access control, key management and cryptography, human resource management, system and application access etc. It is best practice to follow the controls given in these standards to ensure the information security in systems, application and information facilitating assets in the organization.
c. ISO/IEC 27002 is referred as a guideline while designing this document. The standard also provide guidelines to design controls for organization specific security requirements.
d. NIST SP 800- 30 is referred for defining risk assessment and risk management.
e. Cloud Security Standards by cloud standards customer council is referred for providing suggestions regarding controls for cloud environment.

9.6. SRM and Other Reference Models of IndEA

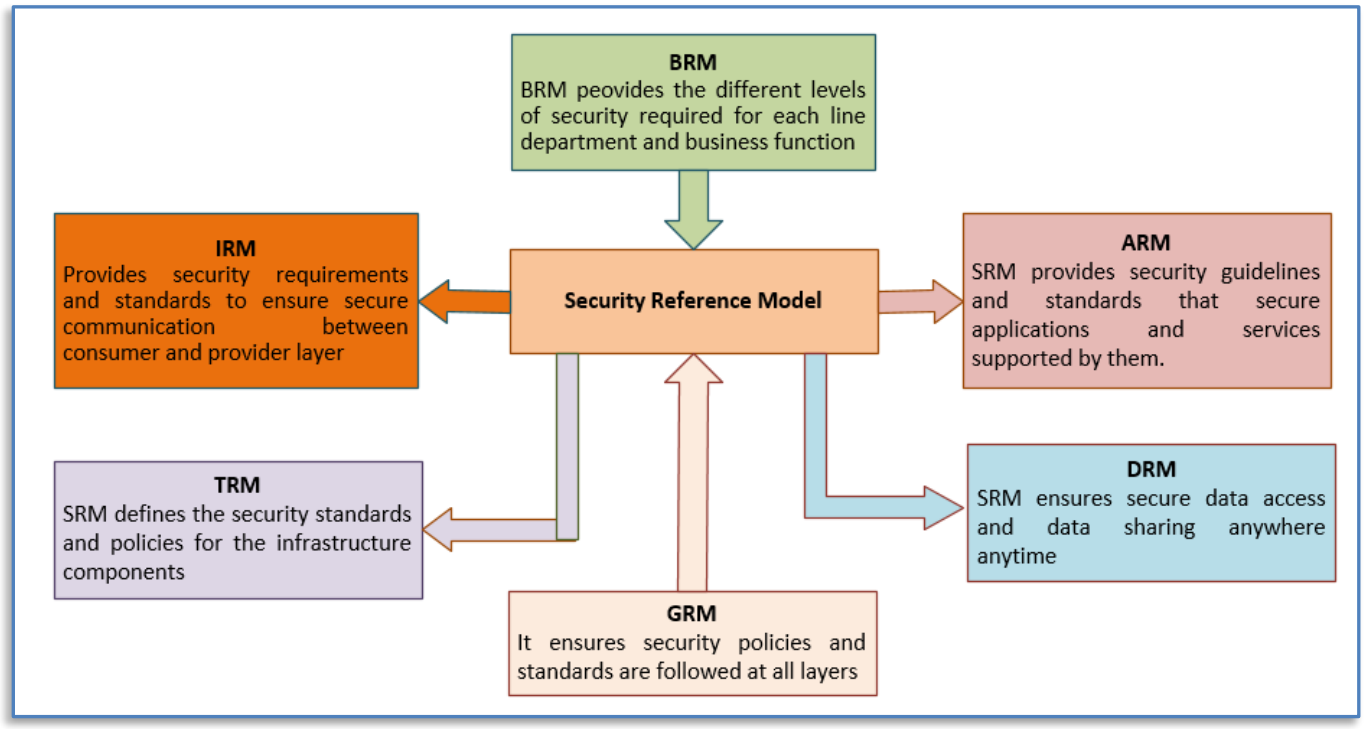


FIGURE 9.3: SRM AND OTHER REFERENCE MODELS

SRM and TRM:

SRM defines the security standards and policies for the interface devices, applications, data, network components, etc. It provides inputs in terms of standard policies and guidelines. It also specifies Audit policies and incident reporting requirements.

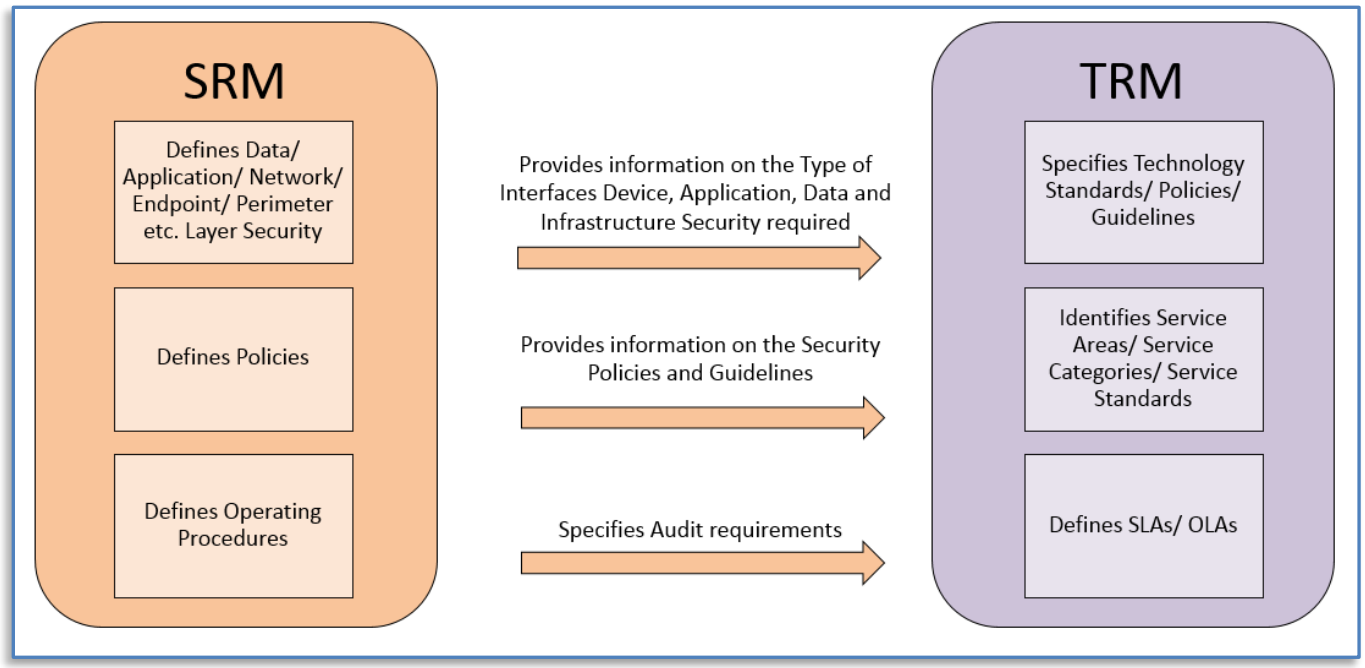


FIGURE 9.4: RELATIONSHIP BETWEEN SRM AND TRM

9.7. Developing Enterprise Security Architecture from SRM

The SRM delineates the overall framework for providing information security to the entire gamut of IT systems in the enterprise. Integrity, privacy, confidentiality, and availability of information / IT systems are the key concerns addressed by SRM. SRM adopts a layered approach to identifying and meeting the information security needs of the enterprise. The model identifies the security controls to be applied at 6 layers, namely, the Business Layer, Data Layer, Application Layer, Perimeter Layer, Network Layer and the End Point Layer. SRM also touches upon the manner of designing Security Policies and Standard Operating Procedures, and provides reference to various security and related standards like ISO 27001, ISO 27002, NIST and Software Engineering Institute (SEI).

Developing the security architecture (the target view) should start with defining security architecture principles. The IndEA SRM provides principles covering Risk and CIA (Confidentiality, Integrity, Availability). The impact of Cloud and SOA on security also needs to be covered. For further details, please refer to 'IndEA Adoption Guide – A Method Based Approach'.

10. IndEA Governance Reference Model (GRM)

Architecture Governance Reference Model (GRM) guides in establishing an institutional structure for the development, management and maintenance of Enterprise Architecture and its artefacts. GRM also defines the processes and structural relationships to ensure that the architecture is consistent with the business vision and objectives of the enterprise and is implemented in strict compliance with the architectures developed. Effective and efficient EA Governance ensures that priorities are based on broad consensus across the enterprise. EA is a continuous activity and governance is an integral part for its successful implementation and maintenance.

10.1. Objectives of IGRM

The Objectives of the EA Governance are

a. To ensure the effective **introduction, implementation, and evolution of architectures** within the organization;
b. To ensure **compliance** with internal and external standards and regulatory obligations;
c. To establish **processes** that support fulfilment of the above objectives
d. To develop **practices** that ensure accountability to a clearly identified stakeholder community, both inside and outside the organization

Right governance model provides many benefits, including the following:

a. It ensures that the proposed architecture meets the overall vision and objectives of the Government.
b. It facilitates clear and quick decision-making on complex issues by bringing in transparency and accountability
c. It brings clarity in roles and responsibilities through management oversight
d. It preserves architectural coherence by weaving in a compliance culture
e. It keeps architecture relevant and useful in a pragmatic manner
f. It promotes architecture thinking in the Government

Enterprise Architecture Governance is not a one-time responsibility, nor is limited to specific projects or to any Government agency. It is an on-going, iterative process which provides:

a. Common vision of the future shared by the Line Departments and IT
b. Guidance in the selection, creation and implementation of solutions driven by requirements
c. Support for the various line departments through improved information sharing – provides plan for the integration of information and services at the design level across line departments
d. Consistent process for creating new systems and migrating old systems
e. An approach for the evaluation, consideration and assimilation of new and emerging technology innovations to meet the requirements

Lack of architecture governance may result in non-standardized technology / product selection / purchasing / development, inconsistence architecture that may lead to building Silo Applications. These will have a long term financial and operational impact and will create issues related to integration, collaboration and standardization which will be further difficult to manage and maintain at the enterprise level.

10.2. GRM Concepts and Definitions

Concepts:

a. **Architecture Governance**: Architecture Governance is the institutional mechanism, along with defined roles and responsibilities, for the development and maintenance of Enterprise Architectures within an organization, besides the review of compliance.
b. **IT Governance**: IT governance is the institutional mechanism, along with defined roles and responsibilities, that links IT resources and information to enterprise goals and strategies and institutionalizes best practices for planning, acquiring, implementing, and monitoring IT performance, to ensure that the enterprise's IT assets support its business objectives.
c. **Conformance**: Conformance is the **degree** of compliance of a specific IT Project to established architectural principles, criteria, and business objectives
d. **Compliance**: Compliance is adherence of a specific IT project to established architectural principles, criteria, and business objectives. In a **fully-compliant** project, all the specifications conform fully to the specification and there are no more or less features than are specified by the architecture.

Definitions:

a. **Architecture Development:** is a method for developing and managing the lifecycle of an enterprise architecture to meet the business and IT needs of an organization. It is an iterative and cyclical process starting with development of the Vision and going through development of various component architectures and establishing a mechanism for governing and implementing the architecture.
b. **Architecture Capability:** is an ongoing practice that provides the context, environment, and resources to govern and enable architecture delivery to the organization. The capabilities required for the Architecture practice vary with the phase of development of the architecture, starting with the development of vision and going through Business, Application, Data and Technology Architectures of EA and its implementation thereafter.
c. **Architecture Capability Maturity** (ACM): is a measure that indicates the organization's ability to execute the different phases of Architecture Development and Implementation, and the practices on which the organization needs to focus in order to see the greatest improvement and the highest return on investment. ACM has typically 6 levels [namely – 0 (none); 1 (initial); 2 (Under development); 3 (Defined); 4 (Managed) and 5 (Measured)]. ACM operates across 9 architectural elements namely
    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 and 9. IT investment and acquisition strategy
d. **Architecture Contract:** is the agreement between development partners and sponsors on the deliverables, quality, and fitness-for-purpose of an architecture and are enforced through effective architecture governance.
e. **Architecture Repository:** is a framework that allows an enterprise to distinguish between different types of architectural assets that exist at different levels of abstraction in the organization and at different phases of the Architecture Development, and include 6 classes of architectural information, namely,

Architecture Metamodel, Architecture Capability, Architecture Landscape, Standards Information Base, Reference Library and Governance Log.

10.3. IGRM Principles

Principle IGRM 1: Primacy of the Principles

Statement: The principles of enterprise information management apply to all organizations in Government.

All the Government organizations implementing IT Projects shall, without exception, adhere to all the EA Principles in letter and spirit. Implementing the set of principles in part or not at all by some organizations would lead to failure to realize the vision and benefits of Enterprise Architecture. In other words, partial implementation of the principles is of no avail.

Principle IGRM 2: Discipline

Statement: All stakeholders of EA Governance structure need to follow the discipline of conformance to the principles and standards.

All stakeholders involved in the development, implementation and deployment of Enterprise Architecture have commitment to adhere to the procedures, processes, and authority of the Governance Structures established by the Government.

Principle IGRM 3: Transparency

Statement: The architectural decisions taken are transparent to all stakeholders.

The decisions taken in the course of design and development of all architectures are visible to all stakeholders, along with the reasons for adopting a particular pattern, specification or design, when alternative options are available.

Principle IGRM 4: Accountability

Statement: Stakeholders, including service providers are accountable for the responsibility assigned to them in the Architecture Development and Implementation, and in strict adherence to the EA principles.

Enterprise Architecture is a collective effort and would succeed in achieving its vision, only of all the members of the 'EA Team' are made full accountable for the decisions and actions taken by them.

10.4. IGRM Schematic

Figure 10.1 provides an overview of the GRM. It is built basically on the 3 pillars, namely the Government, The Architecture Governance Board and the IT Governance Board.

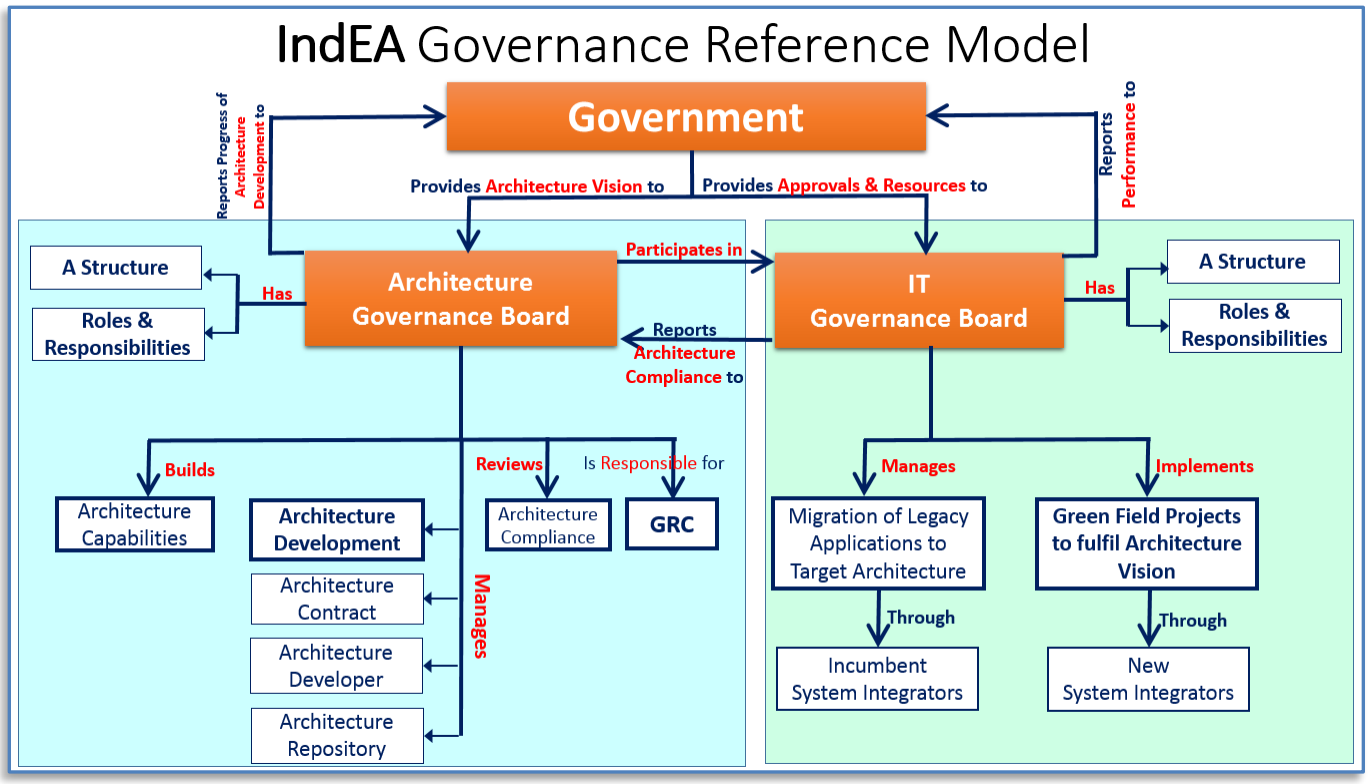


FIGURE 10.1: ARCHITECTURE GOVERNANCE REFERENCE MODEL

IGRM Explained

The structure of IGRM can be understood in the following manner

1. Architecture Governance is based on the 3 main entities, which act as its pillars. These are the Government (the Sponsor), the Architecture Governance Board (the 'Thinker'), and the IT Governance Board (the 'Doer').
2. Each of the 3 entities have their own defined roles and responsibilities, broadly indicated in the Figure 10.2, and is empowered sufficiently to discharge the roles effectively.
3. 'Undue interference' of any entity with the functioning of any other may result in unsatisfactory consequences, including non-realization of the vision of the sponsor, the architecture exercise going on endlessly and the implementations being non-conformant to the designed architecture.
4. Architecture Governance Board is concerned with development and management of the Enterprise Architecture. IT Governance is responsible for its implementation either through a process of migration to the target architecture or through fresh development of greenfield projects or a combination of both.
5. Both the Governance Boards should be small (say, 6 to 7 members) but represented by all *key* stakeholders.
6. The projects and works undertaken by the IT Governance Board are subjected to Compliance Reviews by the Architecture Board.

7. The Figure 10.1 provides a framework for establishing a Governance Structure by any enterprise undertaking an EA initiative. The nature of the entities, their specific roles and responsibilities have to be defined in the context of the specific environment and requirements of the enterprise.

10.5. Roles & responsibilities of key actors in Architecture Governance

While the actual ground level details of the Architecture Governance have to be defined in the context and setting of any enterprise, certain roles, mainly in the category of Architects can be defined in common. These roles are those of

a. Chief Enterprise Architect
b. Enterprise Business Architect
c. Enterprise Application Architect
d. Enterprise Data Architect
e. Enterprise Technology Architect
f. Enterprise Security Architect

10.6. Importance of Communications in Architecture Governance

Critical to the success and effectiveness of EA Governance, is a communication plan that lays down the processes relating to **Why**, **How**, **When**, and **With Whom** communication need to take place. For any enterprise architecture communication to be effective, it must be integrated with its core processes and structure. To achieve this, a robust architecture communication framework is required.

EA Communication Objectives

The objectives of the EA communication plan are as follows:

a. To build the awareness about the significance and vision of EA among all the participants/stakeholders
b. To obtain feedback on specific aspects of EA artefacts
c. To provide a clear, consistent representation of Enterprise Architecture
d. To facilitate collaboration
e. To educate all stakeholders on their roles and responsibilities
f. To educates all stakeholders on the EA metrics on a monthly, quarterly or as needed basis

EA Communication Tools

Tools used for EA communication are listed and described in **Table 10.1**.

Sr. No.	Communication Tools	Details
1	**Knowledge Management Portal**	Knowledge Management (KM) Portal is used to illustrate linkage of Government objective to EA. It demonstrates the linkage of IT projects to EA. KM Portal communicates EA Processes, Standards, Reference Models etc.

Sr. No.	Communication Tools	Details
2	**IndEA Repository**	IndEA Repository acts as the central repository for EA artefacts such as: • Reference Models • Principles and Policies • Business Architecture • Application Architecture • Data Architecture • Technology Architecture • Security Architecture
3	**EA Training**	Training on Enterprise Architecture
4	**EA Printed Documents**	EA Printed documents communicate following: • EA framework overview and its benefits • EA Dashboard with key EA Metrics • Roles and Responsibilities
5	**Emails**	Communication over email about Enterprise Architecture
6	**EA Short Videos**	EA Short Videos communicate following: • EA short Videos covering EA framework overview and its benefits • Discussions on Enterprise Architecture
7	**EA Workshops/Seminars**	EA Workshops/Seminars communicate following: • EA Overview and Benefits • Case Studies and success stories on Enterprise Architecture

TABLE 10.1: LIST OF COMMUNICATION TOOLS

10.7. Strategic Control in IT Governance

An EA initiative necessarily entails implementation of large, complex and centralized IT projects so as to translate the vision of the Architecture to reality.

Large e-Government projects are increasingly being implemented on a PPP Model that contemplates sharing of risk and control between the Government and the Service Provider (SP) appropriately and in such a way that risks are allocated to that party, which is best suited to manage it effectively. Among other risks, Government has to share the risk of answerability for exact compliance with the statute, besides ensuring provision of services in an uninterrupted manner. Against this scenario, it is required to design framework of Strategic Control by Government over the project.

In operational terms, Strategic Control over an IT-based e-Government system translates to the possession and exercise of appropriate privileges to ensure that (i) the system has been designed and established in exact conformance to the applicable statute and the enterprise architecture initially, by the technical team of

Government associating itself with the design and development phases and (ii) any changes to the system are authorized by a set of Government Officials, specially empowered to exercise those privileges.

A framework aiming to design and establish Strategic Control should basically address the requirements of 4 distinct areas of the e-Government system, shown below:

- Application System
- Database System,
- Network System and
- Security System

It is important to note that all the aspects of Strategic Control with respect to each of the above areas shall be applicable to the entire e-Government System environment including all its units i.e. Data Center, Disaster Recovery Center, Service Centers, Back Offices, and Call Center.

A Framework for Strategic Control is described in **Annexure (VIII) - Framework for Strategic Control**.

It is necessary for the Enterprise Architecture Team and both the Governance Boards (Architecture and IT) to assess the requirements of the Target Architecture in terms of strategic control and design an appropriate set of Strategic Control requirements for the portfolio of EA Projects.

11. IndEA Implementation Approach

11.1. From Framework to Architecture to Implementation

The essence of IndEA is adoption of a holistic approach in reimagining government and designing appropriate architectures that are consistent, interoperable, future-proof and facilitate a boundary-less information flow for delivery of services efficiently. The IndEA journey, by its very nature, will be effort-intensive and time-taking. Given that there are very few successful implementations of Enterprise Architecture globally, especially in the public sector, embarking on the IndEA journey enjoins several conditions precedent be satisfied. There are several risks inherent in the exercise. While establishing a ONE Government eco-system is the avowed goal of IndEA, the route to reach the goal has to be carefully planned and delineated so as to mitigate the risks and to derive the maximum benefits of an enterprise approach. In this chapter, an attempt is made to provide guidance on creating a high-level implementation plan that factors the risks and enables a steady progress in crossing the various milestones.

There are four major milestones to be crossed in the IndEA journey – assessing the capabilities and readiness of the organization for undertaking an EA initiative and, subject to a positive result, customizing the IndEA Framework for the domain / enterprise being addressed, converting the Reference Models into a set of Architectures and finally implementing the Enterprise Architecture in a closely coordinated and sequenced manner.

11.2. EA Capability Assessment

EA Capability Assessment involves measuring the capabilities of the enterprise along four dimensions – **People, Process, Technology and Resources**.

The assessment on the **People Dimension** is meant to assess whether there exist an overarching political desire and an executive capacity to undertake what obviously is likely to be an arduous journey, and the persistence to overcome problems *en route*. The need is for highly motivated multi-sectoral team consisting of (i) senior administrators with an understanding of technology in general and the principles of Enterprise Architecture in particular; (ii) senior enterprise architects with an experience in having implemented large transformation projects for the public sector; and (iii) senior program managers.

The assessment on the **Process Dimension** is about knowing the readiness of the organization to take game-changing decisions, adopting global best practices, a keenness to enhance the citizen-centricity, efficiency and transparency and above all, an eco-system empowered to take quick decisions in the overall interests of the EA program. The sponsors should be aware that the process for making significant process changes can itself be tedious and can potentially retard the progress, wear out the people and kill the initiative altogether.

The assessment on the **Technology Dimension** involves gauging the technological maturity of the enterprise, in terms of the availability of enterprise-wide infrastructure and systems, well-established network of service delivery channels and a clear roadmap for adoption of emerging technologies. A high score on the e-Government Development Index is a favorable condition.

The assessment on the **Resource Dimension** is looks at the existing budgetary resources, the recent trends of IT spend of the organization and the political commitment to provide the necessary budget support as needed.

An overall score of 70% in the capability assessment augurs well for the success of the EA initiative. This does not mean that the other enterprises scoring less cannot undertake an EA initiative. It is just that they have to strengthen the capabilities along all the four dimensions as an immediate first step. They have also to start with a reasonably small canvas in defining the scope of the proposed EA initiative.

11.3. Customizing the IndEA Framework to the Enterprise

IndEA Framework is generic by design. It cannot be used straightaway by any enterprise. The framework has to be customized to fit the broad requirements of the business vision and objectives of the enterprise. The following questions need to be addressed to enable such customization. A consultative process has necessarily to be followed.

1. What is the business vision proposed to be supported by the EA initiative?
2. What are the major stakeholder groups to be targeted?
3. What are the top services to be designed and delivered?
4. How many brownfield applications/ services exist that can be leveraged to form part of the EA?
5. How big should the big picture of EA be?
6. What is the timeframe in which tangible results of EA have to be demonstrated?
7. What is the budget available?
8. Do we have the technology expertise/ resources to undertake the exercise?
9. Is the enterprise positioned at the national, state or local government level?

Responses to the above questions enables the EA team to decide upon the scope, scale, timeframe and resource requirements of the effort. The IndEA customization exercise should result in a significant clarity on the following aspects.

1. Verticals, Horizontals, Applications and Services prioritized for the EA initiative.
2. Major Components of the Core Platform
3. Categorization of major applications as Common, Group and Domain-specific applications
4. Number, nature and depth of performance parameters
5. Sub-set of IndEA principles to be observed and enforced mandatorily
6. Sub-set of IndEA standards to be observed and enforced mandatorily
7. List of artefacts to be generated in the design and development of the Architecture
8. Granularity of the design & documentation of the architectural artefacts
9. List of legacy applications to be leveraged
10. Software development methodology to be adopted
11. Procurement Policy
12. Areas requiring BPR on top priority
13. Cloud adoption strategy
14. Integration goal and model
15. Size of governance structure and PMU
16. List of quick wins and game-changers to be targeted
17. High-level roadmap for implementation considering the above factors.

It is an absolute necessity at this stage to conduct an **EA Vision Workshop** such that the choices made on the above issues meets with the requirements of consultation, inclusion and aids general acceptance and broader ownership of the EA initiative.

11.4. Converting IndEA Reference Models to corresponding architectures

The Reference Models of IndEA are abstract by nature and cannot be made use of directly. The RMs provide guidance for the design of the detailed Enterprise Architectures. Each Reference Model leads to a set of Artefacts that form the basis for the next phases of procurement and application development. The **Table 11.1** provides a partial list of artefacts and outputs that have to be derived from each of the 8 reference Models.

Sr. No.	Reference Model	Resultant Artefacts/ Outputs
1	Performance Reference Model	- Outcome Indicators - Output Indicators - Economy Indicators - Measurement Processes - Integration Plan with BRM, ARM & DRM
2	Business Reference Model	- Scope of EA Initiative (Horizontals & Verticals) - IndEA Vision Document - Service Portfolio - Service levels - Service Delivery Infrastructure Plan - Re-engineered Processes
3	Application Reference Model	- Application Portfolio (Big Picture) - Integration Plan for Legacy Applications - High-level design of Quickwin and Game-changer Applications - Detailed design of Core Platform - High-level Functionality of the modules & sub-modules of Applications - Use Case diagrams for major processes - **Templates** for functional & system requirements specification documents, customized to IndEA needs
4	Integration reference Model	- Requirements Specifications of the Integration Platform - Application-Integration method Matrix - High-level design of Integration Operations Centre
5	Data Reference Model	- Core data - Meta Data of Core Data - Data Standards - Principles of data Sharing - Architecture of Core Data - Data Security & Privacy
6	Technology Reference Model	- Catalog of Technology Standards

Sr. No.	Reference Model	Resultant Artefacts/ Outputs
		- Cloud Adoption/ Migration Strategy - IT Infrastructure Roadmap - Policy on Open Source Products - Open API Strategy & Gateway Specifications - MicroServices Architecture
7	Security Reference Model	- Standard Controls to be applied at 6 layers - Security Policy for IndEA initiative - SoPs for IndEA initiative
8	Governance Reference Model	- IndEA Governance Structure (3-Tier) - RACI Matrix - Procurement Policy for IndEA initiative - PMU Structure - Funding Model - Industry Consultation Strategy - Stakeholder Consultation Strategy - IndEA Tools

TABLE 11.1: INDICATIVE LIST OF ARTEFACTS

The above is the list of minimum set of artefacts that need to be developed as part of IndEA initiative taken up by any State. The list can be abridged for to some extent for smaller organizations like local governments and small Ministries.

Conversion of the Reference Models to Enterprise Architectures necessarily involves significant effort especially in compiling information and data specific to the enterprise. Once this major hump is crossed, implementation of IndEA becomes easier. **It is necessary to engage a consultancy firm experienced in EA to undertake this work**.

11.5. Implementing IndEA

Once the design and development of Enterprise Architecture is completed as outlined in the earlier section, a major milestone is crossed. Realizing the Architecture is more about Governance, Procurement and Program management. The method(s) of implementation vary widely across enterprises, depending on the ecosystem of governance and the current stage of evolution of e-Governance in the enterprise. As such it is difficult to lay down any principles or detailed procedures for the implementation stage. However an attempt is made to mention a few guidelines that any enterprise can consider while designing the IndEA implementation plan.

11.5.1. Plan Big, Start Small, Scale Fast

By definition, an Enterprise Architecture has to be designed holistically, keeping the medium- and long-term aspirations in view. It cannot be, and should not be, designed for a small part of the enterprise or with only a selected few services in mind. As a thumb rule, the scope of the Architecture should include all the applications and services that contribute to 80% of the business services of the enterprise. Most often, these functionalities and services touch only about 20-30% of the organization and /or processes.

It is advisable to start the ground level implementation with a small footprint. This could invariably include the Core Platform and a few quick wins, including a few integrated services.

Once the initial realization is completed and the benefits of EA begin to be felt by the stakeholders, like more efficient integrated services, interoperability, easy access to enterprise data, the ground for the rollout would have been well laid out.

The strategy of **'Plan Big, Start Small, Scale Fast'** has been demonstrated to work well for a few national level transformation programs.

11.5.2. Continuity of Architecture Governance

Enterprise Architecture has intricate dependencies and inter-connections between several parts. It is not possible, much less desirable, to pull out individual components and redesign / implement them in isolation as it would seriously impair the interoperability and integration capabilities across government. To this end, it is most essential that there is continuity of the top decision-makers at the political, executive and technical levels of Architecture Governance. This principle is applicable to any major program. However, it is **critically important** for any EA project.

11.5.3. Agility in Procurement

Realizing Enterprise Architecture involves a significant volume of procurement of both hardware and software besides several categories of consultancy services. Unless the procurements are done adopting specially designed agile procurement policies, the program is sure to be hampered at multiple stages for various reasons defeating the very purpose of undertaking the initiative. The following suggestions are made in this regard:

1. Government of India shall endeavor to adopt Open Source Software in all e-Governance systems implemented by various Government organizations, as a preferred option in comparison to Closed Source Software (CSS). Please refer to the following URLs for further details:
   http://meity.gov.in/writereaddata/files/policy_on_adoption_of_oss.pdf
   http://egovstandards.gov.in/sites/default/files/Framework%20for%20Adoption%20of%20Open%20Source%20Software%20in%20eGovernance%20Systems.pdf
2. An agile procurement policy may be designed especially applicable for the IndEA initiative, with suitable checks and balances.
3. An Empowered Committee (s) may be constituted to take all major procurement decisions.
4. Preference may be given to readily available products, provided they conform to open standards and are in alignment with the principles of IndEA
5. Preference may also be given to well established and proven Open Source products.
6. Definitive timeframes may be fixed for the various phases of procurement. Procurement of a typical component of IndEA should not take more than 90 days.

11.5.4. IndEA Program Management Unit

Given the inherent complexities and interdependencies between the various components the implementation of IndEA calls for an extraordinary degree of coordination. A large number of tasks, activities and events have to be monitored closely to contain the program within time and budget. These compulsions lead to the inevitable conclusion that a strong Program Management Unit has to be established fairly early in the

implementation of any EA initiative. It is desirable that appropriate **tools** in the areas of **Program Management and EA Governance** are deployed – also in the early stages of implementation.

Readers are referred to **IndEA Adoption Guide – A Method Based Approach** for detailed elaboration on using the IndEA with an industry standard architecture development and management methodology, the TOGAF ADM.

Key roles & responsibilities in IndEA program management unit are:

- Chief Enterprise Architect (CEA) is responsible for the architecture effort as a whole, both on architecture method and architecture itself. As an experienced architect, CEA knows well every domain modelled in the repository, from strategy to technical infrastructure. CEA needs to coordinate the effort on a day-to-day basis.
- Enterprise Business Architect is responsible for development, documentation, and maintenance of Business Architecture
- Enterprise Application architect is responsible to design, develop, and maintain the Enterprise Application Architecture to ensure alignment to the overall Government Business Objective
- Enterprise Data Architect is responsible for development, documentation, and maintenance of Data Architecture
- Enterprise Technology Architect will be responsible for development, documentation, and maintenance of Technology Architecture
- Enterprise Security Architect will be responsible for development, documentation, and maintenance of Security Architecture

11.6. EA Program Risk Management

The initiative of implementing an Enterprise Architecture is not a Project. It is a Program with several special attributes relating to the difficulty of implementation, like the following:

- **Large scope** in terms of the 8 architecture domains and multiple business domains (16 Verticals and 12 Horizontals discussed illustratively in the Chapter 4 on Business Reference Model);
- **Highly Complex**, in defining the requirements at Architecture, Design and Implementation levels, duly complying with the Architectural Principles, ensuring Integration, Interoperability, Optimization of the portfolio of applications and services and providing a migration path for legacy applications;
- **Long Gestation Period,** on account of the need to go through the multiple stages like developing the Enterprise Architecture from the reference Models of IndEA, designing the multiple projects comprising the IndEA program and implementing the portfolio of projects;
- **Multiple Dependencies,** arising out of the need to maintain uniform standards, principles, formats, to implement the projects preferably in a sequence as per the 4-layered meta-model of ARM and reconciling/ balancing the conflicting requirements of multiple projects/ departments;

In view of the above, implementing EA is **several times more complex** than implementing a large nation-wide IT Project. Accordingly, the risk profile of an EA Program is bound to be bigger, needing a special attention. **Needless to say, an EA Program undertaken without a proper risk assessment and putting in place a Risk Management system is likely to be unsuccessful**. Since the science of Project Risk Management is well developed

and practiced widely, its principles, frameworks and methodologies are applicable significantly to the risk management requirements of an EA Program. Therefore, a brief overview of **Project Risk Management** is provided in what follows, suitably adapted for the EA situation.

11.6.1. Essence of Project Risk Management

The Project Management Institute (PMI) defines 'Risk' as "***an uncertain event or condition that, if it occurs, has a negative or positive effect on the project objectives such as time, cost, scope or quality***." The benefits of managing the risk effectively can't be overemphasized. Unmanaged risk can be the single biggest failure factor for a major EA initiative.

The industry standard methodology of Project Risk Management consists of the following components:

1. Risk Management Strategy & Planning (done alongside Business Architecture)
2. Risk Identification (done alongside Application Architecture & Technology Architecture)
3. Risk Analysis (Qualitative) (done alongside the Solution Design)
4. Risk Analysis (Quantitative) (done alongside the Solution Design)
5. Response/ Mitigation Planning (done at the initial stage of implementation)
6. Risk Monitoring & Control (done as part of Governance function)

(A detailed explanation of the above components may be found in the literature on Project Risk Management)

11.6.2. Risk Matrix for EA initiative (Illustrative)

The **Table 11.2** shows a partial list of Risks associated with an EA initiative and the suggested mitigation methods. The risks more specifically related to Enterprise Architecture Development are identified and specified in the Table (Risks relating to cost and time overruns, as well as implementation and operations are not included). Again, within this scope, only risks with High Impact Level are listed. The enterprise has to work more extensively and identify all the risks in the context of its environment and setting. It is necessary to engage specialists in the area of Enterprise Risk management and Project Risk Management to undertake a structured exercise along the 6-components mentioned earlier.

Research indicates that 55% of enterprises taking up IT projects (not necessarily EA initiatives) fail to recognize the importance of a formal Risk Management effort and therefore, fail to achieve the intended objectives.

Risk Type	Description	Probability	Impact Level	Response	Responsibility
Risk Area: GOVERNANCE					
Support of Political Executive/ Top Management	Top Management (Political Executive in case of Government) may not maintain the same level of **interest** through the program period.	3/5	High	1. Adherence to the Program/ Project milestones 2. Periodic reviews by the Top Executive / Apex Committee	Administrative Secretary PMU

Ownership of Line Departments	Change of the head of any line Department during the currency of the Program may result in change of priorities and philosophy.	4/5	High	1. Institutional arrangement at the highest level to ensure continuity of key officials 2. Structured arrangement for transition. 3. Serious involvement of top executive of line department at all the crucial stages of development & implementation	Top Political Executive PMU, Chief Enterprise Architect PMU, Chief Enterprise Architect
Architecture Governance	The Enterprise Architecture does not get signed off. Architecture gets changed frequently Architecture is not complied in design and implementation	2/5	High	A strong Architecture Board is to be constituted. Changes to EA permitted only by the Board after thorough justification by the proponent.	CEO of EA initiative. Chief Enterprise Architect
IT Governance	There is a conflict between Architecture Governance and IT Governance.	2/5	High	A member of the Architecture Governance Board, preferably the Chief Enterprise Architect, is also a key member in the IT Governance Board	CEO of EA initiative.
Risk Area: Architecture Development					
Scope of EA	Scope of EA is not well-defined. Scope does not get signed off	4/5	High	Vision Workshops and Scope Workshops to be held involving all stakeholders. Strong Architecture Governance Board.	Top Political Executive CEO, Chief Enterprise Architect

	Scope gets altered frequently.			---- Ditto-------	
Statement of Objectives & Requirements	Goals & Objectives not defined clearly. Granularity of Requirements at various stages of Architecture Development not understood properly.	3/5	High	Adopting a good model for converting Goals to Objectives, Objectives to Programs / Projects	CEO, Chief Enterprise Architect, Line Depts
Enterprise Thinking	Whole-of-Government thinking not being adopted consistently across all levels and throughout the Architecture Development Phase, resulting in silo approach being perpetrated	2/5	High	Awareness and sensitization of key officials and service providers on EA Vision, Goals and Principles.	CEO, Chief Enterprise Architect.
Risk Area: Organization					
Architecture Capability	The organization is not technically and administratively mature enough to undertake the EA initiative.	5/5	High	Recruitment of EA Professionals. Intensive Training of the CIOs of the participating departments on EA Concepts, Methods & Practices	CEO, Chief Enterprise Architect.
Coordination	Lack of coordination between the various departments included in the scope leads to delays and rework on several architectural artefacts. Consequently, the EA initiative gets derailed.	4/5	High	A strong administrative mechanism cutting across the Whole-of-Government and sufficiently empowered.	Top Political Executive
Communications	Lack of clear and regular communication on EA leads to poor visibility of the benefits of EA among the stakeholders and the consequent de-prioritization of EA in their agenda	4/5	High	A professionally designed communication plan to be implemented. Depts to be encouraged to	CEO, Chief Enterprise Architect. Heads of Line Depts

				promote the initiative.	
Ownership	Centralization of the planning and development of EA, especially the Value Proposition, Goals and Objectives leading to lack of ownership by the line departments and consequent failure to take-off	5/5	High	Deep involvement of the key officials, especially the top executive of the participating departments is essential.	CEO, Chief Enterprise Architect.

TABLE 11.2: RISK MATRIX FOR EA INITIATIVE (SHOWING HIGH RISKS ONLY)

Since the EA initiatives are inherently more risky than normal IT Projects, it is essential that the EA planners should recognize the importance of Enterprise Risk Management and Project Risk Management and provide specialized resources and effort adequately in the planning phase. Given the importance of risk management, a special responsibility is cast on the Architecture Governance to effectively manage the **GRC** portfolio, relating to **Governance, Risk Management and Compliance**. As may be recalled, GRC is included as one of the distinct responsibilities of the Architecture Governance Board in the Governance Reference Model.

ISO 31000, the International Standard that specifies the principles of Risk Management and provides guidelines for implementation, may be used by the enterprise during the various phases of development and implementation of Enterprise Architecture.

Annexures

I. Key Performance Indicators for Primary Sector

Key Performance Indicators for Departments are mentioned below[8]:

Sl.	Department	User	Objectives	Output Indicator	Outcome Indicator	Economy Indicator
1	Agriculture	Farmer	Increased Gross Agriculture Production through sustainable agricultural practices	% increase annually in timely supply of quality seeds for Kharif and Rabi seasons	% increase annually in agriculture production growth rate	% Deviation from planned Operational Cost of the Business Function.
					% increase annually in per capita food grain production	
				% increase annually in timely fertilizer distribution during Kharif and Rabi seasons	% increase annually in the production of top 10 crops	
				% increase annually in the timely availability of input machineries and tools for purchase / custom hiring	% of annual target achieved in the production of top 10 crops	
				% increase annually of farmers who receives soil health cards and advise on time - Soil Health Management (SHM)		
				% increase annually in the agricultural area under organic farming		
				% increase annually of farmers covered by Climate Change and Sustainable Agriculture Monitoring, Modelling and Networking (CCSAMMN) missions		

[8] Source: e-Pragati

		Farmer	Effective Disaster Management	% increase annually in the accurate coverage of weather forecast and advisories based on crops and phenology stages	% decrease annually in crop destruction due to natural calamities and pests	% Deviation from planned Operational Cost of the Business Function.
				% increase annually in the offtake of insurance products	% increase annually in the farm land area under crop insurance	
2	**Horticulture**	Farmer	Increased Gross Horticultural Production	% increase annually in the area under cultivation of horticulture crops	% increase annually in horticulture production growth rate	% Deviation from planned Operational Cost of the Business Function.
				% increase annually in the agricultural area under irrigation	% of annual target achieved	
3	**Cooperation**	Farmer	Provide financial assistance to farmers	% increase annually in the registered Farmer Producer Organizations	% decrease annually in NPAs from loans to farmers	% Deviation from planned Operational Cost of the Business Function.
				% increase annually in the farmers covered by timely disbursements of interest free loans		
				% increase annually of farmers who received funds through Banks		
4	**Sericulture**	Farmer	Increased Production of Cocoon / Raw Silk	% increase annually in the area under cultivation of Cocoon (CB/BV)	% increase annually in Cocoon / Raw Silk production growth rate	% Deviation from planned Operational Cost of the Business Function.
				% increase annually in the area under cultivation of Raw Silk (CB/BV)		
					% of annual target achieved	
5	**Fisheries**	Fish Farmer	Increased production of Fish by adopting modern practices	% increase annually in the area under cultivation (Marine Fish, Inland Fish, Brackish Water Shrimp, Fresh Water Prawn).	% increase annually in Fish production growth rate	% Deviation from planned Operational Cost of the Business Function.
				% increase annually in the area under fish tanks revived out of Abandonment	% of annual target achieved	

6	**Animal Husbandry**	Farmer	Increased Production of Milk / Meat / Eggs	% increase annually in the production of Milk, Meat, and Eggs	% increase annually in production growth rate	% Deviation from planned Operational Cost of the Business Function.
					% of annual target achieved	
7	**Agriculture Marketing and Agro Processing**	Department	Increased Agro processing capacity	% increase annually in farmers using e-marketing facility	% increase annually on transaction volume at e-market	% Deviation from planned Operational Cost of the Business Function.
					% decrease annually in wastage of agricultural produce	
				% increase annually in the procurement of agricultural produce from farmers		
				% increase annually in availability of cold storage space w.r.t crop categories		

II. Example of Services Provided by the Government

G2C Services

Service Name	Service Description	Service Type	Standard Service Name
Domicile Certificate	Domicile certificate is certification provided to the citizen by the government confirming and testifying their place of residence. This certificate establishes the citizen as a resident of West Bengal for all legal and official purposes.	G2C	Certificates
Income Certificate	Income Certificate is certification provided to the citizen by the government confirming and testifying their annual income. This certificate establishes the expected annual income of citizen for all legal and official purpose.	G2C	Certificates
TIN and Form Search	All stakeholders of the state and other states can get details of a Dealers using TIN Search. Form Search facility helps Assessing officer of other states to verify the CST Form generated in state	G2C	Commercial Tax
Online VAT Returns	Online VAT Returns service is an internet enabled way to fill forms online using DSC, receipt can be generated and kept for record. The service is SMS enabled. Customized Return Form can be downloaded and filled offline during submit all checks are enforced for the authorized signatory.	G2C	Commercial Tax
Generation of Dematerialized C Forms	The service provides the facility of generation and printing of 'C' Form with the required particulars made available to the dealer in his desktop after he has furnished the VAT and CST Returns online	G2C	Commercial Tax

G2B Services

Service Name	Service Description	Service Type	Standard Service Name
Dematerialized Waybill for Registered Dealers	Registered Dealers apply for Waybill using this e-Service. Waybill is required for import of goods from other states.	G2B	Commercial Tax
e-Filling of Entry Tax Return	Dealers has to pay Entry Tax for goods to be imported from outside West Bengal and show evidence of payment at the check Posts. He has to file entry tax return declaring all details of import from different dealers declaring goods and value there of.	G2B	Commercial Tax
e-Registration and Demat RC	Traders/Companies not yet registered under VAT or CST act applies through this option to get himself registered under that act and gets their digital certificate.	G2B	Commercial Tax
e-Registration of Digital Signature Certificate	Dealers Registers their authorized persons DSC by using this e-Service. At the time of return file DSC is verified whether the DSC used is of declared authorized person against the stored information in addition to validity of DSC.	G2B	Commercial Tax
e-Submission of CST Forms Received from other States	Dealers registered under Central Sales Tax Act receive Central Forms Like C F Forms against goods sold to other state dealers. Dealers input sell details against each central forms received.	G2B	Commercial Tax
e-Submission of Form 16	Few Dealers having low turnover are called composite Dealers. This category of dealers files their Return Annually. This dealers require to declare to avail this facility using this e-Service within first few months of new financial year.	G2B	Commercial Tax
Seed License	Licensing of Seeds is to monitor the dealers of seed within a particular state. Seed license can be issued through this service.	G2B	Licenses and Permits

III. Technology Standards for Application Layers

The changes to the existing Technical Standards for Interoperability Framework for E-Governance in India (May 2012 Version 1.0) is given in *italic blue fonts* in the tables below.

TRM Service Standard – Network Access Layer

Sr.No	Interoperability Area	Standard / Specification	Standards Body	References for Standards / Specification
1	Internet Protocol – 32 bit	IPv4	IANA	1. http://egovstandards.gov.in/sites/default/files/Technical%20Standards%20for%20IFEG%20Ver1.0.pdf 2. http://standards.ieee.org/news/2014/ieee_802_11ac_ballot.html 3. https://tools.ietf.org/html/rfc7540 4. https://tools.ietf.org/search/rfc2595 5. https://tools.ietf.org/html/rfc2400
2	Internet Protocol – 128 bit	IPv6	IETF	
3	Wireless LAN - Implementation	*IEEE 802.11ac (Dec 2013)*		
4	Authentication and Authorization Data Exchange	SAML 2.0	OASIS	
5	Hypertext Transfer	*HTTP/2*	IETF, W3C	
6	E-mail Transport	*Extended SMTP additions by RFC 5321*	IETF	
7	Mailbox Access	IMAP4, *IMAP over SSL (IMAPS), POP3*	IETF	
8	Directory Access	LDAP V3 */ X.500-lite*	IETF	
9	Domain Name services	DNS	IETF	

FIGURE III.1: TRM SERVICE STANDARD- NETWORK ACCESS LAYER

TRM Service Standard – Presentation Layer

Sr.No	Interoperability Area	Standard / Specification	Standards Body	References for Standards / Specification
1	Document type for Simple Hypertext Web Content	ISO/IEC 15445:2000 *(HTML 5)*	ISO/IEC W3C	1. http://egovstandards.gov.in/sites/default/files/Technical%20Standards%20for%20IFEG%20Ver1.0.pdf 2. https://www.w3.org/TR/html5/ 3. https://www.w3.org/standards/techs/css#w3c_all 4. https://www.iso.org/standard/66363.html 5. https://www.iso.org/standard/51502.html 6. https://jpeg.org/jpeg2000/
2	Document type for Complex, Strict Hypertext Web Content (XML or non-XML)	*XHTML v5*	W3C	
3	Style Sheets (to define Look & Feel of Web-page)	*CSS 3*	W3C	
4	Extensible Style Sheets (to transform format and addressing parts of documents)	XSL 1.1	W3C	
5	Content for Mobile Devices – Hypertext Markup Language	XHTML Basic v1.1	W3C	
6	Document Type for Editable documents (with formatting)	*ISO/IEC 26300-1:2015 (ODF – Open Document v1.2)*	ISO/IEC OASIS	
7	Document Type for Presentation	*ISO/IEC 26300-1:2015 (ODF – Open Document v1.2)*	ISO/IEC OASIS	
8	Document Type for Spreadsheet	*ISO/IEC 26300-1:2015 (ODF – Open Document v1.2)*	ISO/IEC OASIS	
9	Document type for Non-editable documents	ISO 32000-1:*2013* (PDF 1.7)	ISO/IEC	
10	Graphics – Raster Image (Lossy Compression) – Exchange Format for Restricted Memory Device cases (like Smart Cards)	JPEG2000 /*JP2 Part 2*	ISO/JPEG Committee	

Sr.No	Interoperability Area	Standard / Specification	Standards Body	References for Standards / Specification
11	Graphics – Raster Image (Lossy Compression) – Exchange Format for Normal cases (like Web, Desktop applications)	JPEG	ISO/JPEG Committee	

FIGURE III.2: TRM SERVICE STANDARD – PRESENTATION LAYER

TRM Service Standard – Security Layer

Sr.No	Interoperability Area	Standard / Specification	Standards Body	References for Standards / Specification
1	Secure Electronic Mail	S/MIME 3.1 */ 3.2 latest*	IETF	1. http://egovstandards.gov.in/sites/default/files/Technical%20Standards%20for%20IFEG%20Ver1.0.pdf 2. https://tools.ietf.org/html/draft-ietf-tls-https-03 3. https://tools.ietf.org/html/draft-ietf-tls-tls13-11 4. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf 5. http://standards.ieee.org/news/2014/ieee_802_11ac_ballot.html
2	Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL	HTTPS	IETF	
3	Secure Socket Layer	SSL 3.0	IETF	
4	Transport Layer Security for Server and Web Browser	TLS 1.2 */ 1.3 latest*	IETF	
5	Digital Signature Algorithms	DSA(FIPS186-*4) 2013*	NIST	
6	XML Signature for XML Message signing	XML Signature	W3C	
7	XML Encryption for XML Message encryption	XML Encryption	W3C	
8	Wireless LAN security	*IEEE 802.11ac*	IEEE	

FIGURE III.3: TRM SERVICE STANDARD – SECURITY LAYER

TRM Service Standard –Data Interchange Layer

Sr.No	Interoperability Area	Standard / Specification	Standards Body	References for Standards / Specification
1	Web Services Description Language	WSDL2.0	W3C	1. http://egovstandards.gov.in/sites/default/files/Technical%20Standards%20for%20IFEG%20Ver1.0.pdf 2. https://www.w3.org/TR/soap12/ 3. http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SOAPMessageSecurity-v1.1.1-os.html 4. http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-x509TokenProfile-v1.1.1-os.html 5. http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-x509TokenProfile-v1.1.1-os.html
2	Web service request delivery	SOAP*1.3*	W3C	
3	Web Services Security - Basic Security Profile	Basic Security Profile V1.1	OASIS	
4	Web Services Security – SOAP message security	SOAP message security *V1.1.1*	OASIS	
5	Web Services Security – Username Token Profile	Username Token Profile *V1.1.1*	OASIS	
6	Web Services Security - X.509 Certificate Token Profile	X.509 Certificate Token Profile *V1.1.1*	OASIS	

FIGURE III.4: TRM SERVICE STANDARD – DATA INTERCHANGE LAYER

TRM Service Standard – Data Integration Layer

Sr.No	Interoperability Area	Standard / Specification	Standards Body	References for Standards / Specification
1	Data Description Language (for exchange of data)	XML 1.0	W3C	1. http://egovstandards.gov.in/sites/default/files/Technical%20Standards%20for%20IFEG%20Ver1.0.pdf 2. https://www.w3.org/TR/xmlschema11-1/ 3. https://www.w3.org/TR/xslt-30/ 4. https://www.w3.org/TR/xpath-30/
2	Data Schema Definition	XML Schema (XSD) *1.1* Part 1: Structures, XML Schema Part 2:Datatypes	W3C	
3	Data Transformation for Presentation	XSL 1.1	W3C	
4	Data Transformation for conversion from XML	XSLT 2.0 */ 3.0*	W3C	

Sr.No	Interoperability Area	Standard / Specification	Standards Body	References for	Standards / Specification
	schema format to another format				
5	Content searching and navigation in an XML document	Xpath *3.0*	W3C		
6	XML vocabulary for specifying formatting semantics	XSL 1.1	W3C		
7	Meta-data elements for content	ISO 15836:2009 */ 2012* (Dublin Core Metadata Element set)	ISO/IEC		

FIGURE III.5: TRM SERVICE STANDARD – DATA INTEGRATION LAYER

IV. Technology Standards for Infrastructure Components

The following tables provides the technology open standards and formats for the TRM Solution Building Blocks.

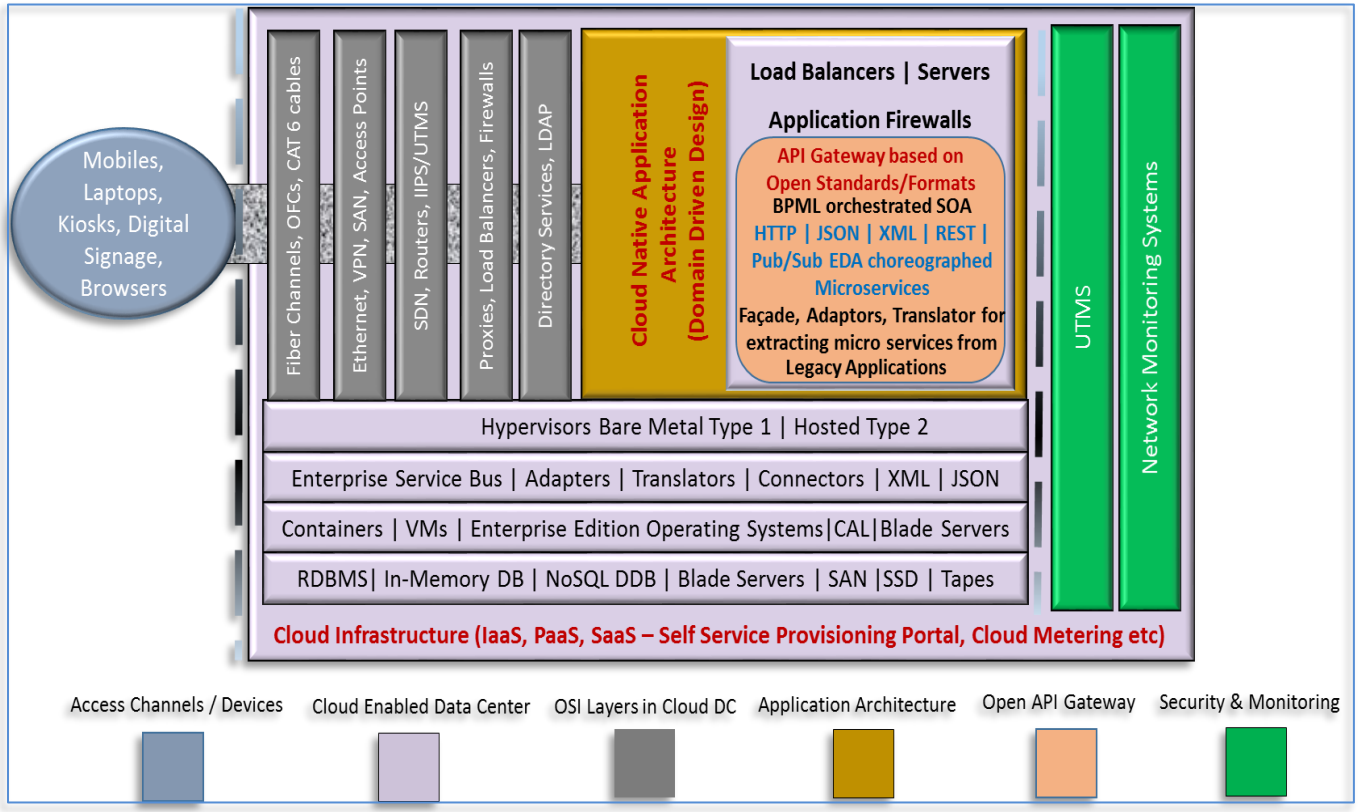


FIGURE IV.1: ARCHITECTURAL PATTERNS BASED ON TRM

TRM Service Standard – Access Devices

Sr.No	Service Standards	Description	Open Technology Standards / Specifications	References for Standards / Specification
1	**Desktops / Laptops / Tablets / Smart Phones**	All these are normal access devices used for availing online services.	All devices with their latest operating system versions.	a) https://www.usaid.gov/sites/default/files/documents/1868/545mat.pdf
2	**IVRs**	It is a touch-tone telephone method used for voice based interaction to enter data and acquire information based on catalogued services.	**IVR Applications** are developed using standards such as VoiceXML, CCXML, SRGS and SSML. The ability to use XML-driven applications allows a web server to act as the application server, freeing the IVR developer to focus on the IVR speech recognition interactions to prompt for and recognize user input such as directed dialogue, open-ended, and mixed dialogue.	NA
3	**Kiosk / Digital Signage**	Kiosk is a touch screen that displays information upon taping the screen. The Digital signage use technologies such as LCD, LED and Projection to display content such as digital images, video, streaming media, and information.	Digital Signage uses HTML5 and Unity3D for interactive content. The Synchronized Multimedia Integration Language (SMIL) is used to improve standardization and interoperability of the digital signage, and JPEG images and MPEG4 videos remains the popular digital content formats for the digital signage.	NA

FIGURE IV.2: TRM SERVICE STANDARD – ACCESS DEVICES

TRM Service Standard – Biometric Devices, Smart Cards and Digital Signatures

Sr.No	Service Standards	Description	Open Technology Standards / Device Specifications	References for Standards / Specification
1	Facial Image Capturing Devices / Sensors		1. ISO/IEC 19794-7:2014 - Part 5 for Facial imaging 2. ISO/IEC 19785 Common Biometric Exchange Formats Framework (CBEFF) – for packaging the biometric data – providing common structure, metadata, and security 3. ISO/IEC 19794-7:2014 - Part 7 – for data formats – for application specific requirement specifications / application profiles – for conformance testing methodology 4. Photographic requirements - ISO 19794-5 Section 7.3, 7.4, 8.3 and 8.4 with Section 8.3 of Technical Corrigendum 2 5. Pose - Per ISO 19794-5 Section 7.2.2 6. Illumination - Per ISO 19794-5 Section 7.2.7 7. Eye Glasses - Per ISO 19794-5 Section 7.2.11 8. Operational - Per ISO 19794-5 Section 7.2.4 - 7.2.10 9. Compression and Storage - Compression ratio to be less than 10:1. JPEG 2000 color compression recommended.	1. http://gsi.nist.gov/global/docs/sit/2014/ETabassiThurs.pdf 2. https://www.iso.org/standard/55938.html 3. https://uidai.gov.in/images/resource/Biometrics_Standards_Committee_report.pdf (page 32)
2	Fingerprint Capturing Devices / Sensors	The device or sensor used to capture fingerprints to ascertain identity of individuals for availing government schemes and services.	1. ISO/IEC 19794-7:2014 - Part 2 and 4 for Fingerprinting 2. ISO/IEC 19785 Common Biometric Exchange Formats Framework (CBEFF) – for packaging the biometric data – providing common structure, metadata, and security 3. ISO/IEC 19794-7:2014 - Part 7 – for data formats – for application specific requirement specifications / application profiles – for conformance testing methodology	1. http://gsi.nist.gov/global/docs/sit/2014/ETabassiThurs.pdf 2. https://www.iso.org/standard/55938.html 3. https://uidai.gov.in/images/resource/Biometrics_Standards_Committee_report.pdf (page 35)

Sr.No	Service Standards	Description	Open Technology Standards / Device Specifications	References for Standards / Specification
			4. Device characteristics - Setting level 31 or above, EFTS/F certified 5. Storage format - ISO Section 8.3 6. Compression - JPEG 2000, and Compression ratio to be less than 15:1 7. Minutiae format for data interchange - ISO 19794-2 8. Transmission - ISO standard minutiae format	
3	Iris Capturing Devices / Sensors	The sensor used to capture iris image to ascertain identity of individuals for availing government schemes and services.	1. ISO/IEC 19794-7:2014 - Part 6 for Iris images 2. ISO/IEC 19785 Common Biometric Exchange Formats Framework (CBEFF) – for packaging the biometric data – providing common structure, metadata, and security 3. ISO/IEC 19794-7:2014 - Part 7 – for data formats – for application specific requirement specifications / application profiles – for conformance testing methodology 4. Device - Tethered, autofocus, continuous image capture, exposure < 33 milli-second, distance >300 mm for operator control, > 100mm enrollee control 5. Image - One eye, > 140 pixel image diameter (170 pixel preferred), image margin 50% left and right, 25% top and bottom of iris diameter 6. Quality Assessment - IREX II recommendations 7. Compression and Storage - ISO 19794-6 data format standard. JPEG 2000 or PNG lossless compression	1. http://gsi.nist.gov/global/docs/sit/2014/ETabassiThurs.pdf 2. https://www.iso.org/standard/55938.html 3. https://uidai.gov.in/images/resource/Biometrics_Standards_Committee_report.pdf (page 40)
4	**Digital Signatures**	A Digital Signature Certificate (DSC) using Public Key Infrastructure (PKI) provides identifying	1. **Class-2 Digital Signature Certificate** is issued to Individuals, and Devices. The Class 2 Device Certificates are appropriate for device authentication; message, software, and content integrity; and confidentiality encryption.	1. http://cca.gov.in/cca/sites/default/files/files/ARCHIEVE/INDIA%20PKI%20IOG/INDIA%20PKI%20IOG%20R2.4.pdf

Sr.No	Service Standards	Description	Open Technology Standards / Device Specifications	References for Standards / Specification
		information, that's forgery resistant and can be verified since it was issued by a trusted certificate-issuing authority (CA) or agency. The certificate contains the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.	The Class 2 Individual Certificates are appropriate for Digital Signatures, encryption, and electronic access control in transactions where proof of identity based on information in the Validating Database is sufficient. 2. **Class-3 Digital Signature Certificate** For organizations to apply for any Government e-tender needs to have a Class 3 Digital Signature Certificate registered in the name of a representative who is authorized to submit online offers for e-Tendering applications. The DSC helps to: • Secure email and web-based transactions, or to identify other participants of web-based transactions. • Prove ownership of a domain name and establish SSL/ TLS encrypted secured sessions between your website and the user for web based transactions. • Proving authorship of a code (for a developer) and retaining integrity of the distributed software programs. • Sign web forms, e-tendering documents, filing income tax returns, to access membership-based websites automatically without entering a user name and password etc.	

FIGURE IV.3: TRM SERVICE STANDARD – BIOMETRIC DEVICES, RFID SMART CARDS AND DSCS

TRM Service Standard – Network Infrastructure

Sr.No	Service Standards	Description	Open Technology Standards / Specifications
1	**Wi-Fi Network**	Wi-Fi or Wireless Fidelity, operates in the free spectrum band of 2.4 GHz to 5 GHz globally.	1. WPA2 with 802.1X security authentication standard provides extremely strong encryption by rotating encryption keys, hence even a cracked key isn't useful. 2. IEEE 802.11u – supports 540 – 100 Mbps throughput over 50 meters. 3. IEEE 802.11ac supports 3x3 multiple-input multiple-output (MIMO) with 3 spatial streams at 5 GHz 4. IEEE 802.11n supports 2x2 multiple-input multiple-output (MIMO) with 2 spatial streams at 2.4 GHz 5. Interfaces - 10/100/1000 BASE-T autosensing
2	**IPv6 / SSO / Directory Services**	IPv6 requires all agencies to transition their equipment and systems that offer or obtain external services to IPv6 standards (from the current IPv4 standards), else the devices / systems that works on IPv6 cannot access / render services to stakeholders who uses IPv4 due to address exhaustion. Single Sign On (SSO) enables the user to log in with a single ID and password to gain access to a connected systems for seamlessly sign on at each system. This is typically accomplished using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on directory servers. Reduced Sign-On (RSO) has been used wherever single sign-on is impractical in addressing the need for different levels	1. **OAuth** is an open standard for authorization, commonly used as a way for Internet users to authorize websites or applications to access their information on other websites but without giving them the passwords. 2. **OpenID** is an open standard and decentralized authentication protocol which allows users to be authenticated by co-operating sites or Relying Parties using a third party service, allowing users to log in to multiple unrelated websites without having to have a separate identity and password for each. 3. **Lightweight Directory Access Protocol (LDAP)** runs directly over the TCP/IP stack. LDAP is an information model and a protocol for querying and manipulating it. LDAPv3 is an update developed in the Internet Engineering Task Force

Sr.No	Service Standards	Description	Open Technology Standards / Specifications
		of secure access and more than one authentication server is necessary. Directory Services is a network service that discovers and identifies resources on a network and makes them accessible to users and applications. The resources include users, e-mail addresses, computers, mapped drives, shared folders and peripherals such as printers and PDA docking stations. Users and computers access these resources without the need to know how or where the resources are connected.	(IETF) which address the limitations found during deployment of the previous version of LDAP.

FIGURE IV.4: TRM SERVICE STANDARD – NETWORK INFRASTRUCTURE

TRM Service Standard – Delivery Platform

Note: It is recommended to have scalable, open standard REST based interaction with services and Message Queues where ever necessary vs ESB which is heavy and may not be required in the e-Gov Apps. ESB must be used only where absolutely required.

Sr.No	Service Standards	Description	Open Technology Standards / Specifications	References for Standards / Specification
1	**Enterprise Service Bus (ESB)**	The enterprise service bus connects disparate applications, databases and security resources which may be spread across geographically to a restricted set of components that are centrally located for reliability, scalability and agility for delivering a SOA. The ESB uses a set of adapters and connectors for application integration and data transformation. It supports asynchronous messaging with publishing and subscription options, complex routing based on rules and security assurance services, while supporting the addition of new applications or platforms in the network in future.	1. JMS 2. JCA 3. JBI 4. OSGi 5. XSLT 6. XML/JSON 7. SOAP/RNI/REST	1. https://uidai.gov.in/images/AadhaarTechnologyArchitecture_March2014.pdf (page 122)

Sr.No	Service Standards	Description	Open Technology Standards / Specifications	References for Standards / Specification
2	**SAN Storage**	The storage devices helps to save the large amounts of structured and unstructured data, voice and video for future use. The Storage Area Networks (SAN) is the most promising storage technology which helps to access the data at block level to maintain high data recoverability and accessibility.	1. For SAN: a) FCoE (requires converged network adapter) aa) SAN Switch/Director bb) IEEE 802.3ae (for 10Gigabit Ethernet over FC) b) iSCSI	NA
3	**Optical Fiber Cables / CAT 6 Cables**	The optical fiber transports huge volume of data at very high speeds between two end points in a network. The fiber cables comes as single mode and multi-mode fiber optic cables. The multimode fiber optic cables does large volume of data transmission over a short distance (OM4 can carry up to 600 meters) while single mode can transmit 10Gigabit data directly to 10 kilometers.	1. FCP 2. iSCSI 3. FCoE	NA
4	**Disaster Recovery - RPO / RTO**	The Recovery Point Objective (RPO) i.e. the permissible data disruption time, and the Recovery Time Objective (RTO) is the time taken by the system to be up and running.	RPO should be less than or equal to 2 hours and RTO shall be less than or equal to 4 hours.	1. http://www.digitalindia.gov.in/writereaddata/files/whats_new_doc/RFP%20for%20Accreditation%20of%20Cloud%20Service%20Offerings%20of%20Private%20Service%20Providers.pdf 2. http://inclusion.skoch.in/story/369/disaster-management-&-disaster-recovery-669.html

Sr.No	Service Standards	Description	Open Technology Standards / Specifications	References for Standards / Specification
Specification for RTO/RPO				
a) The key transaction data shall have RPO of 15 minutes. However, during the change from Primary DC to DRC or vice-versa (regular planned changes), there should not be any data loss. There shall be asynchronous replication of data between Primary DC and DRDC and the CSP (Cloud Service Provider) will be responsible for sizing and providing the DC-DR replication link so as to meet the RTO and the RPO requirements b) The Primary DC (of the Government Department) and the DRC should be in different seismic zones c) During normal operations, the Primary Data Center (of the Government Department) will serve the requests. The Disaster Recovery Site will not be performing any work but will remain on standby. During this period, the compute environment for the application in DR shall be available but with minimum possible compute resources required for a functional DR as per the solution offered. The application environment shall be installed and ready for use. DR Database Storage shall be replicated on an ongoing basis and shall be available in full (100% of the PDC) as per designed RTO/RPO and replication strategy. The storage should be 100% of the capacity of the Primary Data Center site d) In the event of a site failover or switchover, DR site will take over the active role, and all requests will be routed through that site. Application data and application states will be replicated between data centers so that when an outage occurs, failover to the surviving data center can be accomplished within the specified RTO. This is the period during which the Compute environment for the application shall be equivalent to DC.		e) The installed application instance and the database shall be usable and the same SLAs as DC shall be provided. The use of this Full Compute DR environment can be for specific periods during a year for the purposes of DC failure or DR Drills or DC maintenance. The Database and storage shall be of full capacity and the licenses and security shall be for full infrastructure. The bandwidth at the DR shall be scaled to the level of Data center. Users of application should be routed seamlessly from DC site to DR site. The CSP shall conduct DR drill for two days at the interval of every six months of operation wherein the Primary DC has to be deactivated and complete operations shall be carried out from the DR Site. However, during the change from DC to DRC or vice-versa (regular planned changes), there should not be any data loss f) The CSP shall clearly define the procedure for announcing DR based on the proposed DR solution. The CSP shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to DR. The CSP shall plan all the activities to be carried out during the Disaster Drill and issue a notice to the Department at least two weeks before such drill g) The CSP should offer dashboard to monitor RPO and RTO of each application and database	

Sr.No	Service Standards	Description	Open Technology Standards / Specifications	References for Standards / Specification
			h) The CSP should offer switchover and switchback of individual applications instead of entire system i) Any lag in data replication should be clearly visible in dashboard and alerts of same should be sent to respective authorities	

FIGURE IV.5: TRM SERVICE STANDARD – DELIVERY PLATFORM

V. TRM Service Standard – Cloud Computing Stack

Cloud computing[9] is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

- **Essential Characteristics:**
  - On-demand self-service
  - Broad Network Access
  - Resource Pooling
  - Rapid elasticity
  - Measured Service
- **Service Models:**
  - Software As A Service
  - Platform As A Service
  - Infrastructure As A Service
- **Deployment Models:**
  - Private Cloud
  - Community Cloud
  - Public Cloud
  - Hybrid Cloud

For further details, please refer to:

1. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
2. http://meity.gov.in/writereaddata/files/GI-Cloud%20Strategic%20Direction%20Report%281%29_0.pdf
3. http://meity.gov.in/writereaddata/files/GI-Cloud%20Adoption%20and%20Implementation%20Roadmap%281%29_0.pdf

[9] Source: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Cloud Interoperability Standards (Indicative List):

a. **For IaaS:**
- Open Cloud Computing Interface (OCCI) specification set from Open Grid Forum
- Cloud Infrastructure Management Interface (CIMI) set from the Distributed Management Task Force (DMTF)

b. **For PaaS:**
- PaaS-specific standard22 has been started by the OASIS Cloud Application Management Protocol (CAMP)

c. **For SaaS:**
- IP (v4, v6), TCP, HTTP, SSL/TLS, HTML, XML, REST, Atom, AtomPub, RSS, and JavaScript/JSON, since SaaS works via web browser based management interfaces

d. **For Distributed Applications / Interfaces / Cloud Services:**
- Interoperability standards for distributed applications, interfaces, packaging, and transport are SOAP, WS-* and ebXML
- Interoperability standards for cloud services are OpenID, OData, CDMI, AMQP, and XMPP
- Topology and Orchestration Services for Applications (TOSCA) from OASIS, to address portability concerns between services and applications that may be required to be deployed on different cloud providers and platforms due to reasons such as regulatory concerns, evolving technical requirements, and market factors.

Data Centre Standards required for Cloud Enablement (Indicative List):

- The standards that needs to be adhered by a data centre to maintain operational consistency and stability.
- The Data Center should be certified for the latest version of ISO 27001 (2013 or above) and provide service assurance and effectiveness of Management compliant with SSAE 16 / ISAE 3402 standards
- The NOC offered for the Data Center Facilities must be within India and the managed services quality should be certified for ISO 20000:1
- The Data Center should conform to at least Tier III standard (preferably certified under TIA 942 or Uptime Institute certifications by a 3rd party) and implement tool-based processes based on ITIL standards
- All the physical, environmental and security features, compliances and controls of the Data Center facilities (as required under this RFP) shall be enabled for the environment used for offering cloud services
- Provide staff, technical and supervisory, in sufficient numbers to operate and manage the functioning of the DC & DRC with desired service levels
- Physical Security Standards as per the latest version of ISO 27001 (year 2013 or above) standards

- Facility shall be certified (either with respect to Tier Standards or Physical Security Standards) by a Third Party at regular intervals indicating the conformance to the Tier III standards

VI. Commonly used Application Integration Patterns

Integration Pattern	Details
Canonical Messaging	• Provide a standard representation of business data entities e.g. Customer, PO etc. • Facilitate reduction in number of data transformations from n(n-1) to 2n • Applicable in A2A and B2B integration scenarios • Provide application neutral message format typically in XML • XML schemas are used to model canonical messages • Common Information Model (CIM) can be used to define canonical messages • Used to communicate between different data formats
Remote Facade	• Remote Facade can be used to shield the service consumer from the invocation details of the actual service provider • The ESB provides the Remote Facade and acts as the service provider • Enables loose coupling between service consumer and provider • Allows ESB to handle complex transformation, mediation and infrastructure tasks “behind the scenes” • Allows ESB to lookup or aggregate information from multiple service providers and provide a single response to the consumer
VETRO	• VETRO is the standard integration pattern used by the ESB • Validate: This step checks for conformity to a particular schema or WSDL document that describes the message • Enrich: This step adds specific content data to the message • Transform: The transformation component of the ESB would retrieve the payload of the SOAP message and transform it in the destination format. • Route: The transformed message is then assembled as a SOAP message using the original SOAP headers, and then routed to the appropriate subscriber endpoint based on the subscription lists. • Operate: This step is to interact with the subscriber application. Adapters can be used if the subscribing application is not service enabled.

Two Step Cross Reference	• The two step cross reference pattern helps in segregating data format and content transformation • Helps in performing lookups and cross-referencing independent of the format e.g. For EDI cross reference lookup, currency code lookup etc. • Helps in building reusable components for database lookups and cross-referencing
Forward Cache	• This pattern enables a consumer application to access data from a cache of results even if the provider application is unavailable • Provides a fast, “always available” means to access data from external systems • Useful if the integration involves a portal based application as the consumer; as it would provide a seamless experience to the users by avoiding connectivity delays to external systems • A typical use-case is of an e-commerce portal integration. The e-commerce portal application would be served by the cache service for all its data requirements from external systems. • The cache service would pre-fetch and store data typically in a lightweight database for consumption.

VII. Controls at Security Layers

Controls at Perimeter Layer

Operating Security	
Objective: To define operating procedures to ensure the security at the data centre.	
Documenting operating procedures	Operating procedures at the data centre should be well defined, documented and should be made available to whom so ever concern.
Change Management	Any change at the organization level, in the business processes, in the rules related to information processing facilities that affect the information security procedures should be reflected in the security operating procedures and should be controlled through change management.
Capacity Management	The use of resources at the data centre should be regularly monitored, and tuned. Projections for the future capacities should be made to ensure the required system performance even for the future requirements.
Separate environments for development, testing and production	A separate environment should be maintained for development, testing and production to reduce the risk of unwanted access and /or changes to the production environment.
Installation of software into the production environment	In order to ensure the integrity of the systems at the production, procedures should be defined and implemented to install the software

Physical Server

Physical Server Security Management	
Objective : To ensure the protection of physical access and no damage to the servers in the network	
Lock the server room	Ensure that there are good locks on the server room door. Develop policies regarding the key access for these locks.
Set up surveillance	An authentication system should incorporated into the locking devices, so that a smart card, token, or biometric scan is required to unlock the doors, and a record is made of the identity of each person who enters.

	A video surveillance camera may also be placed in a location to record access activities in server room.
Positioning **vulnerable devices in locked room**	Place as many network devices as possible in locked room, or if they need to be in a different area, place them in a locked closet.
Pack up the backups	Keep the set of backups off site, and ensure that they are secured in that offsite location.
Disable the drives	Disable or remove floppy drives, USB ports, and other means of connecting external drives to servers and workstations.
Limit user access	Limit the number of users who have physical access to the server.
Use uninterrupted power sources (UPS)	UPS with significant power backup protects the server from power loss that can cause server failure or file corruption.
Fire detection and suppression	Server room needs to be equipped to face fire like situations.
Air Conditioning / Cooling	In the data center temperature and humidity should be maintained on pre-defined ranges. Appropriate backup plan also should be provided for cooling.
Server Inventory Control	Servers and equipment within the server room should be checked regularly on functionality and existence.
Handling of Servers hardware	The safest and most effective method of handling server hardware should be used.
Usage	There shall be no eating, drinking, or smoking allowed in the server room at any time
Record Keeping	Documentation of all repairs and modifications to the physical components related to security (e.g., doors, hardware, locks) shall be maintained.

Virtual Server/ Cloud

Cloud set ups are used to provide various services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The security controls need to be defined based on the type of the cloud service. Although majority of the security concerns for cloud based services and non-cloud based services are similar, there is an added responsibility of secrecy, privacy, access control and the possible threat to data.

Cloud Security Management	
Objective : To ensure the security for the cloud infrastructure	
Data Protection	Data protection control should consider the effective measures for risks involved in data theft, unauthorized disclosure of information, loss of data, data deletion or modification.

	• Applying controls related to Identity and Access Management • Defining and implementing controls for different type of service such as IAAS, PAAS and SAAS • Standards which can be considered for data security (ISO 27002 along with ISO 27017 for cloud specific services)
Data Privacy Policy	Appropriate controls should be in place to ensure the data privacy such as by applying mechanisms of data integrity, data availability by the means of regular back-ups, intrusion detection and prevention etc. Standards such as ISO/IEC 27018 address the requirement for protection of Personal Identifiable Information (PII).
Application Security	Based on the type of cloud services such as IAAS, PAAS, SAAS which are being offered the required controls along with possible risk factors should be defined to ensure the application security.
Network Security	Network security comprises of protection of external as well as internal network activities by defining controls to address the following: • Network Monitoring • Prevention of DDOS and DOS • Determination and prevention of possible attacks on the application • Controls to prevent the internal network
Physical Infrastructure Security	Controls which are applicable and are defined for the Physical Infrastructure security also apply here.
Operational Security	Operational security controls such as identity and access management should be in place to ensure the access to the various resources and the services deployed in the cloud environment.

To abide the first principle mentioned above, access control is the most essential requirement. To secure the data, infrastructure, assets, information in the organization or state, the access to all these should be controlled at all the four layers defined in the security architecture i.e. business, information, application and data. Controls related to access control at various layers are given ahead.

Authentication and Access Control

Application Access Control / User Access Management
Objective: To ensure the authorized access to the systems and services / applications.

Registration and Deregistration	Only authorized users should be allowed to access systems and services. In order to identify the authorized users, a facility of registration and de-registration should be provided for every service. This will help enable the appropriate access rights.
Access Provisioning	A formal access provisioning of the users should be implemented. It will assign or revoke the access rights for the users.
Authentication Mechanism	Appropriate authentication mechanism such as password, OTP, Digital Certificate, PKI, Biometrics should be implemented for providing the access to the services. That access can be controlled based upon the data and service sensitivity and in accordance with the security policy of the state/organization/department.
Secured Log-in process	Every service/ application can be accessed only through the secured log-in mechanism based on the chosen authentication mechanism as per the policy of state/organization/department.
Access control to source code of the program	Access to program source code should be restricted.

Security Metrics

Information Security Reviews	
Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.	
Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.
Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
Technical compliance Review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

VIII. Security Policy Document

TABLE OF CONTENTS

1. INTRODUCTION

This section provides the information about what the security policy document covers and why is it required. It also mentions about various levels at which the security needs to be address. It provides information about the stake holders, various roles and responsibilities that are addressed in the security policy.

1.1 Purpose

It specifies the intension of the security policy document.

1.2 Scope

Specify the scope of the document in this section. Whom does which part of the policy apply.

1.3 History

The history of the document revision and the reason behind the change is specified here. A template table for the same is shown below

Table 1: Revision History Table template

Version	Description	From	To	Author	Reviewer	Reason for modification
1.0	Initial version	8/1/2017	7/1/2018	ABC	PQR	--

From – To date : The validity of the document is mentioned in from and to dates. Usually To date gives the date at a regular interval when it should be revised or atleast audited to check if any changes are required in the policy.

Author : Name of the author of the document.

Reviewer : Name of the policy reviewer.

Reason for modification: If any revision is made in the policy the reason for the policy should be mentioned here.

1.4 Responsibilities

Identify the roles and their responsibilities in order to enforce the policy. Below table gives the template for the same.

Table 2: Roles and Responsibilities Template

Roles	**Responsibilities**
Chief Information Officer	• Accountable for all aspects of the Organization's information security.
Information Security Officer	• Responsible for the security of the IT infrastructure. • Plan against security threats, vulnerabilities, and risks. • Implement and maintain Security Policy documents. • Ensure security training programs. • Ensure IT infrastructure supports Security Policies. • Respond to information security incidents. • Help in disaster recovery plans.
Information Owners	• Help with the security requirements for their specific area. • Determine the privileges and access rights to the resources within their areas.
IT Security Team	• Implements and operates IT security. • Implements the privileges and access rights to the resources. • Supports Security Policies.
Users	• Meet Security Policies. • Report any attempted security breaches.

1.5 General policy Definitions

List of all the policies that are related to this document should be listed here for reference.

2. IT Asset Policy

This section covers security policy regarding secured handling of IT assets.

Under IT asset policy there can be policy definitions such as-

- Every user is responsible for the preservation and correct use of the IT assets they have been assigned.
- Active desktop and laptops must be secured if left unattended.
- All desktops and laptops must have appropriate anti-virus installed and should be accessible only as the access control policy.
- Every desktop and laptop must have password protection as a minimum access control mechanism.
- Access to assets in the Organization location must be restricted and properly authorized, including those accessing remotely. Company's laptops, PDAs and other equipment used at external location must be periodically checked and maintained.
- The IT Technical Teams are the sole responsible for maintaining and upgrading configurations. None other users are authorized to change or upgrade the configuration of the IT assets. That includes modifying hardware or installing software.
- Disposal of the assets must be done according to the specific procedures for the protection of the information. Assets storing confidential information must be physically destroyed in the presence of an Information Security Team member. Assets storing sensitive information must be completely erased in the presence of an Information Security Team member before disposing.

3. Access Control Policy

   This section lists the policy related to access control of various kinds such as network access control, guest access control, remote access control etc.

   Under Access Control policy there can be policy definitions such as-

   - Any system that handles valuable information must be protected with a password-based access control system.
   - Any system that handles confidential information must be protected by a two factor -based access control system.
   - Discretionary access control list must be in place to control the access to resources for different groups of users.
   - Whenever possible, access should be granted to centrally defined and centrally managed identities.
   - Access shall be granted under the principle of "less privilege", i.e., each identity should receive the minimum rights and access to resources needed for them to be able to perform successfully their business functions
   - Users should refrain from trying to tamper or evade the access control in order to gain greater access than they are assigned.
   - Automatic controls, scan technologies and periodic revision procedures must be in place to detect any attempt made to circumvent controls.

4. Password Control Policy

   This section lists the policies regarding securing password control.

Under Password Control policy there can be policy definitions such as-

- Every user must have a separate, private identity for accessing IT network services.
- Identities should be centrally created and managed. Single sign-on for accessing multiple services is encouraged.
- Each identity must have a strong, private, alphanumeric password to be able to access any service. They should be as least 8 characters long.
- Each regular user may use the same password for no more than 90 days and no less than 3 days. The same password may not be used again for at least one year.
- Whenever a password is deemed compromised, it must be changed immediately.
- For critical applications, digital certificates and multiple factor authentication using smart cards should be used whenever possible.
- Identities must be locked if password guessing is suspected on the account.

5. Email Policy

This section covers the lists of policies for securing electronic mail.

Under Email policy there can be policy definitions such as-

- Use of official email address should be mandated for official work.
- Use of the Organization resources for non-authorized advertising, external business, spam, political campaigns, and other uses unrelated to the Organization business is strictly forbidden.
- Use of the Organization email resources is maintained only to the extent and for the time is needed for performing the duties. When a user ceases his/her relationship with the company, the associated account must be deactivated according to established procedures for the lifecycle of the accounts.
- Privacy is not guaranteed. When strongest requirements for confidentiality, authenticity and integrity appear, the use of electronically signed messages is encouraged. However, only the Information Security Officer may approve the interception and disclosure of messages.
- Scanning technologies for virus and malware must be in place in client PCs and servers to ensure the maximum protection in the ingoing and outgoing email.

- Security incidents must be reported and handled as soon as possible according to the Incident Management and Information Security processes. Users should not try to respond by themselves to security attacks.
- Corporate mailboxes content should be centrally stored in locations where the information can be backed up and managed according to company procedures. Purge, backup and restore must be managed according to the procedures set for the IT Continuity Management.

6. Internet Policy

   This section covers the lists of policies for securing Internet Access.

   Under Internet policy there can be policy definitions such as-

   - Limited access to Internet is permitted for all users.
   - The use of Messenger service is permitted for business purposes.
   - Access to pornographic sites, hacking sites, and other risky sites is strongly discouraged.
   - Internet access is mainly for business purpose. –some limited personal navigation is permitted if in doing so there is no perceptible consumption of the Organization system resources and the productivity of the work is not affected. Personal navigation is discouraged during working hours.
   - Inbound and outbound traffic must be regulated using firewalls in the perimeter. Back to back configuration is strongly recommended for firewalls.
   - In accessing Internet, users must behave in a way compatible with the prestige of the Organization. Attacks like denial of service, spam, fishing, fraud, hacking, distribution of questionable material, infraction of copyrights and others are strictly forbidden.
   - Internet traffic should be monitored at firewalls. Any attack or abuse should be promptly reported to the Information Security Officer.
   - Reasonable measures must be in place at servers, workstations and equipment for detection and prevention of attacks and abuse. They include firewalls, intrusion detection and others.

7. Antivirus Policy

   This section covers the lists of policies for securing using anti-virus and other forms of protection mechanisms.

   Under Anti-virus policy there can be policy definitions such as-

   - All computers and devices with access to the Organization network must have an antivirus client installed, with real-time protection.

- All servers and workstations owned by the Organization or permanently in use in the Organization facilities must have an approved, centrally managed antivirus. That also includes travelling devices that regularly connects to the Organization network or that can be managed via secure channels through Internet.
- Traveling computers from the Organization that seldom connect to the Organization network may have installed an approved antivirus independently managed.
- All the installed antivirus must automatically update their virus definition. They must be monitored to ensure successful updating is taken place.
- Visitors computers and all computers that connect to the Organization's network are required to stay "healthy", i.e. with a valid, updated antivirus installed.

8. Information Classification Policy

This section covers a framework for classification and the use of information according to importance and task.

Under Information classification policy there can be policy definitions such as-

- Information in the Organization is classified according to its security impact. The current categories are: confidential, sensitive, shareable, public and private.
- Information defined as confidential has the highest level of security. Only a limited number of persons must have access to it. Management, access and responsibilities for confidential information must be handled with special procedures defined by Information Security Management.
- Information defined as sensitive must be handled by a greater number of persons. It is needed for the daily performing of jobs duties, but should not be shared outside of the scope needed for the performing of the related function.
- Information defined as shareable can be shared outside of the limits of the Organization, for those clients, organizations, regulators, etc. who acquire or should get access to it.
- Information defined as public can be shared as public records, e.g. content published in the company's public Web Site.
- Information deemed as private belongs to individuals who are responsible for the maintenance and backup.
- Information is classified jointly by the Information Security Officer and the Information Owner.

9. Remote Access Policy

This section covers a security policy for remote access to the organization's resources.

Under Remote Access policy there can be policy definitions such as-

- To gaining access to the internal resources from remote locations, users must have the required authorization. Remote access for an employee, external user or partner can be requested only by the Manager responsible for the information and granted by Access Management.
- Only secure channels with mutual authentication between server and clients must be available for remote access. Both server and clients must receive mutually trusted certificates.
- Remote access to confidential information should not be allowed. Exception to this rule may only be authorized in cases where is strictly needed.
- Users must not connect from public computers unless the access is for viewing public content.

10. Outsourcing Policy

This section covers a security policy for outsourcing IT services, functions and processes.

Under outsourcing policy there can be policy definitions such as-

- Before outsourcing any service, function or process, a careful strategy must be followed to evaluate the risk and financial implications.
- Whenever possible, a bidding process should be followed to select between several service providers.
- In any case, the service provider should be selected after evaluating their reputation, experience in the type of service to be provided, offers and warranties.
- Audits should be planned in advance to evaluate the performance of the service provider before and during the provision of the outsourced service, function or process. If the Organization has not enough knowledge and resources, a specialized company should be hired to do the auditing.
- A service contract and defined service levels must be agreed between the Organization and the service provider.
- The service provider must get authorization from the Organization if it intends to hire a third party to support the outsourced service, function or process.

11. Network Policy

This section covers a security policy for network. The policy will contain other policy documents related to the network such as-

- Router and switch security policy
- Wireless communication policy
- Wireless communication standard

12. Server Security Policy

This section covers a security policy for servers. The policy will contain other policy documents related to the network such as-

- Database credential policy
- Information logging standard
- Server Security policy
- Workstation policy
- Lab security policy
- Technology equipment disposal policy

13. Application security Policy

<This section covers a security policy related to the application.>

Under application security policy there can be policy definitions such as-

- Web applications are subject to security assessments based on the following criteria:
  a) New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.
  b) Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.
  c) Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.

d) Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.

e) Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

- All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

f) High – Any high risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.

g) Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.

h) Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

- The approved web application tools for development are-

<tool 1>

<tool 2>

14. Annexures –

Note that each of the policy chapters or sections should have below subsections.

- Purpose
- Scope
- Policy Definitions

The template given here is the bare minimum fields. Each of the sections on policies covered in this template may have a detailed policy document.

IX. Framework for Strategic Control

The Figure below is a logical representation of the Scheme of Strategic Control. For the purpose of Strategic Control, the Security System depicted in the figure below and related requirements described in the following paragraphs include the Network System with all the relevant aspects of it.

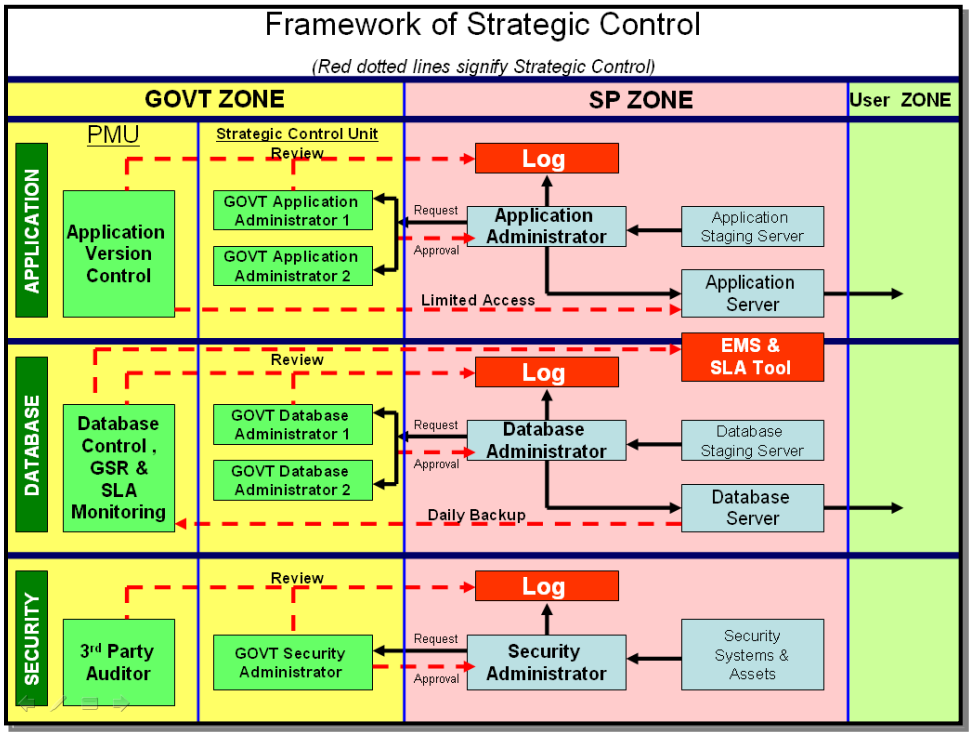


FIGURE IX.1: STRATEGIC CONTROL FRAMEWORK

The salient features of the Strategic Control Framework are explained below:

i. The scheme visualizes the entire e-Government system as consisting of 3 Zones – the Government Zone, the SP Zone and the User Zone, represented in yellow, pink and green background respectively in the figure.

ii. The scheme defines the requirements in 3 horizontal layers in a logical representation – Application, Database and Security. The requirements of Strategic Control of the Network System are subsumed in the Security layer.

iii. The scheme envisages a hierarchical system of exercise of privileges across the 3 zones. The User Zone confers privileges that are required to access the system for making requests and to operate the system for effective transactions in the course of providing services. As this is purely operational and not strategic in character, User Zone is not further elaborated in the scheme.

iv. The SP Zone relates to the development and production environments at the central system level controlled by the SP. The privileges in this zone relate to administration of the application, database, and security at a high level subject to certain permissions and approvals required from the administrators operating in the Government Zone as defined in the Security and Access Control Policy

v. The Government Zone contains the highest level of privileges exercised over a system to ensure realization of the primary objectives. The Government Zone itself consists of two compartments, one relating to a set of administrators to exercise privileges of the highest order and the other relating to the privileges exercised by the PMU. **The technical personnel of Government shall be associated with the design and development phase of the Project and continue through the life of the project.**

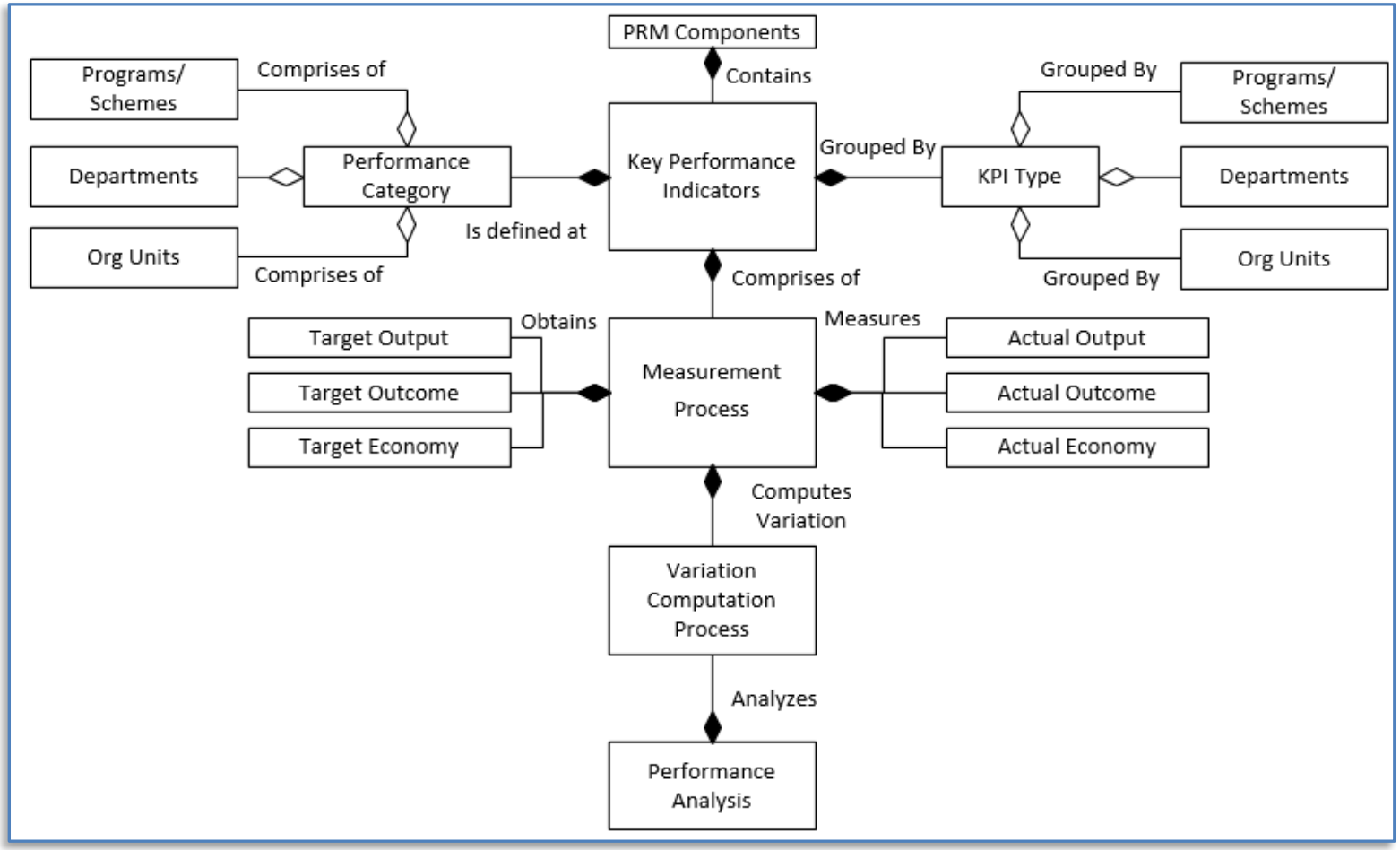
vi. The red dotted lines signify the strategic control that the personnel operating in Government Zone exercise over the system.

vii. In the following sections, we lay down certain high level requirements and norms for specifying the privileges to be exercised by personnel operating in the SP Zone and Government Zone in the three areas, namely, application, database and security. The scheme at the same time envisages that the precise rules and privileges at various levels are defined by the SP during the design phase of the SDLC and get the same approved by the Government before entering the development phase.

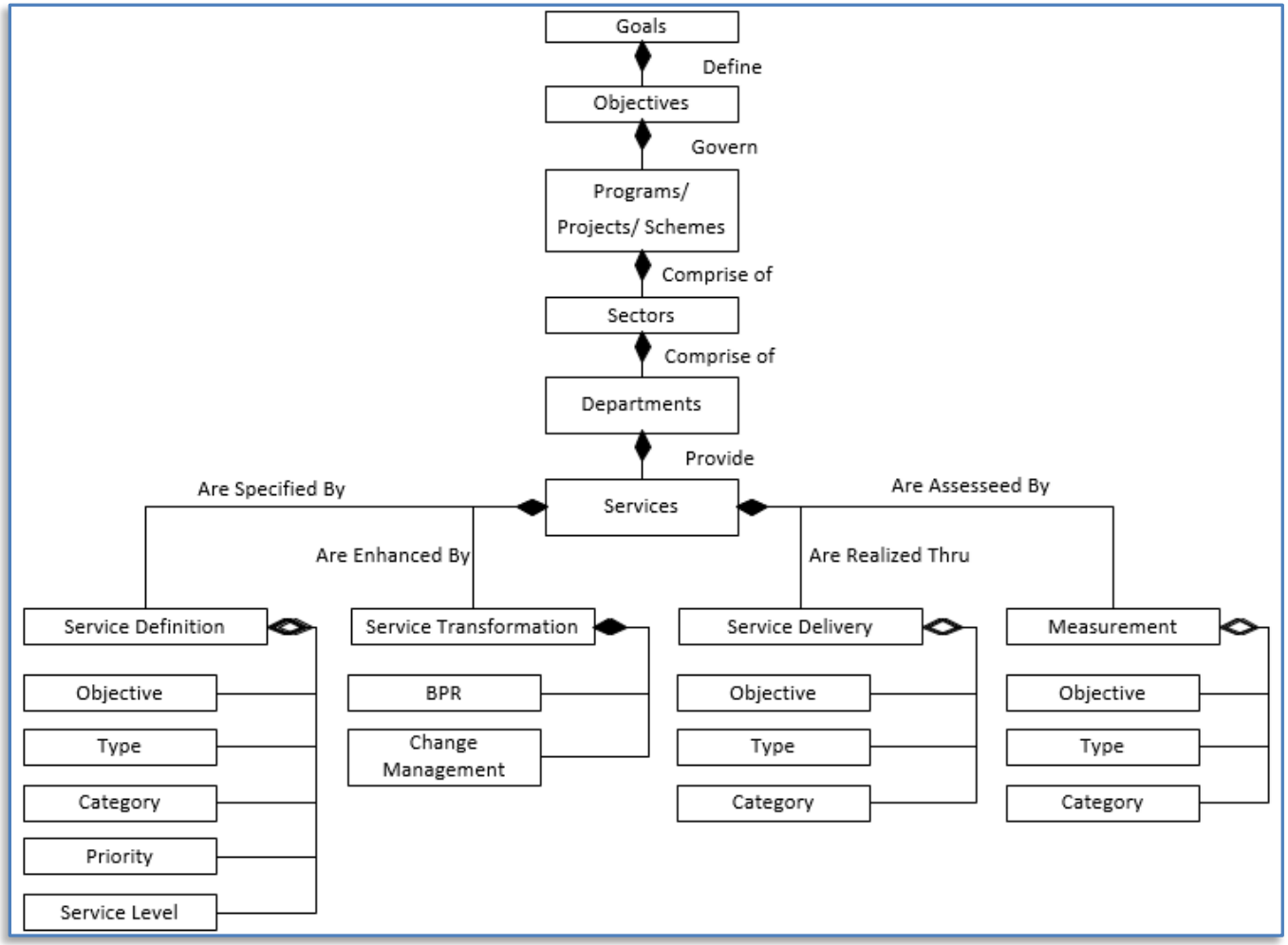
viii. The Strategic Control framework also envisages that the bidders responding to a public sector RFP provide a specific solution that addresses the requirements of Strategic Control, as a part of their technical proposal.

X. Reference Models in UML Notations

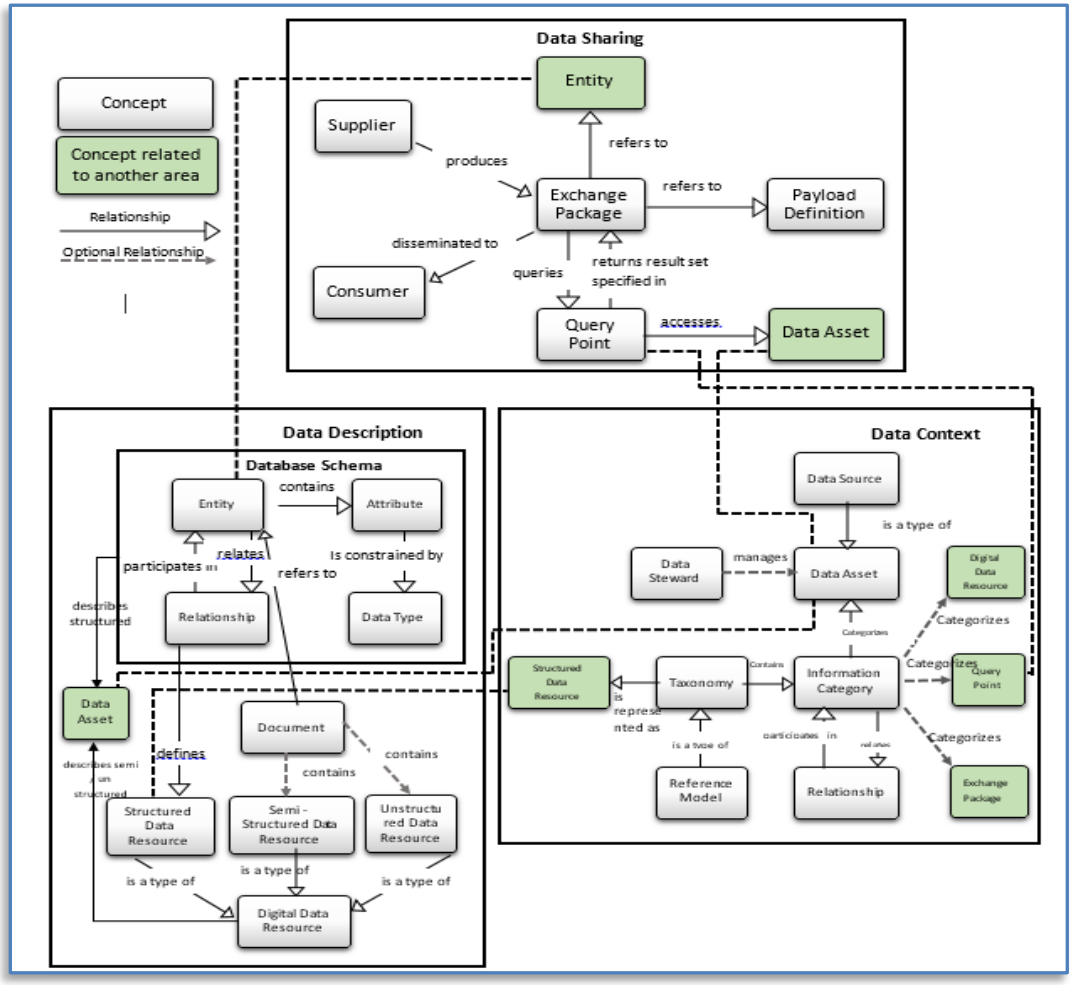
Performance Reference Model



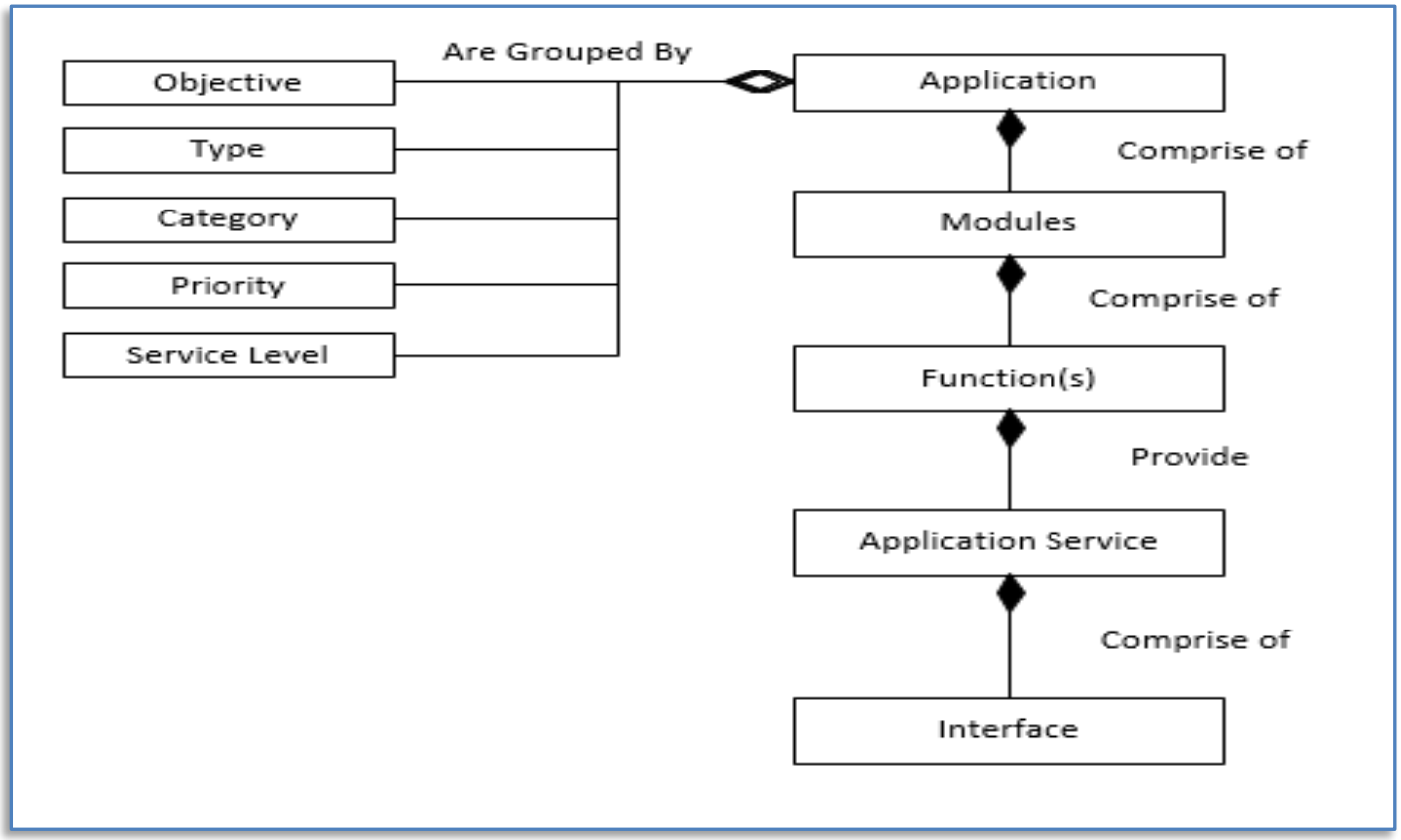
Business Reference Model



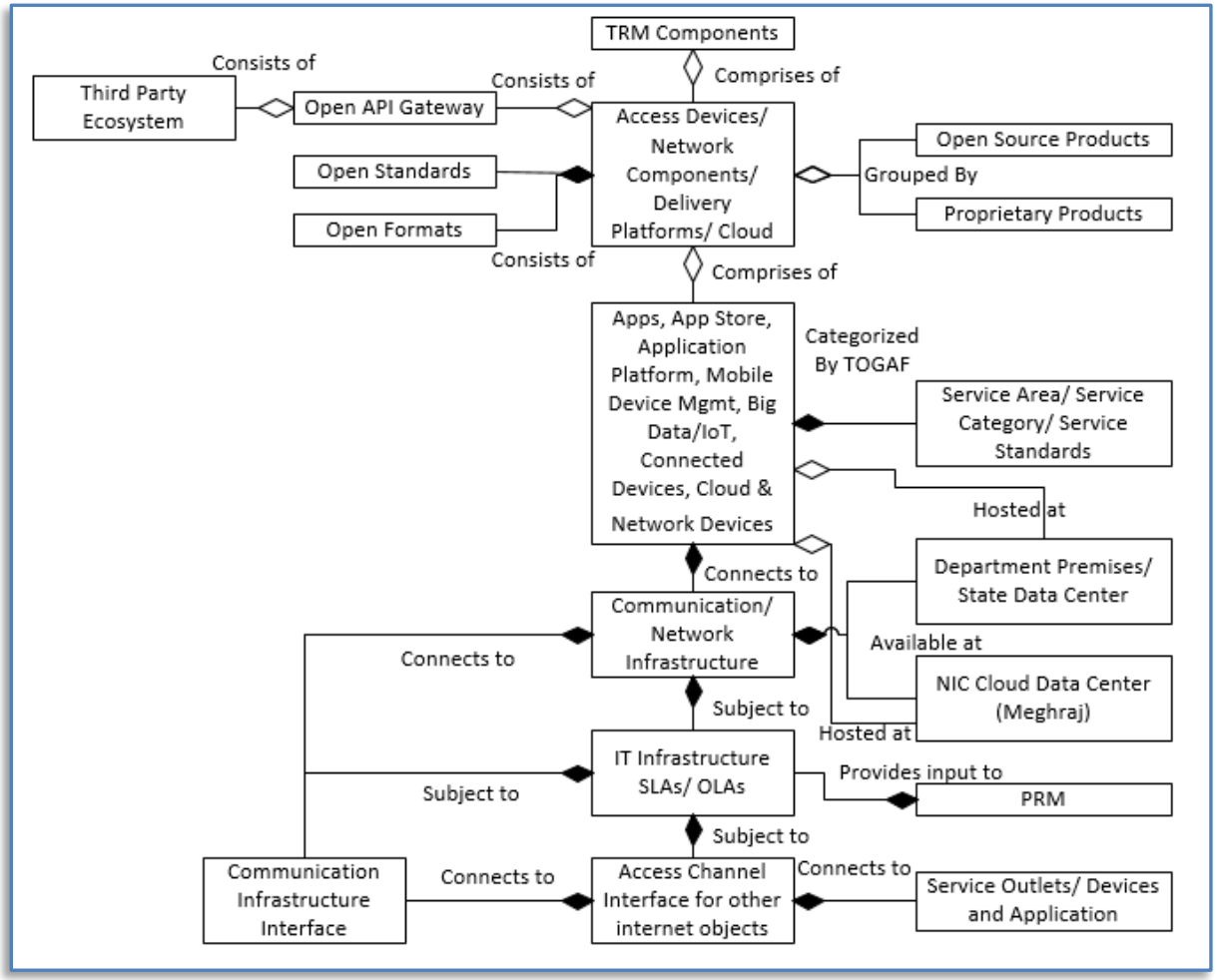
Data Reference Model



Application Reference Model



Technology Reference Model



XI. List of Acronyms

Sl.#	Acronym	Full Form
1	**PRM**	**Performance Reference Model**
2	KPI	Key Performance Indicator
3	SLA	Service Level Agreement
4	**BRM**	**Business Reference Model**
5	BPR	Business Process Re-engineering
6	BLA	Business Level Agreement
7	OLA	Operation Leve Agreement
8	WoG	Whole of Government
9	G2C	Government to Citizens
10	G2B	Government to Business
11	G2G	Government to Government
12	G2E	Government to Employee
13	**DRM**	**Data Reference Model**
14	DBMS	Data Base Management System
15	DR	Disaster Recovery
16	**ARM**	**Application Reference Model**
17	SOA	Service Oriented Architecture
18	ReST	Representational State Transfer
19	HTTP	Hyper Text Transfer Protocol
20	LoB	Line of Business
21	IAMS	Identity and Access Management
22	HRMS	Human Resource Management System
23	RTI	Right to Information
24	GIS	Geographical Information Centre
25	IFEG	Interoperability Framework for e-Governance
26	CSS	Closed Source Software
27	SQuaRE	Systems and software Quality Requirements and Evaluation

28	ASD	Adaptive software development
29	AUP	Agile Unified Process
30	DSDM	Dynamic systems development method
31	XP	Extreme programming
32	RAD	Rapid application development
33	**TRM**	**Technical Reference Model**
34	SMAC	Social Media, Mobile, Analytics and Cloud
35	ROA	Resource Oriented Architecture
36	IoT	Internet of Things
37	VM	Virtual Machine
38	IaaS	Infrastructure as a Service
39	PaaS	Platform as a Service
40	VPN	Virtual Private Network
41	DDD	Domain Driven Design
42	BPML	Business Process Modeling Language
43	**IRM**	**Integration Reference Model**
44	EAI	Enterprise Application Integration
45	MFT	Managed File Transfer
46	SOA	Service Oriented Architecture
47	ESB	Enterprise Service Bus
48	API	Application Programming Interface
49	iPaaS	Integration Platform as a Service
50	QoS	Quality of Service
51	**SRM**	**Security Reference Model**
52	DLP	Data Loss Prevention
53	SOP	Standard Operating Procedure
54	CC	Common Criteria
55	SIM	Security Information Management
56	SEM	Security Event Management
57	VAPT	Vulnerability Assessment and Penetration Testing
58	SDC	State Data Centres

59	NAC	Network Access Control
60	WPA	Wi-Fi Protected Access
61	WEP	Wired Equivalent Privacy
62	GDCC	Govt. Desktop Core Configuration
63	ITSRA	Insider Threat Security Reference Architecture
64	SEI	Software Engineering Institute
65	**IGRM**	**India Governance Reference Model**
66	ACM	Architecture Capability Maturity
67	PMU	Program Management Unit