सत्यमेव जयते
Ministry of Education
Government of India

OPEN STANDARDS & SPECIFICATION FOR National Digital Education Architecture (NDEAR)

11th November 2022

TABLE OF CONTENTS

List of Figures

List of Tables

List of Abbreviations

AI	Artificial Intelligence
API	Application Programming Interface
AR/VR	Augmented Reality/Virtual Reality
CBSE	Central Board of Secondary Education
BRC	Block Resource Center
CCC	Command and Control Center
CEO	Chief Executive Officer
CIET	Central Institute of Educational Technology
CRC	Cluster Resource Coordinator
CSC	Common Service Center
CSR	Corporate Social Responsibility
CWSN	Children with Special Needs
DIKSHA	Digital Infrastructure for Knowledge Sharing
DoSEL	Department of School Education and Literacy
DSEP	Decentralized Skills and Education Networks
ECCE	Early Childhood Care and Education
EdTech	Education Technology
FLN	Foundational Literacy and Numeracy
GSTN	Goods and Services Tax Network
HPC	Holistic Progress Card

ICT	Information and Communication Technology
ID	Identity Document
IDER	India Report on Digital Education
IEC	Information, Education and Communication
IndEA	India Enterprise Architecture
ISO	International Organization for Standardization
IVR	Interactive Voice Response
KPI	Key Performing Indicator
MeitY	Ministry of Electronics and Information Technology
MIS	Management Information System
ML	Machine Learning
MOE	Ministry of Education (formerly known as Ministry of Human Resource Development (MHRD))
MOHFW	Ministry of Health and Family Welfare
MSDE	Ministry of Skill Development & Entrepreneurship
NAS	National Assessment Survey
NCERT	National Council for Education Research and Training
NDEAR	National Digital Education Architecture
NDHM	National Digital Health Mission
NDSP	National Data Sharing Policy
NEP 2020	National Education Policy 2020
NETF	National Educational Technology Forum
NGO	Non-Governmental Organisation

NIC	National Informatics Centre
NITI Aayog	National Institution for Transforming India
NODE	National Open Digital Ecosystems
NPCI	National Payments Corporation of India
NROER	National Repository of Open Educational Resources
ORF	Oral Reading Fluency
OTP	One-Time Password
PAN	Permanent Account Number
PARAKH	Performance Assessment, Review, and Analysis of Knowledge for Holistic Development
PDP Bill	(Indian) Personal Data Protection Bill, 2019
PII	Personally Identifiable Information
PM WANI	Pradhan Mantri Wireless Access Network Interface
PMU	Programme Management Unit
PSC	Project Steering Committee
PSSB	Professional Standard Setting Body
QuML	Question Markup Language
SAS	State Assessment Survey
SCERT	State Council of Educational Research and Training
SDG	Sustainable Development Goals
SMS	Short Message Service
SOFIE	Specification for Open Feature Integration and Extensions

SoR	System of Record
SQAAF	School Quality Assessment and Accreditation Framework
SSA	Sarva Shiksha Abhiyan
SWAYAM	Study Webs of Active-Learning for Young Aspiring Minds (https://swayam.gov.in/about)
TERM	Teacher Energized Reference Manual
TLM	Teaching Learning Materials
UDISE+	Unified District Information System for Education
UIDAI	Unique Identification Authority of India
UNICEF	United Nations Children's Fund
UT	Union Territory
UX	User Experience
VOIP	Voice over Internet Protocol
WCD	Ministry of Women and Child Development

Executive Summary

Standards bring order from chaos and allow us to understand our world in ways that would not be possible otherwise. For example - The International Standards Organization (ISO) defines a standard as “a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose.”

We encounter standards daily. We have standard ways to measure time, distance, and volume. Imagine how difficult it would be to compare products in the supermarket if there were no standards for weight or volume. Without the English and Metric systems of weights and measures, products like milk would be sold in arbitrarily sized containers without a label. You wouldn’t know how much milk you were getting or even if it was the right type of milk. We depend on containers of milk either to use a standard size, such as “one liter,” or to provide labelling indicating “how much” (weight and volume) and “what” (type and ingredients).

Just as standards for weight or volume or labelling enable the consumer to make informed choices regarding appropriateness and content in the supermarket, education standards can ensure that services and support are efficiently and effectively made available to all students, enabling evidence-based and equitable education delivery.

NDEAR envisages the evolution of an entire ecosystem in the education sector to provide a wide range of services to the stakeholders in a digitally enabled manner. Such seamless and boundary-less interoperability is possible only if all the building blocks and the digital systems are built using the defined standards which are openly licensed, accessible, and usable by the whole ecosystem.

It is important to understand who will be using these standards. The sheer size and variety of education data stakeholders is the most important reason for data standards. At the classroom level, the student, the student’s parent or guardian, and the teacher will view education data, education standards, and education vocabulary through their own lenses. Add to that the principal, the counsellor, the superintendent, a variety of program staff, the school board, education programs and organizations within the community, and the entire community itself. Also included at the local level are the IT staff responsible for integrating multiple systems of data and analysts who conduct research to inform all the above.

Beyond the local level, the audience grows even more to include education software vendors, education organizations, central and state education staff, legislators,

policymakers, researchers, and the public. Each audience member will engage education data standards at different times and for different reasons. This expansive breadth of audience requires substantial consideration to ensure all are informed and that information is consistently defined and understood.

NOTE:

The document is in public domain with the caveat that the policies are dynamic by nature and will be adapted, modified or edited based on industry and market needs. This is the first step towards building the architecture.

Scope of this document

NCERT has adopted 6 standards in DIKSHA (all except DSEP) and are proposing them to be adopted as NDEAR standards. For DSEP, NCERT is looking to adopt the DSEP for DIKSHA ecosystem in context to mentoring and content platforms interoperability. NCERT proposes that they will engage with the relevant communities for each standard to evolve.

Standards	DSEP	QuML	Learning Object Model	DIAL	SOFIE	Telemetry	Verifiable Credentials and INCOMS	SCORM
Learning	✓	✓	✓	✓	✓		✓	
Admin	✓							
Content		✓	✓	✓			✓	✓
Technology					✓	✓	✓	
Open Data & Analytics						✓		
Federated Identities							✓	
Registries							✓	
Governance							✓	
Admin							✓	
Reference Data				✓				

Table 1: Adoption Matrix

Further, this document briefly addresses the types of currently available education standards and then focuses specifically on an entry-level view of education data standards that can be leveraged for NDEAR. The intent is to bring together a compendium of EdTech standards to provide a starting point for education stakeholders and not to be exhaustive. It focuses specifically on the Open Education Data Standards. It does not include technical standards related to learner facing systems or general technical standards that are used within education systems (e.g., internet protocols). Where relevant, the document provides links and resources to enable further knowledge development for the reader.

NDEAR - Technology Architecture and Standards

The NEP 2020 has defined the vision of 'education for all'. Continuum of services is a concept strongly advocated by the NEP 2020. These policy goals are sought to be achieved by refactoring the existing schemes and introducing several new schemes including some digital initiatives. NDEAR envisions digital infrastructure for school education that allows all ecosystem actors across government, civil society, and market players to build and innovate platforms, solutions and tools that are compatible or compliant with NDEAR. The core of NDEAR provides the following:

1. Specifications & Standards: A set of nationally interoperable standards and specifications allowing interoperability and portability across all systems.

2. Microservices & APIs: A set of unbundled services deployed in a federated manner and available via APIs, which can be used by the ecosystem to build and innovate solutions to address the diversity and scale.

3. Reference Solutions: A set of reference solutions and apps that can be deployed in a federated manner and used freely out of the box by students, teachers, parents, administrators, and community members.

All these aspirations can be realized principally by leveraging the power of digital technologies. In the context of India, with its size and diversity, this mammoth task requires that a holistic, comprehensive, and interoperable digital architecture is crafted and adopted by all the stakeholders. In the absence of such architecture, the use of technology in the education sector will continue to grow in an uneven manner and in silos.
Digital technologies have proliferated in school education, and its outreach is continuously increasing. Digital technologies are enabling students, teachers, and administrators to impart quality education and overcome the challenges in school

education. An overview of the government-led education technology landscape (indicative, not a complete list) is shown below along with the India Stack Infrastructure.

NDEAR Architecture Principle

Technology Architecture Principles

The governments, Central and State, must play the role of facilitators, enablers, and advocates of these principles to speed up the evolution of the National Digital Education Ecosystem.

#	Principle	Description
1	Adopt India Enterprise Architecture (IndEA) framework	The artifacts prescribed by the IndEA Standard will be prioritized and sequenced. The design of the building blocks of NDEAR will adapt and conform to IndEA by default. Other national and international standards will be adopted in areas not covered by IndEA. NDEAR shall adopt the latest version of the India Enterprise Architecture (2.0) Framework or any other appropriate framework at the appropriate time.
2	Built on open-source, built as open-source, and using open standards	All services (except which are notified as sensitive) built into the digital infrastructure (core of NDEAR) should be based on and built as open source, whenever possible, ensuring vendor neutrality, transparency, and strategic control of the core digital infrastructure. Applications that are built aligned with NDEAR may choose to use non-Open-Source Software, especially when these applications are built outside the Government (private school apps, etc.). In addition, open international and national

#	Principle	Description
		standards should be adopted when available and new standards should be created, when necessary, to ensure interoperability and portability. Open standards and specifications must also be regularly upgraded, new specifications introduced as open source using experts from the community.
3	Portable	Design for portability of data, certificates, credentials, documents, content, etc. based on open standards.
4	Scalable	All technology services and processes that are part of NDEAR must be designed for operating at the intended scale (be at Global country scale or State or local scale). Extreme automation, distributed human processes etc. are key aspects for overall system scale and manageability.
5	Resilient	Services that are part of NDEAR must be built to withstand failures by building automated recoveries and adaptation. Similarly, all processes established as part of NDEAR must be designed to allow flexibility and re-adaptation to handle disruptions.
6	Interoperable via open APIs and standards	Design interoperability via open APIs and open standards to support federated design principles, so that various solutions built by the ecosystem can work in a unified manner.
7	Use of emerging technologies	NDEAR should be architected to leverage various technology innovations as and

#	Principle	Description
		when they become viable and useful to improve education.
8	Open Data and Observability via “data emit”	By design, NDEAR services must be built to emit anonymized telemetry events for generating aggregate open data, understanding system behaviour, supporting policy evolution, etc. Multiple data entries and time-consuming data extractions etc. must be eliminated. All such open data must be made available as “public good” for access by all for enhancing research, interventions, policies, solutions, and overall understanding of the effectiveness of the education system as per National Data Sharing and Accessibility Policy.
9	Minimal, reusable, unbundled microservices	Core NDEAR services must be minimal (both data and functional minimalism), atomic, and generalized, allowing solution builders to “reuse and extend” them to build contextual solutions. All services that are part of NDEAR are to be designed in a “generalized” manner to allow diverse use cases to be built on the same set of services. These generalized services must “externalize” its configurability and expose various configurations within the API itself to allow solution building across diverse contexts.
10	Security, Privacy, Trust, Data Empowerment by Design	Security of services and data should be designed into all blocks of NDEAR using strong security design principles. Security should be baked into all aspects of a digital system. All solutions and services within

#	Principle	Description
		NDEAR must adhere to appropriate data protection and privacy laws.
11	Registries and Master codes as Single Source of Truth	Considering NDEAR being a federated architecture with decentralized systems and applications, for interoperability and unification, it is essential that various master codes and decentralized electronic registries are established and made available via common APIs. The discovery of decentralized services and registries also need meta registries (registry of registries or service discovery registry) and should be designed into the architecture.
12	Evolvable	NDEAR architecture and the building blocks of the digital infrastructure should not be thought of as a one-time exercise, rather, an evolving construct. Given the large and diverse ecosystem of actors and applications, it necessitates all NDEAR building blocks to be clearly versioned, backward compatible, and have well-defined and transparent version retirement policies. This is to ensure that various applications/systems depending on NDEAR can adopt and upgrade asynchronously at their pace and evolve along.

Table 2: NDEAR Architecture Principles

Federated Architecture and Building Blocks

Digital technologies are playing an important role in school education today. NDEAR provides an approach to establish a “Federated Architecture”, defined in terms of its building blocks. The federated architecture approach seeks to enable the education

ecosystem by streamlining information flows across players in the ecosystem, while keeping student/ teacher, their privacy and confidentiality of data at the forefront. A good design can help accelerate the adoption and improve the delivery of education services across both the public and private sectors, while also addressing the digital divide through innovative integrated solutions across digital-physical contexts. NDEAR identifies key building blocks by looking at the most common requirements of the overall education ecosystem.

Federated Architecture

Federated architecture (FA) is a pattern in enterprise architecture that allows interoperability and information sharing between semi-autonomous, de-centrally organized entities, information technology systems and applications. For ensuring the security and privacy of personal and sensitive information of students/ teachers, while ensuring interoperability, technological flexibility and independence, the federated architectural pattern in NDEAR is essential. Such an architectural pattern is also ideally suited to the conditions prevalent in a federal set up like India and includes both public and private institutions.

Salient Features of Federated Architecture

The following are the salient features of the architecture:

i. The federated architecture is indicative. It can be modified, enhanced, and evolved with time.

ii. The federated architecture is modular in nature. The combination of modules necessary at each level/ setting will be decided while designing the information systems.

iii. The architecture is laid out at various administrative levels (National, State/UT/Board and Local(school/student) level) as well as educational societies and other accreditation bodies.

iv. Each administrative level may have one or more building blocks representing key interactions.

v. The 36 building blocks within 12 categories across 3 administrative levels are loosely coupled on a ‘need to connect’ basis, using standardized API’s and open specifications. The principles laid out within NDEAR are applied at each level and layer, and in the design of these building blocks.

vi. To ensure data consistency, interoperability, and national portability, only the minimum required number of building blocks are designed, developed, open sourced, held and managed centrally.

vii. Open interoperable standards, specifications, and protocols are developed in a collaborative manner, and maintained at the national level to ensure national interoperability and portability.

viii. “Reference Applications” at various levels should be designed and developed as reusable, multitenant, open-source and standards-compliant applications, made available to all via open-source repositories, websites, and/or app stores.

ix. Data shall be maintained at different levels where data is generated called the “System of Record (SoR)”. All the technology requirements, legal data protection and empowerment aspects, and specifications of data shall be supported appropriately within each SoR. It may be observed that each education data type (including master and transaction data) is maintained at one level only within an SoR (be at Central or State or school level), to ensure uniqueness and consistency. For instance, a student’s education record is maintained by the school level and is made available digitally through local or national lockers, where such data links can be maintained. All user data should be in the control of the user and made portable as per Data Empowerment and Protection Architecture (DEPA) principles in accordance with the Personal Data Protection bill.

x. A repository of standards and master codes shall be maintained at the national level as electronic registries with open APIs, for various systems to integrate. All registries shall conform to well documented, standard search/ access APIs with published schemas.

As you can see in the above below, NDEAR is not envisaged to be a set of central applications, rather a set of core building blocks along with few reference applications running in a federated manner across Center, State/board, and school levels. Around the whole stack, across levels, are ecosystem partners who can use, contribute, and

extend NDEAR services and applications to provide contextual learning environments to students and teachers.

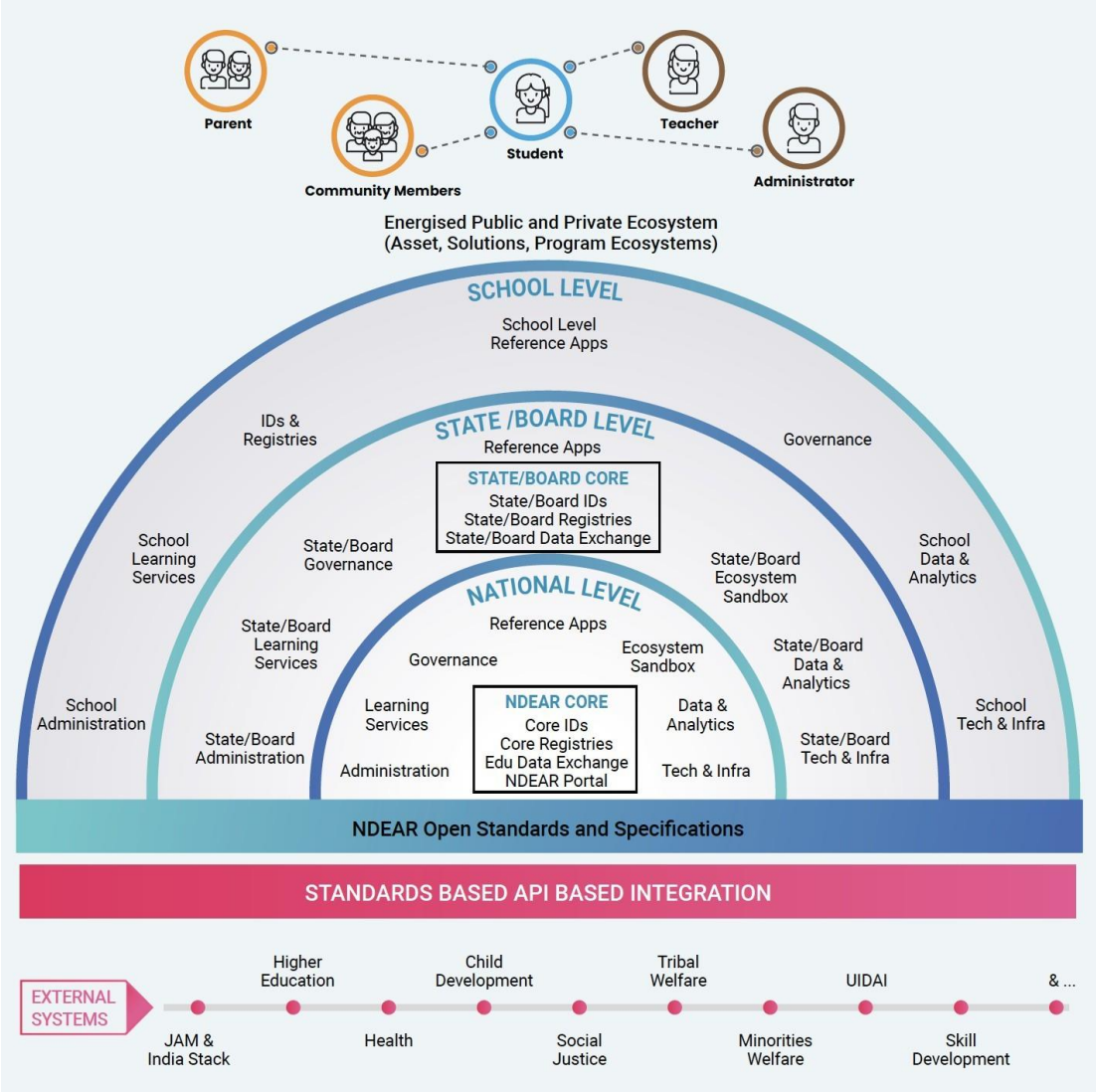


Figure 1: Federated Architecture

Building Blocks

A building block is a package of self-contained functionalities defined to meet business needs through a set of services made available via APIs and optionally via reference solutions. Building blocks must interoperate with other building blocks within the same system and across other systems. A good choice of building blocks will facilitate legacy system integration, improved interoperability, and flexibility in the creation of new systems and applications.

Characteristics of Building Blocks

In addition to adherence to technology architecture principles laid out earlier, each building block must have the following characteristics:

i. Provide a standalone, useful, reusable, interoperable, and implementable set of services.
ii. Cross-functional across the value chain by design.
iii. Applicable to multiple use cases in the education domain.
iv. Ensure evolvability to ensure it is independently evolving.

Building blocks within India Stack are great examples of designing self-contained, reusable, services. All building blocks must adhere to the architecture principles laid out in this document. Typically, each building block has two parts:

i. A set of microservices powering the functionality, with well-documented open APIs for other systems to integrate.
ii. A set of interfaces (mobile, Web, SMS, etc.) that allow users to interact.

Each building block within NDEAR must be owned by a national, State, or local institution, having clearly defined roles for 'Business Ownership' and 'Technology Ownership'. While all minimum viable blocks are core to NDEAR, registries and master codes form the centrepiece for integration with all the other blocks and solutions. These federated registries allow master data and user/entity profile data to be maintained in an interoperable fashion with trustworthy attestations under user control. Identification of new blocks and adding new services within each block is an ongoing activity.

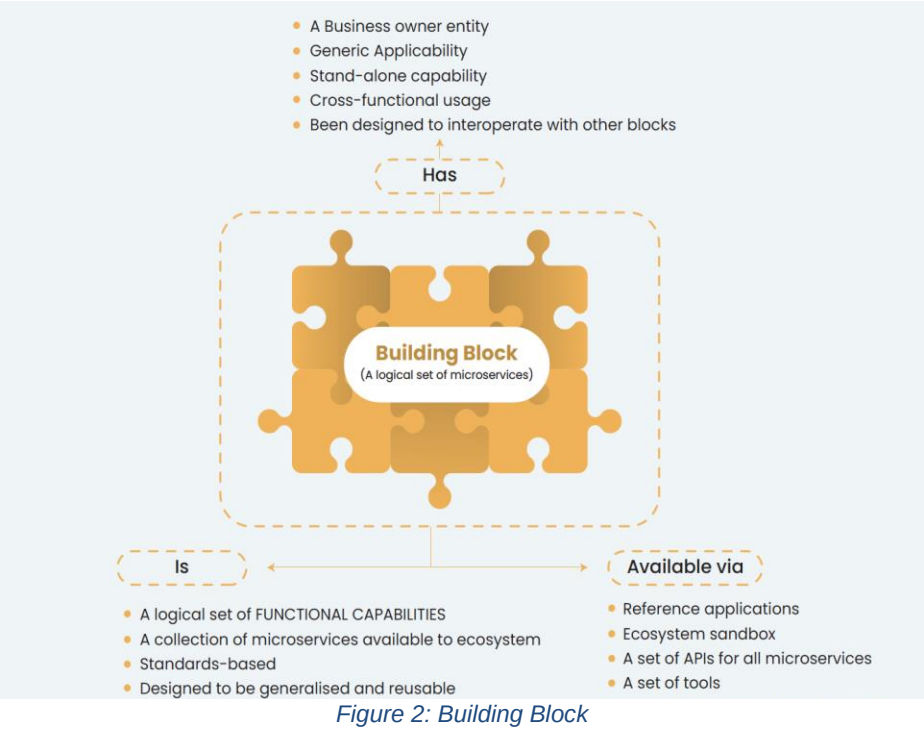


Figure 2: Building Block

Building Blocks of NDEAR

Based on detailed studies of the existing education systems and discussions with stakeholders, 12 key building block categories consisting of 36 minimum viable Building Blocks have been identified within NDEAR across the 3 administrative levels. NDEAR differentiates its building blocks into the following to help classify and develop them during its evolution:

Core Building Blocks

These constitute those building blocks that are necessarily built and managed as public goods and not given to the ecosystem to build. These are typically created and maintained at the National/State/ Board Level (in a federated structure). These building blocks enable interoperability and act as glue between the rest of the building blocks and various solutions built on top. Core building blocks such as electronic registries, identities, etc. also act as Single Source of Truth and/or System-of-Record (SoR). Core building blocks are offered as hosted services/applications at appropriate administrative levels. Core building blocks necessarily must adhere to the architectural principles of NDEAR to ensure interoperability and combinatorial solution building.

Common Building Blocks

These constitute those building blocks that are built and offered as a choice to all the NDEAR ecosystem. Like other building blocks, these may also be created and maintained either at the Centre or at State/board levels. Like core building blocks, common building blocks are also offered as a hosted services/application at the appropriate administrative level, except that these are offered as an option and the ecosystem may build alternative/enhanced versions of these to provide further choice.

Reference Building Blocks

These constitute those building blocks that are built and offered only as “source code/data” to enable various ecosystem players to rapidly build their services/ applications. These are to be seen as “accelerators” and unlike Core and Common building blocks these are not offered as a hosted service/application.
All building blocks across Core, Common, and Reference should be organized well to allow easy discovery and reuse through machine readable catalogues, directories, and dictionaries within NDEAR Portal. At the time of developing various Building Blocks identified within NDEAR, it must be classified into any of the 3 (Core, Common, Reference) and organized.

As depicted in the figure above, NDEAR comprises 36 minimum viable building blocks across the following 12 categories:

1. Open Standards & NDEAR Portal
2. Federated Identities
3. Reference Data
4. Infrastructure
5. Technology
6. Governance
7. Administration
8. Content
9. Learning
10. Reference Solutions UX
11. Open Data & Analytics
12. Ecosystem Sandbox

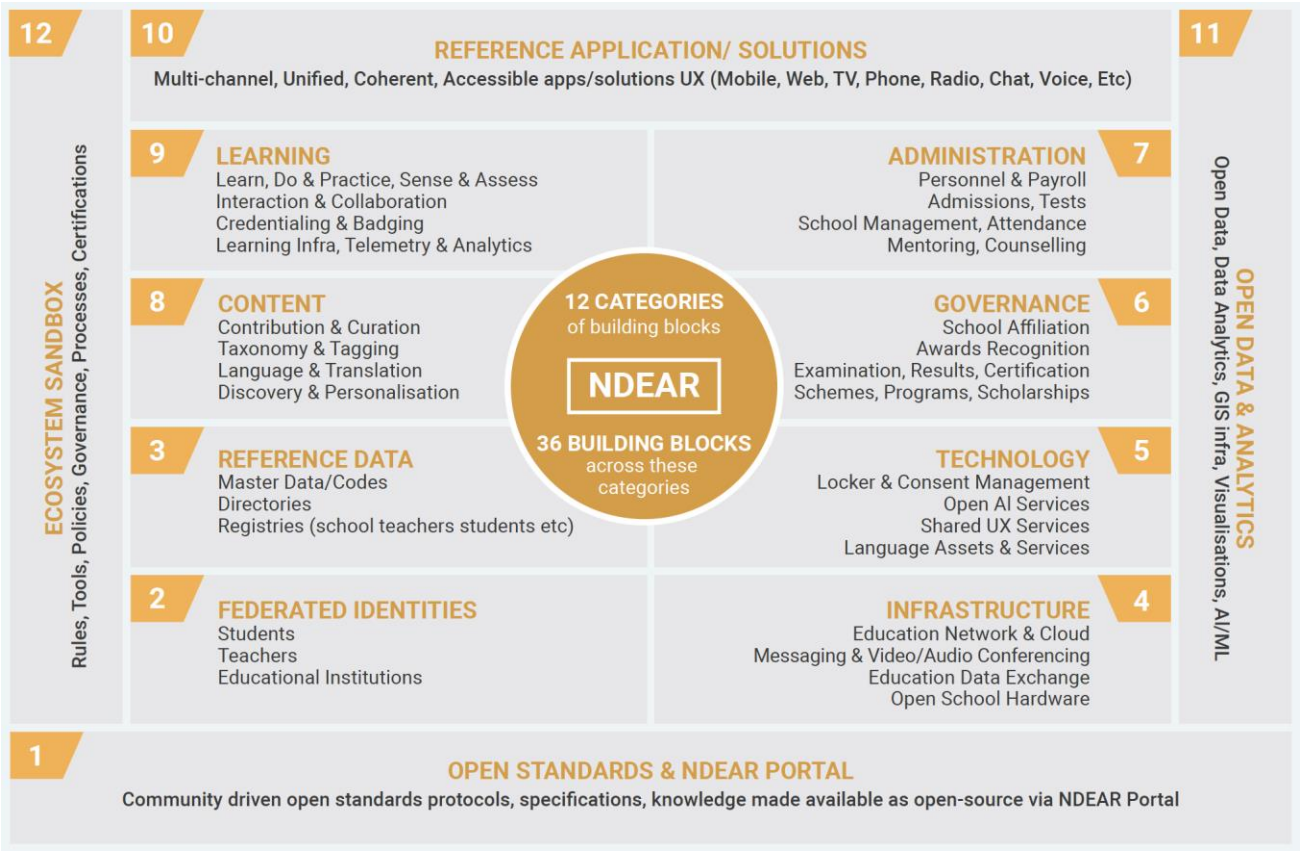


Figure 3: NDEAR Building Blocks

NDEAR envisages the evolution of an entire ecosystem in the education sector to provide a wide range of services to the stakeholders in a digitally enabled manner. Such seamless and boundary-less interoperability is possible only if all the building blocks and the digital systems are built using the defined standards which are openly licensed, accessible, and usable by the whole ecosystem.

The objective of this section is to identify the standards required for ensuring interoperability and portability within the National Digital Education Ecosystem. It is proposed to recommend a set of minimum viable standards in the initial stages. The scope of the standards is defined keeping the foregoing in view. The table below depicts the areas chosen to define the standards for NDEAR.

#	Category	Purpose

#	Category	Purpose
1	Learning Environment	Standards related to schools and other learning environments and its evaluation
2	Consent	Consent from students/ parents need to be covered from two perspectives — consent for data collection and for data use
3	Content	Standards related to educational content creation
4	Interoperability	Standards related to exchange of education data
5	Assessments & Results	Standards related to assessments and harmonization of marks
6	Privacy & Security	Standards related to data privacy (through access control) and security of data at-rest and at-motion. Also, aspects such as data immutability and non-repudiation with audit trail
7	Application design & development	Standards related to design and development of applications including the UI/UX.

Table 3: NDEAR Standards

SECTION A:

A1. OPEN STANDARDS & NDEAR PORTAL

Community driven open standards protocols, specifications, knowledge made available as open source via NDEAR Portal.

a. Open Standards

NDEAR being a federated architecture, various applications are expected to be deployed across Government, society, and market actors. Given this decentralised design, to ensure that these applications interoperate in a unified manner by providing a seamless experience to its users, it is necessary to define national level open standards. This also ensures the portability of assets and data across States and applications. Defining national level standards (or, in some cases global level standards) is also critical for governance, strategic control, data security, privacy, and overall compliance. Hence this is one of the key building blocks that cut across all building blocks of NDEAR and across all administrative levels. Later in this section, the standards and recommended specifications are provided in detail. Note that these are evolving in nature and hence this list should not be construed as the only and final list. With time, these standards need to be updated, new ones introduced, and old ones retired.

b. NDEAR Portal

Considering NDEAR is an evolving, ecosystem enabling architecture, it is essential that all the architecture artifacts, documents, standards, governance, directories (of building blocks and compliant applications), collaboration, etc. are managed through a single public facing website. This is the sole purpose of the NDEAR Portal. Bringing the NDEAR artifacts and governance through the common portal allows it to be a living and ever evolving architecture, with strong collaboration with the ecosystem. The institution who is the custodian of NDEAR will be in charge of this portal.

A2. FEDERATED IDENTITIES

This category provides the fundamental building blocks that manage the key entities and their identities required for any ecosystem transaction/ interaction.
Digital identity, of people, things, and entities, plays an important part in building interoperable and portable assets and experiences for users. Given the decentralized architecture of NDEAR, it is essential to understand that even the IDs will be defined, managed, and captured in a decentralized manner. The essence of an ID is to provide unified control to the subject represented by the ID (or owner of the subject represents a “thing” such as devices). The ID enables the subject to be able to obtain, manage, control attributes, receive attestations, manage profile and transaction data attached to that ID, consent to one’s own profile and/or data, if required revoke, and manage the lifecycle. A digital identity system typically provides the following core capabilities:

i. Management: creation, updates, lifecycle management, and protection of the ID.
ii. Authentication: verifying ID claim by the requesting party of the ID holder using one or more factors (Password, OTP, biometrics, etc.).
iii. Attestations: receive, attach, consent, share attestations that are stored against specific attribute/ attribute-set in the ID (e.g., if ID profile has an address, ability to have a digital proof of address or if ID has an academic qualification, the ability to have digital proof of the qualification, etc.) Given India’s large diversity and education levels, it is essential that the architecture of Government systems be that of supporting diversity and be most inclusive. While the intent of the State is to care for the
vulnerable and poor, systems must still be designed to provide agency and choice to people.

Understanding Uniqueness

The uniqueness of ID is an important subject to explore. It is essential to understand if the “uniqueness” is from the ID owner perspective or from the perspective of the State. These two are fundamentally different and both are necessary for different purposes. State enforcing uniqueness must be used sparingly and only when it is necessary. The Supreme Court of India clearly articulated the need to have privacy as a fundamental right, while allowing Government systems to enforce the uniqueness of ID for specific usage, where it is appropriate and necessary.

NDEAR and Identities

Under the NDEAR federated architecture, ID should be kept as local to the context of the ID owner instead of all being held centrally. Each ID record should be owned and controlled by the owner of the ID record. All these IDs are just locally unique within the ID registry and not nationally unique unless explicitly needed (e.g., school ID). Since these will be within the registry, ID context will be of that registry and reference will be made to the ID using the registry URL. Depending on the sensitivity of the data, access to the ID and profile registry may be of 3 types:

1. Fully protected: all records and attributes of the records accessible only via consent (e.g., student/ teacher records).

2. Partially public: some attributes are public while others are protected via consent (e.g., school registry where several attributes of schools such as name, location, etc. are public while contact details of the person in charge may only be available with consent).
3. Fully public: all attributes and records of the registry with IDs are available as public data (e.g., geographic data records with IDs).

NDEAR ID architecture shall be federated, privacy protected, and designed to work seamlessly with consent manager and virtual IDs as per the upcoming Personal Data Protection Bill in India. The recently released discussion paper on DEPA (Data Empowerment and Protection Architecture (DEPA) by NITI Aayog spells out consent manager and federated virtual ID architecture where the user is in control of ID, consents, and their data. NDEAR ID and data architecture shall be in alignment with this architecture. Operationalization of IDs needs to be planned through a set of guidelines, especially those relating to the minimal data elements, the format of the ID, if any, the process to make it portable, obligations of the institution/ ID Provider, etc. This is beyond the scope of this document.

A3. REGISTRIES AND REFERENCE DATA

a. Master Data/Codes

Master codes are pre-assigned codes to data elements, so that the data entered a system can be reliably read, sorted, indexed, retrieved, communicated, and shared

between systems. Indicative list of data elements for which master codes shall be required are as follows:

Marksheet, Award types
• School Category
• Stream
• Managing Body type
• Subjects
• Social Categories
• Benefit types/categories
• Languages
• Location (Local Government Directory or LGD)
• Other Category codes

These master codes must be maintained in a single source at an appropriate level (national or State) in digital form (machine-readable) and made available via APIs for other blocks and applications to use.

b. Directories

Directories are a public listing of various master data and codes in machine representable and API accessible way. These are simpler versions of electronic registries and only list fully public data. Since data listed in directories have no link to any person, entity, or things (controlled in person/entity), directories are considered part of open data (master data) and do not require any consent mechanisms and access restrictions.

c. Electronic Registries

In the education domain, it is essential that data about schools, teachers, students, administrative officials, subjects, textbooks, etc. are maintained through a set of federated 4th generation registries (not kept central but kept within various State/ Centre/ department systems which are the primary keeper of that data). These registries must be designed to be easily accessible by other building blocks and usable through “registry-as-a-service with open APIs” beyond the traditional portals for end users to view and access. School, teacher, and student are core registries envisaged in NDEAR (across federated levels and not as a central database), not to mention other registries such as asset registries, device registries, etc. While all State and Central governments have the need to maintain master data within the education domain, few have managed to successfully collect and keep it up to date. Almost no system today has exposed reusable registries for others to build on. Many States

today have such master data scattered across paper lists, databases, and spreadsheets. Below are a few key registries that are enabled within NDEAR.

School Registry

Currently, each school is uniquely identified by a Unified District Information on School Education (UDISE) code. In addition to these, there are multiple schools / institutions which are not onboarded on UDISE+ or may be using their own codes for institutes. There is a need for a master registry to facilitate institution-controlled CRUD (Create, Read, Update, Delete) operations while keeping attestations/approvals to appropriate authorities and act as a single source of truth for all other building blocks and systems. Similarly, it is proposed to have a unique identifier for institutes who don't have a unique identifier for unifying various registries/databases maintained by different stakeholders. UDISE code has been recognized for the purpose of uniquely identifying schools, pre-schools, vocational training institutes and other institutions pertaining to school education. UDISE+ shall be augmented with the features required to perform School Registry with open APIs.

Teacher Registry

Similarly, teachers have multiple entry and exit points in the education system and shall require the teacher registry to be maintained at the Central level or at the State level with national access (with necessary access control and consent flows). Student and Teacher Directory may leverage Aadhaar, PAN or other existing identifiers for unique identification as necessary. As mentioned in InDEA 2.0 report published by MeitY, GoI, in every registry it is necessary that the subjects in that registry are "identified" in a unique and trusted fashion. These identifiers may be purely numeric (e.g., Aadhaar number, mobile number, health ID within ABDM, etc.) or alpha-numeric (e.g., PAN number, Vehicle number, email address, UPI Address, etc.) with or without any logic attached in generating the identifier itself (random vs logic-based identifier).

Depending on the policy, uniqueness can be either "user controlled" (user may have more than one ID within the same registry, say, using two different mobile numbers) or "state controlled" (by linking the ID to a globally unique ID like Aadhaar, and hence making sure a user has one and only one entry within the registry).

Custodians of such registries should ensure appropriate policy is applied to either allow user-controlled uniqueness or state-controlled uniqueness. In addition, the fields in the record of that subject are to be verified/attested or marked as self-

declared. When registering, people must be given an option to use their existing digital IDs such as Aadhaar, mobile, etc as appropriately to fit the purpose of that registry and also allow people to control, update, manage their record using the common IDs such as Aadhaar, mobile, etc.

Student Registry

It is important to standardize how students are identified at any point. For the entire lifecycle, a student has multiple entry and exit points into and from the education system. Different IDs are allotted which are only relevant within the scope of a limited digital environment and thus calls for a unified, but decentralized registry for students. It will be used to help students, parents, and teachers map and facilitate the entire journey of a student spanning across different stages of scholarly life including childhood care, school education, distance learning, up-skilling, and vocational training. This ensures that the education records created for a student can be issued to the correct individual, in the control of the student/ parent, and can be shared/ used using consented access. By providing control of the record back to the student/ parent, the record and contact information can be kept updated by the student/ parent.

Other Registries

Apart from student and teacher registries, other key directories in an educational ecosystem are mentioned below:

- Education Boards
- Examination Boards
- Education Research & Training Institution
- Management Bodies
- Philanthropy /NGOs
- Counsellors etc.

A4. INFRASTRUCTURE

a. Education Network & Cloud Services

Privacy by design being a key principle of the NDEAR, an infrastructure layer needs to be established for the management of the key data services in a compliant manner. The objective of this building block is to ensure that education data and its transfer/ movement is always secure and adheres to all privacy requirements.

Secure Education Networks

Entities running NDEAR compliant services should be built to work on public networks by default with open security standards. Wherever access to sensitive or aggregated data is involved, additional layers of security such as VPN or MPLS etc. may be explored.

Education Cloud

Entities running NDEAR compliant services should look to build or leverage cloud infrastructure built on the MeitY initiative of Government Community Cloud (GCC) with stronger security and privacy policies.

Security and Network Operation Centre

To ensure 24x7 availability and security, entities running NDEAR compliant services should build Security Operations Centre (SoC) and Network Operations Center (NoC) as necessary or leverage existing operations infrastructure. Given the federated nature of NDEAR, these centres may be at National or State or department/school levels, as appropriate.

b. Messaging Services

SMS/Email/IVR/IM

These services provide generic APIs for integrating messaging platforms like email, SMS, Instant Messaging and IVRs etc. along with bridges to popular commercial chat and messaging platforms. This allows other blocks of NDEAR, or solutions built on top of NDEAR to leverage these APIs.

Video/Audio Conferencing

Various interactions within the education domain, across both learning and administration blocks, require a mechanism for users to conduct “synchronous” sessions using video/ audio conferencing technologies.
NDEAR technology block could provide a default video/audio conferencing capability as a set of APIs that can be embedded within application services in other building blocks. While NDEAR may provide a reference solution for video/audio, NDEAR applications should be designed to provide a “choice” to users by offering standard pluggable integrations with other video/audio solutions as well.

c. Education Data Exchange

A common data exchange platform may be made available for various NDEAR building blocks and systems to interchange their data in a secure and, if the data involves sensitive personal data, in a privacy protecting manner. Such an exchange platform does not store the data, rather, allows end-to-end secure exchange of data in an interoperable manner. It is not necessary that a central exchange be used for exchanging data among systems, rather, this is an optional service that can be leveraged by entities building NDEAR building blocks and solutions.

d. Open School Hardware

To ensure access to digital education across the country, it is essential that a set of open hardware components are encouraged by the ecosystem to be plugged into NDEAR to consume content and enable learning interactions within a school, labs,

and classrooms. Hardware components could include, but not limited to, smart boards, local Content Delivery Network servers (CDN servers), open Wi-Fi hubs compliant to PM WANI, etc. Building hardware that can be used seamlessly with NDEAR services requires standards,

A5. TECHNOLOGY

This block provides various shared technology services that can be used across all other blocks to enable reuse, scale, security, and avoidance of duplicated efforts. In addition to the core architecture principles of all services, characteristics of services in this block are:

i. Generalized: Services in this block are atomic, minimal, and most importantly generic in nature. This generalization is very critical to ensure all services from this block can be used by services from other blocks in a wide array of contexts to meet diverse use cases.

ii. Non-functional: Services within this block are necessarily non-functional and technological in nature. All functional services are abstracted into other blocks whether it be registry functions, learning functions, or administrative functions. Services within this block are reusable non-functional services that are generalized, abstracted, and made available as APIs.

iii. API-driven: Since services in this block are consumed by/ within services of other functional blocks, it is essential that these services are built using a set of open APIs with well-defined and documented input schema, output schema, version control, and a set of automated test cases that act as the “promise of the interface contract” along with backward compatibility policy.

iv. Accessible: Services within this block shall provide technology support for designing the user experience for atypical/ differently abled persons and those with special needs. With the predicted growth of digital presence in the education sector, this is essential for ensuring universal inclusion.

The following sections describe many of these Technology services in brief. Note that this list of services is evolving and not complete, by design.

a. Locker & Consent Management Education Locker / Depository

The Education Locker is a standards-based interoperability specification that can be implemented by multiple players to enable the creation of an Education Record ecosystem. Locker/ Depository shall leverage the DigiLocker/ National Academic Depository. The locker/depository offered by the industry may also be leveraged if they conform to NDEAR ecosystem

Consent Manager

Education records are personal for an individual and every access to each record requires the explicit consent of the individual. The electronic consent framework specifications notified by MeitY and National. Data Sharing Policy should be used to develop the information sharing processes within the framework. The consent Manager shall take care of granular/ parental consent as per Personal Data Protection (PDP) Bill and be compliant with legal requirements and best practices in dealing in personal data.

b. Open AI Services

Leveraging AI/ML technologies is critical to empower users and provide access to knowledge and learning experiences. A set of reusable AI services, open-source libraries, open-source models, and data sets could be built for the education domain that can be leveraged and embedded within other building blocks. While AI is leveraged, it should be built to amplify human actors, eliminate biases, and should assist in effective teaching / learning and management rather than seeing it as a full replacement for humans. Content translation in regional language, speech recognition, personalisation, etc. is a critical part of this.

c. Shared UX Services

Similarly, new user experience technologies such as “conversation engines” (e.g., chatbots), “AR/ VR/ 3D/ Gamification”, maker experiences such as robotics, IoT devices, etc. should be explored as reusable core services that can be used across various functional blocks.

d. Language Assets & Services

Considering India's language diversity and richness, NDEAR should look to create common language assets e.g., wordnets and technologies to help with learning, knowledge organisation, translation, speech, and other aspects. Many Indian open-source projects already exist that can be leveraged to bring these together for comprehensive generic "bhasha" APIs. Assets built within various Government and research institutions must be leveraged by upgrading and integrating them as reusable open-source assets or services to amplify and extend the work.

A6. GOVERNANCE

a. School Affiliation Services

These services address school affiliations, approvals, audits, inspections, recognition, school score cards, monitoring, and other feedback/grievances. These services can be used by States and by School Boards to manage the affiliation of schools under them. These transaction services will fully leverage the school registry and unified profile.

b. Awards & Recognition Services

These services address the workflows, rules, and transaction capabilities for Centre, States, Boards, and ecosystem partners (an NGO could also use award services, if they wish to) and schools to issue awards, recognition etc. for teachers, students, and other users. Awards can be issued in digital format via DigiLocker and printable format. These services shall allow the creation and lifecycle management of awards and recognitions. These services shall leverage registry services and infrastructure services (such as SMS/Email, etc.). Reference applications (portal/app) would interface with these services out of the box while still exposing these services as independently usable APIs.

c. Examination, Result, Certificate Services

Formal testing/examination is an integral part of education to ensure that learners are acquiring the knowledge as per expected learning outcomes. Results / Certificates are recognition provided by the schools / institutes to the students after successful completion of undertaken learning through the assessment process. Results portal is a great example of a gateway to exam results in India. NDEAR shall support multiple types of assessments as part of learning services as per the varied needs of learners and courses offered. Federated depositories shall be created for online storage and sharing of awards details online with external parties with consent. National Academic Depository / Digi locker shall be leveraged for award depository. Other such initiatives a part of federated architecture may also be leveraged. All awards and certificates will be issued as machine-readable, verifiable documents, with a print option, as per common schema standards.

d. Schemes, Programs, Scholarships

Government, as well as non-government, bodies provide multiple welfare programmes / schemes for weaker sections of the society. These programmes / schemes are owned by Central, State or jointly by both. NDEAR shall support the implementation and monitoring of schemes by government or nongovernment bodies. Some of the schemes are Samagra Shiksha, Mid-Day Meal, Padna Likhna Abhiyan, National Means-cum-merit Scholarship Scheme, National Scheme for incentives to Girls for Secondary Education, and National Awards to teachers. Scheme management services shall address scheme planning, definition, rollout, funds disbursed, monitoring, auditing, and so on and shall be integrated with registries. Scheme management allows the Government to ensure unification across schemes, easier enrolment for beneficiaries, and efficient fund management.

Scholarship Services

Scholarship services address the workflows, rules, and transaction capabilities for Centre, States, Boards, and ecosystem partners (a company could also provide scholarship via CSR if they wish to) to provide scholarships for teachers and students. Scholarships can be given based on academic performance or other rules and can leverage the Aadhaar-enabled direct benefit transfer (DBT) model to directly deposit in a bank account. These services shall leverage registry services and infra services (such as SMS/ Email, etc.). Scholarship services are already available through a national scholarship portal (as a common application) catering to the entire nation.

A7. ADMINISTRATION

Administration services building blocks help in providing education efficiently to the child and goes beyond imparting knowledge and ensures that the daily needs of students/ teachers are fulfilled, and they can focus on learning and teaching.
When built, these services shall be made reusable with open APIs and as open-source code, so that many applications can reuse these services as-is or embed these capabilities within those applications, be at Centre or State or school levels. These can be then offered either as API services, open-source components, and via a set of reference applications for States to use.
The following list is merely indicative and many more services like Vidyanjali towards management of CSR, management of school facilities (sports, library, labs, playground, etc.), services that enable and support extra-curricular activities, etc. can all be subsequently added.

a. Personnel & Payroll

These services address various aspects of personnel management, payroll, appointment, transfers, pension, service books/records management, manage payments, etc. These services will leverage teacher and other personnel registries to use the unified personnel profile ID within the registry to attach various workflows and transactions.

b. School Management, Attendance

These services are meant to be used for building school management solutions. These include admissions, attendance, feedback, event management, community engagement, virtual PTA meetings, etc. All these services and reference UX shall be made available as open-source (so that affordable private schools can leverage as well) and also as hosted environments (for Government schools). These services will be integrated with registry services, shared infra services, and other building blocks.

Civil Works, Projects

These services allow states and schools to manage civil projects end-to-end for school facility improvement programmes. Services shall include most of the typical

project management capabilities such as budget management, personnel assignment, task management, calendaring, tracking, auditing, and so on. Reference application block shall also have out of the box reference app/portal for using these capabilities.

Finance & Accounts

Finance and account management are key services to manage budgets, allocation, accounting, and related aspects for both at State and school levels. Administration building block shall contain these services provided for the Governments. As per NDEAR principles, open sourcing these modules allow even
affordable private schools and communities to leverage these, enabling faster digitisation of accounts and financial aspects of the entire ecosystem.

c. Mentoring, Counselling

One of the core services children need is access to various counselling services in various matters such as study, career, physical & emotional, exams, admissions, etc. While high end schools and children coming from privileged backgrounds do have access to these, a large population of students do not have access to any form of formal counselling. It is important that these services are made available across the country in various languages. These digital services shall use open protocols to bring the entire ecosystem of counsellors onto a common infrastructure through registries, attestations, feedback, etc. so that students
get access to virtual counselling services (both anonymous and identified). These services should be embeddable into school management systems and also available as standalone for consumption in various contexts.

A8. CONTENT

Content services are at the heart of this building block. An entire set of content services shall provide a mechanism for all key personas to engage in learning and teaching interactions through a series of coherent, integrated, guided journeys. These services shall be enabled to ensure that core NDEAR principles such as “enabling diversity”, “enabling access”, “enabling ecosystem”, etc. are fully adhered
to. Digital infrastructure shall provide agency to institutions and users in terms of building appropriate content, supporting different taxonomies, and creating contextual

solutions and fully support seamless interplay between physical-digital mediums, synchronous-asynchronous modes, diverse device types, and self-assisted interactions. DIKSHA content services are currently the best example of this and are used by millions of users daily across the nation.

a. Contribution & Curation

These services allow curriculum-linked content sourcing and curation, be it for linking to energised textbooks, online courses, quizzes, or any content for that matter. Contribution service supports multiple models for content sourcing - sourcing from a pre-selected set of individuals or organisations, crowdsourcing contributions from masses - both organisations and individuals, and re-using digital content already published. The Centre, States and education Boards can leverage content sourcing tools to engage the ecosystem of their teachers, different government institutes, community of organisations and individuals at large. When seeking contributions, additional capabilities to go through a nomination process can also be enabled.

Apart from content sourcing tools, content authoring tools shall also be available allowing teachers or users, designated by centre or state departments, to create interactive digital content. For example, NROER (*It is a digital repository for Open Educational Resources. The Repository houses a wide range of educational content and resources covering all subjects and all grades for school students, teachers, and other stakeholders. In addition to the educational resources which are available in a wide variety of forms, the NROER also provides opportunities to users to enroll in various online courses and participate in online contests.)*
Content curation services can be used by sourcing organisations to ensure that only good quality content is eventually published to users. Once the sourced or created content is ready, it needs to be checked for content guidelines of the sourcing organisation (note that while common guidelines may exist, the federated nature of the architecture allows various administrative organisations at various levels to have their own rules to meet their context). Once the quality check is done, it needs to be tagged, organised by attaching to one or more categories, pedagogic correctness verified, and eventually published. Curation services shall provide a wide variety of tools (both automated as well as manual) and workflows to content sourcing organisations to manage this process.

b. Taxonomy & Tagging

Framework service (for mapping various taxonomies and curriculum frameworks) allows various boards to create one or more of their own curriculum frameworks

linked to classroom learning or teacher professional development. Taxonomies may include grades K-12 school education, early learning, foundational learning, inclusive education, teacher training and several others. Defining various taxonomies as machine
represented semantic structure helps with organisation and categorisation of content and serves for easy discovery of content by users. This also allows efficient tagging of each content on the platform to relevant grade, medium, topic, learning outcomes or learning objectives. Frameworks are crucial, for e.g., for content to be tagged to energised textbooks, during course creation, among other uses. Efficient framework infrastructure enables personalised learning by leveraging artificial intelligence and machine learning algorithms. Learning analytics of achievement (by learning outcome or learning objectives) is
enabled through framework service of the learning building block. An open taxonomy infrastructure for organising knowledge across multiple learning frameworks is extensively implemented within DIKSHA.

c. Language & Translation

Education infrastructure will not be complete if the core building blocks, and services do not address the language diversity of India. NDEAR shall give special focus to address these through technologies to enable dictionary/wordnet services, input capture services, speech detection and analysis services for children learning language, translation services specialised for learning content, text digitisation services (such as optical character recognition or OCR) for capturing assessment data, etc. With the advancement in AI/ML and wide access to mobile devices (with camera and microphone), time is ripe to ensure these technologies are leveraged to enable millions of users to interact, discover, learn, and collaborate in Indian languages.

d. Discovery & Personalization

For large scale adoption and usage, it is critical to ensure users across all personas can efficiently discover, share, and consume content that is most relevant to them when needed in their learning context. While “search paradigm” is popular, at scale, most users find it hard to discover relevant content for them. This is due to various factors such as complexity of search semantics, language and vocabulary differences, lack of context when doing general searches, lack of capable adults supporting discovery, and so on.

Hence discovery services shall provide multitude of unbundled capabilities such as using QR codes, chatbots using conversational techniques, metadata-based advanced searches, easy sharing of content and collections by users, multi-lingual mappings, advanced tagging to do push targeting, etc. Discovery services shall offer advanced search and discovery capabilities using the terms in the taxonomy, their equivalent terms, or adjacent/related terms. For example, a teacher searching for “Single Digit Addition” may also discover content related to “Double Digit Addition” and “Carry Over” because these are related terms.

Personalization is an advanced gradient of discovery where the system automatically learns user behaviour, tries to get the right context, and then creates recommendations and “directed journeys” for the user by leveraging content and taxonomy services. It is pertinent to remember that NDEAR needs to address all key personas and hence these services should not only focus on students; it should also be built as generalised services for personalisation for teachers, parents, administrators across consumption, creation, and management interactions. Personalisation also should not be misconstrued as a mechanism for replacing teachers and mentors; it is merely an aid in easing discovery and navigation. Personalisation can be done at a cohort level allowing the system to gradually move from most generic to cohort based to most individualised in an evolving manner.

To implement the above capabilities, it is critical that content repository and searches are seen not as simple database and text indexing issues, rather as a careful architecting of “semantic knowledge structure” mapping, layered with multi-dimensional discovery services and then building advanced telemetry-based cohort or individual personalisation capabilities, all as unbundled and reusable services within NDEAR.

A9. LEARNING

Learning services building block shall provide unlimited access to robust and comprehensive learning experiences and associated services to all the actors. The DIKSHA platform, with microservices, is a great example of this block. As part of the harmonisation of various learning platforms, they can be upgraded or consolidated by MoE to leverage and unify.

This building block is one of the most critical blocks to enable a wide variety of services spanning from learning, assessments, tracking learning outcomes to interactions and credentialing. In addition to these services already available on

DIKSHA, reference applications such as the DIKSHA portal/mobile app and SWAYAM are offered to make the learning experience easily accessible to the entire nation. These learning experiences are not limited to students, rather, these services shall be used for learning of students, teachers, administrators, and anyone who wants to learn (including children who have dropped out, not in school, learners with special needs, etc.).

a. Learn, Do and Practice, Sense and Assess

Assessment has always played an important role in education. Most, if not all, types of formal education use some sort of assessment, typically including a final exam to earn a grade, a degree, a license, or some other form of qualification. Today, assessment is no longer restricted to grading at the end of an instruction (summative assessment). Its value for continuous monitoring & feedback (formative assessment) and guiding of the learning progress (means to learn), without being necessarily used for grading purposes is recognised. Formative assessment, including self-assessment, can play a vital role in motivating learners since it provides them a way to judge their own competency level and allows them to track their progress.

Answering questions and solving problems is an effective way to learn. If the questions focus on micro- concept level assessment of student's proficiency, it is possible to identify strengths, areas that need focus and improvement, and recommend the relevant content to the student that specifically addresses the individual learning needs. Questions that are tagged with appropriate pedagogic metadata and associated with relevant concepts will enable "questioning" to be used as an effective means to encourage learning. Combining these capabilities with the "standardised learning outcome" taxonomy allows continuous sensing of learning levels across the nation.

b. Interaction & Collaboration

Active communication and collaboration between practitioners are known to lead to significant

improvement in learning outcomes. In the offline world, such shared learning requires the facilitation of meetings, workshops and conferences and necessitates physical affinity. This requirement puts a burden in terms of scheduling, logistics and cost of operations.

A digital infrastructure provides unparalleled opportunities for extensive collaboration without requiring users to be physically together, extensive scheduling, and logistics. A well-designed digital infrastructure can significantly reduce the cost of collaboration while dramatically increasing access to expertise and mentorship. In addition, collaboration on a digital platform allows for the

participation of diverse groups across geographies and enables sharing of best practices, discussion on key topics, celebration of successes through hackathons, webinars, virtual classrooms etc.. Imagine the possibility of a student in Kerala learning Hindi from a master teacher from UP or getting the best mentorship and guidance from experts sitting far away using a smartphone and Internet connection. This interaction and collaboration with teachers, mentors, experts, and peers are what these services are built to address. These generalized interactions and collaboration capabilities are unbundled and can be made available as microservices for reference applications and ecosystem applications to use. These interactions can be either synchronous (when users are virtually together at the same time, audio/video conferencing, phone call, etc. are examples of these) or asynchronous (when users can interact with each other without being virtually available at the same time, chat, discussion boards, etc. are examples of these). It is also important to ensure these services are not specifically built only for one persona, rather built in a manner which can be used across student-teacher, student-student, teacher-teacher, teacher- parent, and other interactions.

Also, it is necessary that these services are not thought of as a standalone feature (such as video conferencing portal or independent discussion boards). Instead, they should be thought of as microservices and components that can be embedded into the actual transaction context. Learning interaction and collaborations services focus primarily on bringing collaboration into the learning context.

c. Credentialing & Badging

Learning is a continuum of micro-loops of “Ask, Act, Assess” cycles. Asking to understand and learn; Acting to practice and implement; and assessing to validate if the Ask-Act steps indeed resulted in the desired outcome. Every significant action result in a “proof of that action” which can be issued to the actor as a “credential” that is verifiable and portable. This design of NDEAR allows unbundling of learning itself into micro-steps resulting in a series of micro-credentials that are attested by various systems/people allowing learners to carry those proofs (of actions and assessments) from one context to another (one school to another, one application to another, school to jobs, etc.). Badging is a simpler form of credentialing typically used to indicate higher trust levels for people/ things/ entities. For example, a content could be badged as “NCERT Approved” (an entity attesting the content and issuing a badge) or “Most Popular” (a system deriving popularity score and auto issuing a badge). Thus, it is essential to have core credentialing and badging capabilities to be built as “generalised”, “templatised”, “rule/ rubric-based”, “event-based triggerable” services that can be embedded and consumed by various application layers across the NDEAR ecosystem. NDEAR proposes to make all credentials (certificates, awards, badges, etc.) natively digital, machine readable,

verifiable, and universal across various public and private educational issuers/systems.

A “lifelong learning passbook” (electronic Personal Learning Record - ePLR) shall be created that constantly accumulates all competency proofs based on micro/ macro-assessments as well as other credentials (proof of internships, proof of projects, etc.) in machine readable formats. This is then given in the control of the learner (or parents in the case of minors) as part of data empowerment using DEPA architecture.

d. Learning Infra, Telemetry & Data Analytics

Learning infra services provide shared services within this building block that are leveraged across all learning services. These include data pipelines, graph-based knowledge engines, virtual ID services, semantic indexing services, event services, versioning services, etc. These are horizontal lower-level technology services that are shared across all learner services, built using open-source, and provided as APIs within this building block.

The philosophy of micro-functional services extends to data architecture, tracking micro-level events and data products that enable micro-level computations. Just like the overall platform is a composition of several such micro-services, the data architecture allows higher order insights to be built by composing and combining the micro-level telemetry and data products. Telemetry is generated during system usage based on interactions between the users and the system, or between subsystems. Telemetry represents a fact emitted via an event stream and is immutable. Any additional derivations from the raw fact generate new events. All learning services shall emit telemetry (telemetry can be implemented across all building blocks for understanding interaction behaviour in an anonymized fashion).

Open telemetry specification implemented in DIKSHA provides the fundamental definition of what the event represents, what attributes it must have and a guideline on when to generate it. The telemetry specification is a formal contract. It allows the apps that generate events to be decoupled from the data products that process them by standardizing the structure and semantics of the events.

Based on the raw telemetry data, data products are developed as services. Data products read the data from the telemetry datastore, run the aggregate computations, and generate output that is stored as derived metrics or published for downstream processing. Derived metrics are available via on-demand APIs or as exhaust. In-line with the microservice architecture, data products can also be seen as micro- computations that can be assembled to achieve a deeper insight from the data. All derived metrics and data sets shall be available via APIs for building visualizations, running advanced algorithms, and use for policy and research purposes.

A10. REFERENCE APPLICATIONS/SOLUTIONS

For enabling core learning- and administration- related interactions in a unified manner to all primary stakeholders, it is important to provide a set of reference solutions as a choice for friction-free access. The term “reference solution” is used clearly to indicate that these solutions/apps offered as part of NDEAR are just “one of the choices” for the end users. Given the fact that underlying building blocks (learning, administration, registry, etc. described earlier in this document) are API based and NDEAR being an ecosystem-driven architecture, many of the ecosystem partners across Governments, society, market players, and others, will be actively encouraged to build solutions beyond these reference solutions to cater to the diversity of India. This ecosystem-driven solutioning approach is truly the essence of “digital education infrastructure as public good” where many contextual solutions are available to users freely or commercially ensuring choice, contextualization, and continuous innovation. UX built as part of reference solutions should try to achieve the above by providing multi-channel, coherent experiences (not siloed and broken), across mobile, web, radio, TV as appropriate, in an accessible (supporting accessibility best principles to cater to users with special needs) and inclusive way (taking first time users, language barriers, and digital divide aspects into account). NDEAR identifies the key access and service delivery points that would be required by the actors of the educational ecosystem. These are mentioned below:

Mobile/Web Applications

A wide range of mobile apps can be built on top of government reference applications by the NDEAR solution ecosystem, including start-ups and existing Education Tech companies. The end user thus has the choice of selecting the app that suits their needs best. DIKSHA is the default reference application for learning interaction within NDEAR. Various other reference applications shall be built as open source and made available either at the Centre or at State/school levels while stakeholders still have the ability to build their own or obtain a solution from the market.

Television (TV) & Radio

Television and radio are widely prevailing mediums for transmitting digital educational programmers / lectures to the ecosystem actors. While it is essential that these mediums are used to ensure children get access to good content, it is also essential to ensure coherence via allowing seamless interplay between various modes. For example, a program on TV about a topic could show QR code for users to scan and continue the experience on a smartphone or similarly TV and radio programmers

could be made available on web/mobile interface for asynchronous consumption for those who missed out the shows.

Voice/IVR/SMS

This includes providing voice assistance and transmitting educational programmes / lectures through voice services or VOIP services. Voice-based services shall be available in spoken Indian languages. Similarly, a missed call or an SMS could trigger the system to call back with stories, explanation content, and by sending links to subsequently navigate to alternate channels such as the web. Not only learning services, various administration services such as admissions, certificate requests, etc. can be made available via IVR, missed calls, SMS to help users take actions, get information, etc. without having to physically visit offices, fill forms, etc.

Support Centres

Communities should be encouraged to create local support groups, support centres, etc. to bridge the digital divide and help users adopt and leverage digital resources and interfaces. Considering India's vast diversity in language and contexts, central call centres do not work well and are not a viable scalable model. Instead, these support centres should be designed as federated and made as local as possible. Community members and entrepreneurs (similar to ASHA workers (Accredited Social Health Activist) in healthcare or banking correspondents in the financial domain) should be encouraged to join and provide support to users. Interactive chatbot shall be encouraged for responding to frequent queries, get access to information, and conduct transactions.

A11. OPEN DATA AND ANALYTICS

For effective and quick decision making, it is essential to have a business intelligence architecture block that will assist the governance team in making necessary changes in on-going schemes, along with introducing new initiatives across 3 administrative levels - Centre, State/board, and school.

The following services should be built to be reusable and open sourced. This will ensure that these can be used within other building blocks, and still be deployed in a federated deployment architecture, without having to take an entire analytics solution. These are not to be built as monolithic applications or portals, since data should not

be pooled centrally to be able to use the following services; rather these services should be deployed where the data is to ensure data privacy and security.

Anonymizer

The Anonymizer service implements various data anonymization techniques, including deidentification, masking, randomization, etc. so that applications wanting to “emit” open data for analytics purposes can anonymize various datasets in a standard and efficient manner. Best practices and standards shall be based on international standards such as ISO and work already available from areas like EU General Data Protection Regulation (GDPR) This service receives data from the Education Locker and/or other Education data sets, removes all personally identifiable information to protect the privacy and provides anonymized data to the seeker.

Education Analytics & Visualization

The objective of this technology component is to provide decision support to the stakeholders on a wide variety of themes i.e., Quality of Education, Quality of Data, Public Education and Policy etc. by analysing the aggregated datasets to be accessed from various systems, through reusable analytics and visualization services. These services from this building block shall be available freely to various applications to embed within them, to leverage data and analytics within the application context and provide actionable insights to users for to taking decisions.

Education GIS Services

Visualization of data in a map form, enabling location aware services (e.g., finding nearest test centre), etc. requires underlying geographic information system (GIS) capabilities. This is one of the essential reusable services/components within this building block that can enable various applications to embed map visualizations and location-aware services easily without having to build from scratch. As per MeitY National Data Sharing Policy (NDSP) and the policies regarding Open Government Data (OGD), it is important that various anonymised datasets (non-sensitive and non-personal data) are made available publicly in an easily consumable form. NDEAR architecture embraces full adoption and implementation of NDSP in the education domain. Various applications in the education domain shall emit all such open data as part of their applications in machine-readable form (CSV, JSON, XML, etc.) and ensure these are available to all other applications and ecosystems in general, with no restrictions.

A12. ECOSYSTEM SANDBOX

IndEA 2.0 thinking is all about building a strong ecosystem around digital infrastructure to drive innovation, contextualisation, and solutioning to cater to the evolving and diverse needs of India. NDEAR fully embraces IndEA and its ecosystem architecture across the 3 ecosystems - programme, asset, and solution ecosystems - around NDEAR federated architecture. To ensure easy participation, rapid solutioning, and wide adoption of NDEAR based education infrastructure, an ecosystem sandbox has been identified as a key building block within NDEAR. Ecosystem Sandbox is defined as a unified environment for all ecosystem actors to discover, understand, engage, experiment, innovate, and build on the NDEAR infrastructure.

SECTION B: RECOMMENDED STANDARDS & SPECIFICATIONS

NDEAR envisages the evolution of an entire ecosystem in the education sector to provide a wide range of services to the stakeholders in a digitally enabled manner. Such seamless and boundary-less interoperability is possible only if all the building blocks and the digital systems are built using the defined standards which are openly licensed, accessible, and usable by the whole ecosystem. The objective of this section is to identify the standards required for ensuring interoperability and portability within the National Digital Education Ecosystem. It is proposed to recommend a set of minimum viable standards in the initial stages. The scope of the standards is defined keeping the foregoing in view. The table below depicts the areas chosen to define the standards for NDEAR.

#	Category	Purpose
1	Learning Environment	Standards related to schools and other learning environments and its evaluation
2	Consent	Consent from students/ parents need to be covered from two perspectives — consent for data collection and for data use
3	Content	Standards related to educational content creation
4	Interoperability	Standards related to exchange of education data
5	Assessments & Results	Standards related to assessments and harmonization of marks
6	Privacy & Security	Standards related to data privacy (through access control) and security of data at-rest and at-motion. Also, aspects such as data immutability and non-repudiation with audit trail
7	Application design & development	Standards related to design and development of applications

Table 4: Categories of NDEAR Standards

Evolution of Standards

Within the education realm, we can classify standards into 3 broad categories - Academic Standards, Data Standards and Technical Standards.

1. Academic Standards – Standards about what students should learn. Academic standards represent the criteria established by an educational institution to determine levels of student achievement.
2. Data Standards – Vocabulary and formats for sharing, exchanging, and understanding data. Data standards provide consistency in how data is viewed or stored and generally refer to elements, element definitions, and option sets.
3. Technical Standards – Technical protocols, engineering criteria for systems, methods, processes, and practices (including for the exchange of data between systems). Technical standards allow communication between software, hardware, applications, systems, etc., without having any misunderstandings of what is being communicated.

Within the NDEAR ecosystem, the education standards have been further subdivided under broader categories as follows:

Standards allow people or machines to have a common understanding about the meaning of information. To illustrate this point, consider the following classroom example. A student is required to learn how to plot an address on a map. The requirement to understand how to plot an address represents an academic standard. The data the student provides to the system such as Street Address, City, State, and Zip Code represent a data standard. The student may use a Global Positioning System (GPS) tool to find the location. The ability for the GPS to provide this information represents a technical standard.

The Common Education Data Standards

CEDS is recognized as the primary education data standard with a breadth of elements that span from Early Childhood through Workforce. The purpose of CEDS is to provide common element names and definitions for the data Local Education Agencies (LEAs) and State Education Agencies (SEAs) typically handle student demographic, achievement, staff information, and school program information. The goal of this work is to increase the accuracy of data exchanged between systems, increase data quality by removing ambiguities in definitions, and provide a common vocabulary for educators, researchers, and other decision makers to understand what

the data mean, so they can work together to improve programs and outcomes for students. CEDS is developed in conjunction with a variety of nationally recognized education stakeholders and uses existing definitions whenever possible. The CEDS data standard encompasses all of the various aspects of the P-20W (early learning through postsecondary and workforce) system that LEAs and SEAs use.

B1. Standards for Learning Environment

Currently, education is not limited to schools. Students have multiple choices with regard to modes for education, each requiring their own learning environment. It is important to understand various learning environments and set up standards that will help in imparting effective education across these learning environments. Standards shall also help to evaluate the learning environment, including formal and non-formal education systems. Given below are the phase 1 standards that have been benchmarked against some of the prominent frameworks.

#	Purpose	Applicable Standards
1	School Standards and Evaluation Standards	• National Programme on School Standards and Evaluation(NPSSE) - Shaala Siddhi • Performance Grading Index PGI/State/District https://pgi.udiseplus.gov.in/#/home
2	School Quality Assessment and Accreditation Framework (SQAAF)	As per NEP 2020 (Draft stage)

#	Purpose	Applicable Standards
3	Teacher Education	Governance of National Professional Standards of Teachers (NPST) as per NEP 2020 (standards will be developed by 2022, by the National Council for Teacher Education in its restructured new form as a Professional Standard Setting Body (PSSB) under the General Education Council (GEC), in consultation with NCERT, SCERTs, teachers from across levels and regions, expert organizations in teacher preparation and development, expert bodies in vocational education, and higher education institutions)
4	Early Childhood Education	National Curriculum framework as per NEP 2020 (The formulation of a new and comprehensive National Curricular Framework for School Education, NCFSE 2020-21, will be undertaken by the NCERT. By 2022, a new and comprehensive National Curriculum Framework for Teacher Education, NCFTE 2021, will be formulated by the National Council for Teacher Education, NCTE in consultation with NCERT). National Initiative for Proficiency in Reading with Understanding and Numeracy (NIPUN) has qualified the standards. The NIPUN BHARAT portal may be viewed here https://nipunbharat.education.gov.in/Login.aspx

#	Purpose	Applicable Standards
5	Skills & Education	DSEP (Decentralized Skills and Education Networks) https://dev.DIKSHA.gov.in/#/document/open-standard-specification
6	Learning Object Model	https://dev.DIKSHA.gov.in/#/document/open-standard-specification
7	Integration with external apps	SOFIE (Specification for Open Feature Integration and Extensions) https://dev.DIKSHA.gov.in/#/document/open-standard-specification

Table 5: Standards for Learning Environment

B1.1.1 School Standards and Evaluation Standards:

The need for effective schools and improving school performance is increasingly felt in the Indian education system to provide quality education for all children. The quality initiatives in the school education sector, thus, necessitate focusing on school, its performance and improvement. In a major step towards comprehensive school evaluation as central to improving quality of school education in India, National Programme on School Standards and Evaluation was initiated by **National Institute of Educational Planning and Administration (NIEPA),** under the aegis of Union Ministry of Human Resource Development in 2015.

NPSSE visualizes ‘School Evaluation’ as the means and ‘School Improvement’ as the goal. It refers to evaluating the individual school and its performance in a holistic and continuous manner leading to school improvement in an incremental manner. The major objectives of NPSSE are to develop a technically sound conceptual framework,

methodology, instrument, and process of school evaluation to suit the diversity of Indian schools; to develop a critical mass of human resource for adaptation and contextualization of the school evaluation framework and practices across states.

The programme envisions reaching 1.5 million schools in the country through a comprehensive system of school evaluation. As part of this endeavour, the School Standards and Evaluation Framework (SSEF) has been developed as an instrument for evaluating school performance. This has enabled the schools to evaluate its performance against the well-defined criteria in a focused and strategic manner. The SSEF comprises seven ‘Key Domains’ as the significant criteria for evaluating performance of schools. The ‘Framework’ has been developed through a participatory and mutual consensus approach on 'How to evaluate diversified Indian schools for Incremental Improvement’. The SSEF has the flexibility that makes it eminently suitable for adaptation, contextualization, and translation in state-specific languages. It has been designed as a strategic instrument for both self and external evaluation. Both the evaluation processes are complementary to each other and ensure that the two approaches work in synergy for the improvement of the school as a whole.

Salient Features of SSEF:

- Identifies Key Domains as critical performance areas and a set of Core Standards under each Key Domain as reference points for evaluation and improvement
- A comprehensive instrument for both self-evaluation and external evaluation
- Flexible and adaptable for contextualization by the states, addressing the needs of diverse schools
- Clear, logical, and easy-to-use by the school and external evaluators
- Makes the evaluation process consistent and transparent
- Enables schools to evaluate their current level of performance and provide concrete directions towards the next level of improvement

As part of the SSEF, a ‘School Evaluation Dashboard e-Samiksha’ has been developed to facilitate each school to provide a consolidated evaluation report, including areas prioritized for improvement. The School Evaluation Dashboard is developed both in print and digitized format.

The SSEF comprises seven ‘Key Domains’ as the significant criteria for evaluating performance of schools. Each ‘Key Domain’ has a set of ‘Core Standards’ that addresses the most significant elements of the respective Key Domain. The evaluation of each ‘Key Domain’ entails sequential steps. These steps are ‘Reflective Prompts’, ‘Factual Information’, ‘Core Standards’ (with descriptive content), ‘Supportive Evidence’s, which together facilitate schools in making professional

judgment of their level of performance. Each school is expected to prepare a consolidated evaluation report in the' School Evaluation Dashboard'.

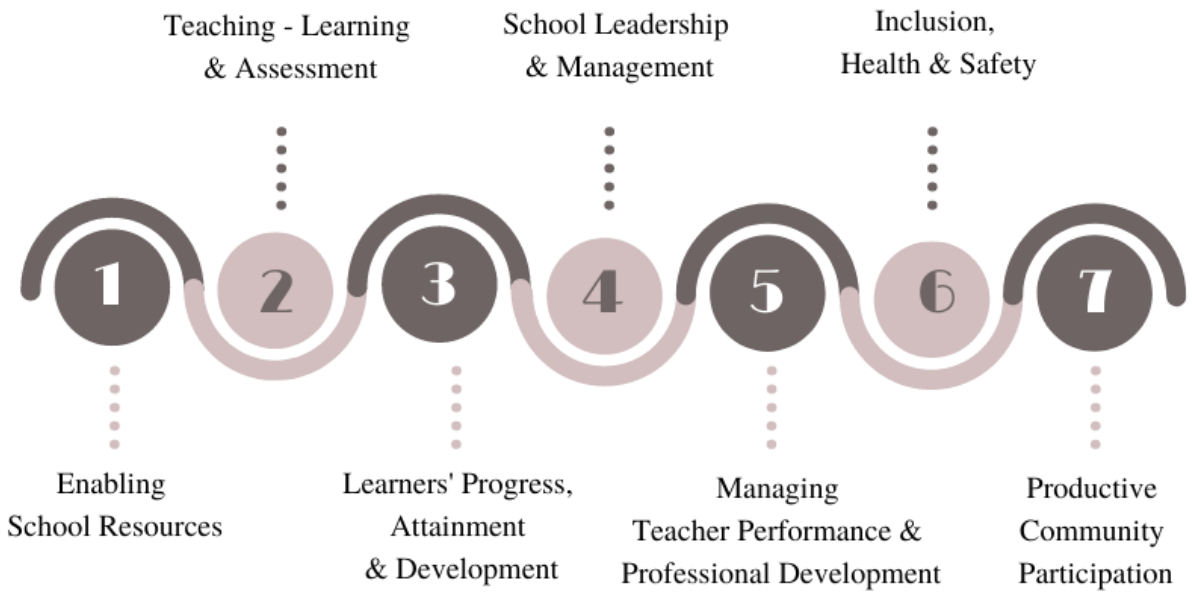


Figure 4: School Standards and Evaluation Standards

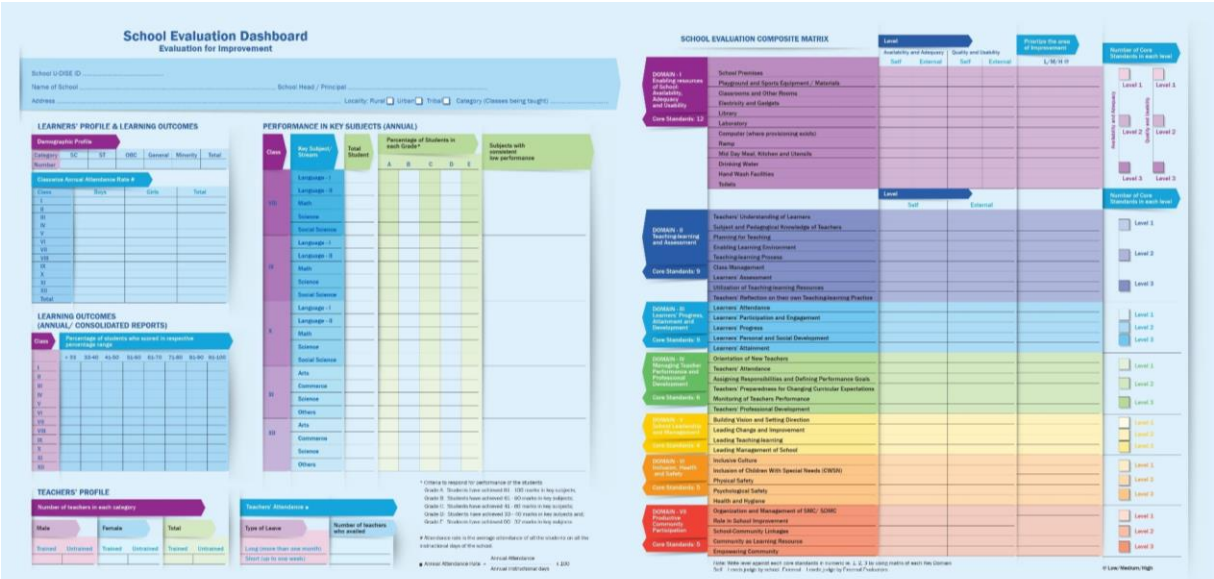


Figure 5: School Evaluation Dashboard

The School Evaluation Dashboard, obtained from each school, gets consolidated at cluster, block, district, state, and national level for identifying school-specific needs and common areas of intervention to improve school performance.

For more details - http://www.niepa.ac.in/School_Standards_Evaluation.aspx

B1.1.2 School Education Quality Index (SEQI)

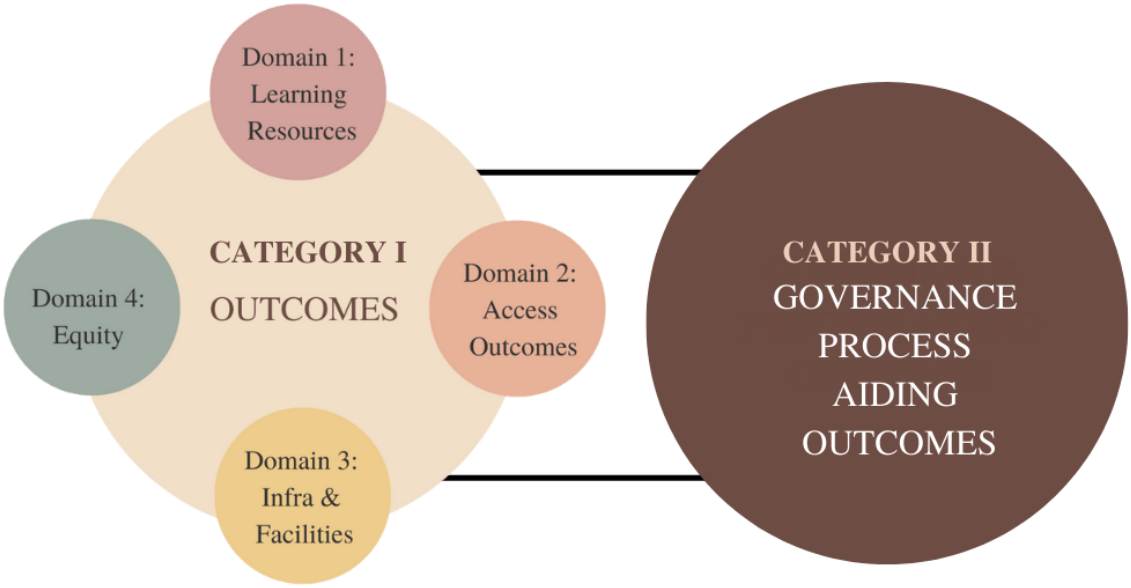


Figure 6: Categories of SEQI

The School Education Quality Index (SEQI) has been developed to provide a tool for evaluation of performance of States and Union Territories (UTs) in the school education sector. The index aims to bring outcomes focus to education policy by providing States and UTs with a platform to identify their strengths and weaknesses and undertake requisite course corrections or policy interventions.

SEQI is based on a set of indicators that measure the overall effectiveness, quality, and efficiency of the Indian school education system. The index encourages States/UTs to improve their scores by showing progress across these aspects.

Category	Domain	Number of Indicators	Total weight
1. Outcomes	1.1 Learning Outcomes	3	360
	1.2 Access	3	100

Category	Domain	Number of Indicators	Total weight
	Outcomes		
	1.3 Infrastructure & Facilities for Outcomes	3	25
	1.4 Equity Outcomes	7	200
2. Governance Processes Aiding Outcomes	Covering student and teacher attendance, teacher availability, administrative adequacy, training, accountability, and transparency	14	280
TOTAL		30	965

Table 6: Evaluation Matrix

For more Information - https://www.niti.gov.in/content/school-education-quality-index

B1.1.3 School Quality Assessment and Accreditation Framework

SQAA is an exhaustive, objective, transparent and implementable self-assessment tool benchmarked by best global standards and also rich in its local requirements for educationists, leaders, management, and all those involved in making a difference in the lives of children. It is an affirmation of 'Quality'. It highlights the fact that Self- Assessment as an internal

accountability is intrinsically important in building a sense of responsibility and ownership.

SQAA is different from Outcome Based Inspection for Affiliation. Although both of them focus on Qualitative Enhancement in School Processes, SQAA is process driven and Outcome Based Inspection for Affiliation is outcome driven.

SQAAF empowers and enables schools to self-assess their performance in different domains by providing them guidelines, tools, and instruments to achieve a self- set target and goal thus helping to move further on the developmental continuum. It would reassure stakeholders such as employees, professional bodies, and the general public that the school aspires for continual improvement and thus will benefit the student learning outcomes. SQAA will help a school to:

- Assess how well it is doing in different areas of school functioning
- Review its ongoing process of improvement of the institution
- Use the feedback to plan for the future.

Each school affiliated to the Board must undergo the process of SQAA and update its information online on the 8 domains (given below) of school functioning once every three years, starting from the year 2020.

Figure 7: SQAA domains

For more information- http://cbseacademic.nic.in/sqaa/handbook.pdf#:~:text=School%20Quality%20Assessment%20and%20Assurance%20%28SQAA%29%20Framework%20is,making%20a%20difference%20in%20the%20lives%20of%20children.

B1.1.4 Teacher Education

Teaching is considered one of the most noble professions globally and is associated with social progress. In earlier times, a teacher was the most respected member of society, and only the very best and most learned of all became teachers. Teachers were the centre of the education system and were needed to pass on their knowledge, skills, and ethics optimally to students. With the evolution in the education system and changing role of teachers, enhancing teacher quality becomes of utmost importance for long-term and sustainable nation-building. The professional teaching standards highlight the improvements to be made in the profession of teaching to contribute to the country's progress.

Teaching, one of the largest of all professions, employs nearly 9.7 million teachers in India (UDISE+) and still, there is a deficit of 1 million teachers. The demand for high-quality teachers is ever increasing. To ensure the teaching profession can attract and

retain high-quality individuals, broad changes are needed in the way that the profession is professed.

In the 20th century, more emphasis was made on standardizing curricula and standards, and this led to the development of scripted lesson plans and instructional content. As a result, a downward trend started in the level of autonomy of teachers. At the turn of the 21st century, teacher professionalism came into renewed focus for reforming the state of education. Improving teacher quality was identified as a critical factor in enhancing student learning and achievement.

Historically, the concept of professionalism was associated with the quality of practice and the public status of the job. It referred to the level of autonomy and regulations within the occupation to provide services to society. It requires specialized training, knowledge, qualification, and skills. However, teaching as a profession goes beyond meeting these formal characteristics/criteria. It also includes emotions that are at the heart of teaching. The combination of the formal criteria & informal requirements, along with changing student learning needs, has led to the evolution of the teaching profession and the role of a teacher.

Standards, in general, are considered to define and measure the quality of teaching in a valid way. They represent "good teaching", as well as identify what "meeting the standards" means. Professionally, these standards are classified on the basis of their purpose and coverage. These standards may be generic or specific to the domains of practice. These can also be defined in a basic manner covering all teaching professionals together or progressively for teachers at different career stages, providing a roadmap from entry to advanced practice level.

The NEP 2020 defines that the school education system will follow a 5 + 3 + 3 + 4 curricular and pedagogical structure, consisting of the Foundational Level (5 years covering age group 3-8 years), Preparatory Level (3 years covering Grades 3-5 and age group 8-11 years), Middle Level (3 years covering Grades 6-8 and age group 11-14 years, and Secondary Level (4 years covering Grade 9-12 and age group 14-18 years)

The National Professional Standards for Teachers (NPST) will inform the design of pre-service teacher education programmes and would cover expectations of the role of the teacher at different levels of expertise/rank and the competencies required for that rank.

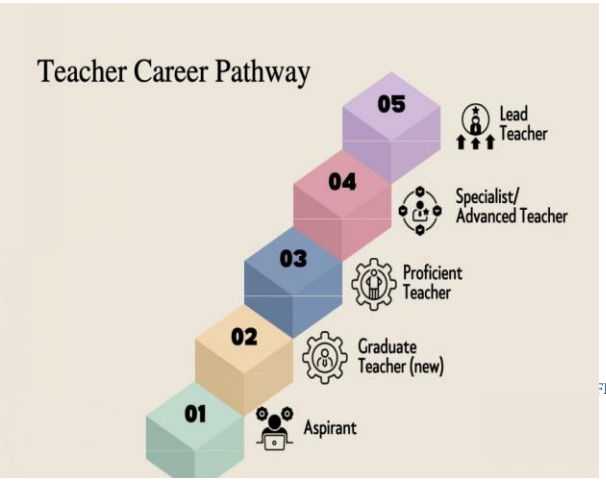


Figure 8: Teacher Career Pathway

The current NPST document proposes four career stages and professional standards for

teachers at each stage. These four stages have been defined as follows:

- ❖ Beginner Teacher (PragammiShikshak)
- ❖ Proficient Teacher (PraveenShikshak)
- ❖ Expert Teacher (KushalShikshak)
- ❖ Lead Teacher (PramukhShikshak)

Areas and Standards of NPST

The career dimensions of the National Professional Standards for Teachers framework can be described through specific aspects of teachers' work. The framework is arranged in the following four interrelated areas called 'Standards' covering multiple domains.

1. STANDARD 1: Core Values and Ethics: This standard will cover domains related to core values and ethics a teacher is expected to develop at each career stage.

Figure 9: Core Values & Ethics

2. STANDARD 2: Professional Knowledge and Understanding: This standard will cover domains related to what a teacher is expected to know and understand about their students and about teaching-learning in order to function effectively at each career stage. The standards also map how a teacher design developmentally appropriate learning experiences for children while carrying out the teaching-learning process and learning assessment.

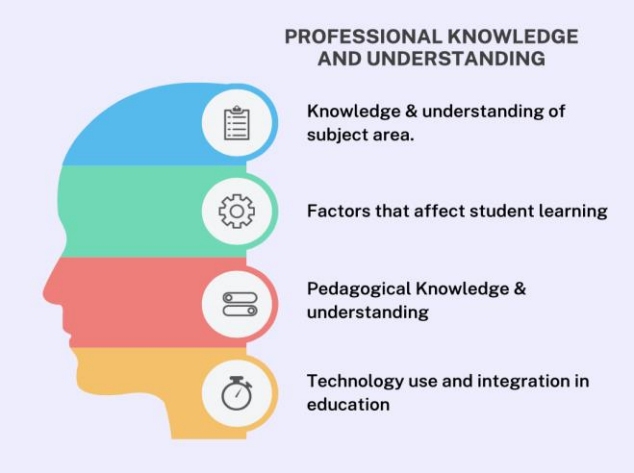


Figure 10: Professional Knowledge and Understanding

3. STANDARD 3: Professional Competence and Practice:

   This standard will cover domains related to what a teacher is expected to be able to do effectively in applying professional knowledge and skills at each career stage for carrying out

   teaching-learning-assessment practices relating to one's specialization. (i.e., stage specific, teacher- education programme.

Figure 11: Professional Competence and Practice

4. STANDARD 4: Professional Development & Growth: This standard covers domains related to what a teacher is expected to do to improve professional knowledge/competence and practice at each career stage through participation in programmes for continuous professional development of teachers.

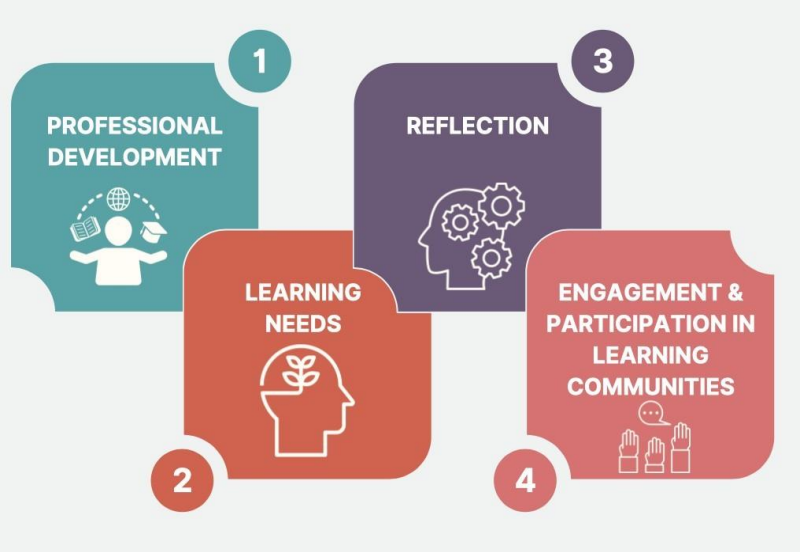


Figure 12: Professional Development and Growth

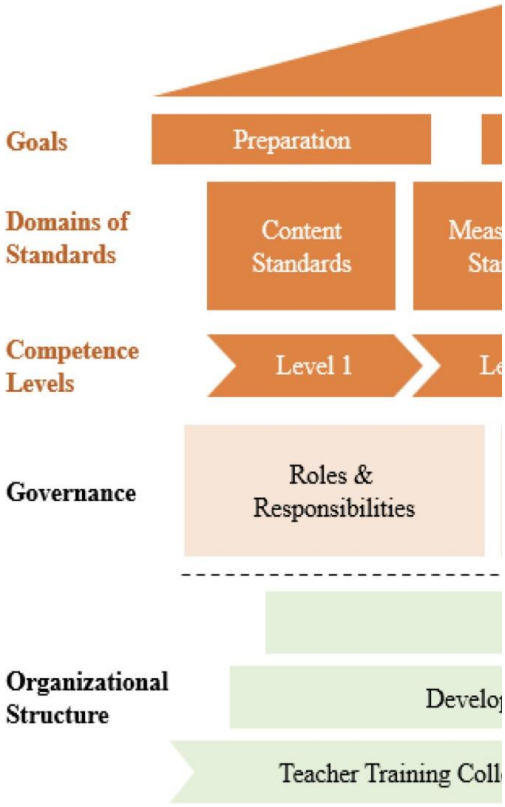


Figure 13: Suggested Teacher Professional Standards Framework as per NPST draft

For more information - https://ncte.gov.in/WebAdminFiles/PublicNotice/Hindi_0_17_11_2021_637727482281976435.pdf

B1.1.5 National Mission for Mentoring (Draft Stage)

Teachers and School Heads need new solutions to today's unprecedented demands and challenges. The community of stakeholders in itself is rich with experts, who possess the knowledge and skills to contribute towards problem-solving and capacity building of peers. Systems capable of adapting to the rapidly changing environment can empower their citizens with the right mix of skills to allow them to lead satisfying professional and personal lives. At an aggregate level, it leads to inclusive and sustainable economic growth. A structure of mentoring, therefore, offers a solution to address the existing gaps in a more decentralized manner. These are the gaps in accessing expertise, continuous professional development, connecting with peers from similar contexts and the absence of a platform to leverage cross-learning. Mentoring offers individuals to engage in the processes of learning under an experienced professional. The different ways of engaging in mentor-mentee interactions can enable skill and capacity building for teachers, school leaders and professionals. This comes with an opportunity to network with experts, engage in forums to exchange learnings, best practices, and disseminate findings across various domains such as but not limited to school leadership & management, curriculum, pedagogy, educational policies, and assessments.

The hierarchical, unidirectional top-down flow of information and learning designed as training events have been prevalent woes in our current education system. Mentoring has an opportunity to soften the boundaries of hierarchies and bring a fundamental paradigm shift. It will make learning more peer and community led. It will also make learning more personalized and continuous. The main actors at play for this mentoring mission are mentors and mentees. Mentees are individuals from a cadre of the education sector that are seeking professional development in a field. Mentors are individuals from the same cadre or above, who have been seeking professional development in the same field for a while and are adept at facilitating discussions and conversations suited to "Seeking."

While the roles of a mentor and mentee might be enough to conduct small-scale mentoring activities, the mission involves a third element to facilitate and sustain mentoring structures at a much larger scale. Administrators (individual or unit) are responsible for continuously improving the quality and frequency of all interactions taking place between mentors and mentees. In addition, they ensure the continued development of the mentoring structure and its institutionalization by the ecosystem. Since the scale of any mentoring program in the education ecosystem is likely to be vast, there is immense opportunity for other system partners to develop technology and online platforms to make mentoring a seamless experience for all actors.

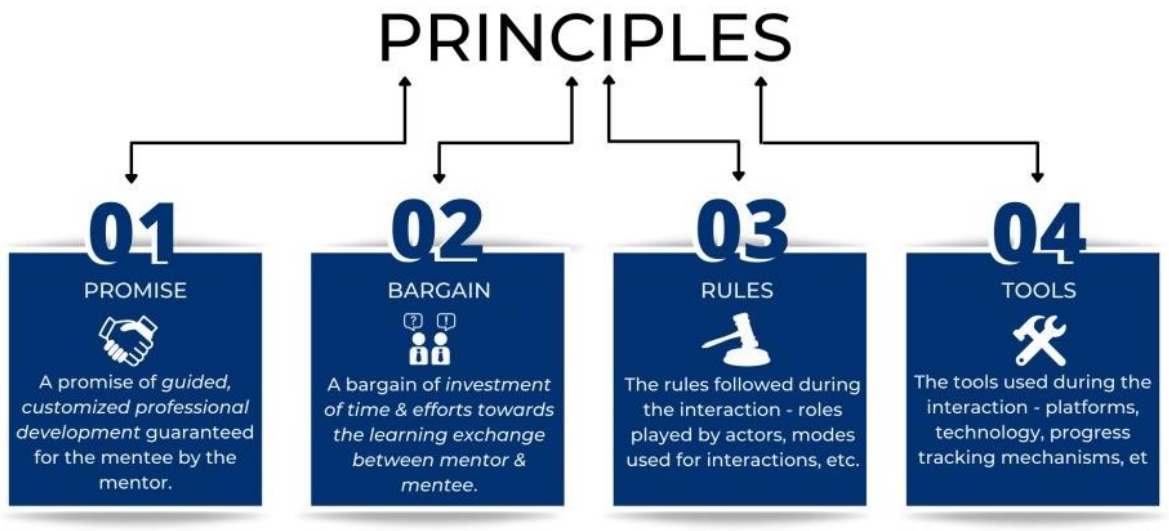


Figure 14: Principles of National Mentoring Mission

The ultimate goal is improvement in school education through enhanced, decentralized leadership in education.

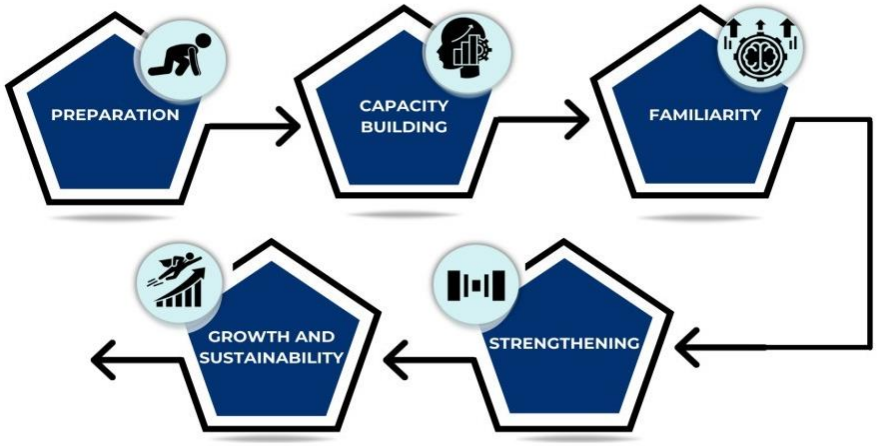


Figure 15: Phases of National Mentoring Mission

Phase 1: Preparation The stakeholders in a system may conduct a needs assessment for professional development and map the landscape for sufficient resources to implement a mentoring program to fulfil the needs. At this time, system actors may use resources, such as this book, to orient themselves towards the implementation of a large-scale mentoring system.

Phase 2: Capacity Building Once the mentors have been recruited, this stage allows for building their capacity in skills relevant to the field, along with essential mentoring skills and techniques.

Phase 3: Familiarity During this phase, mentors may practice the skills they learnt during phase 2 in a controlled environment. The familiarity phase may also be used to refine the methodology used for capacity building in phase 2 based on feedback from mentors and mentees on the quality and value offered during mentoring interactions.

Phase 4: Strengthening Once the actors are confidently implementing mentoring structures in controlled environments, mentors start gaining experience in mentoring in their fields of expertise. This phase allows for the continuous development of the mentors through ongoing capacity building sessions. At this time, tracking metrics towards an end outcome of the mentoring relationship will help understand the effectiveness of the mentoring structure and re-align it to achieve the stipulated outcomes. Outcomes should be aligned with the objectives intended for the mentoring program. For instance, in a program to enhance student learning outcomes in foundational literacy and numeracy through teachers' peer mentoring circles, an outcome to evaluate is the percent (%) increase in student performance in foundational literacy and numeracy assessments.

Phase 5: Growth and Sustainability This phase shifts attention from testing the mentoring structure to building a community of practice in mentoring. The mentoring structure can now be scaled to ensure participation by all relevant stakeholders in the system, and their continued interest in it. This can be achieved by introducing mechanisms to A) trigger the need for participation by demonstrated value offering; B) institutionalize to enable participation by everyone; C) motivate actors for continued participation in the structures through relevant incentives.

For more details - https://ncte.gov.in/WebAdminFiles/PublicNotice/English_0_04_11_2021_637716090580188670.pdf

B1.1.6 DSEP (Decentralized skills and education networks)

This project provides open interoperable specifications for creating decentralized skills and education networks. It is an adaptation of beckn protocol core specification with added taxonomies and sample network policies for the skills and education sector.
For more details- https://dev.DIKSHA.gov.in/#/document/open-standard-specification

B1.1.7 Learning Object Model

An implied requirement of today is to provide mechanisms that store, manage, and discover resources in an efficient way. This becomes a necessity for all kinds of digital resources, the number of which is increasing at an extremely rapid rate. Digital repositories are mechanisms that fulfil this requirement if they utilize appropriate metadata schemata for the characterization of their content. Although generic metadata specifications (such as Dublin

Core) seem to fulfil the need for documenting digital objects in general, educational resources demand a more specialized treatment and characterization.

A learning object, as per IEEE, is "any entity, digital or non-digital, that may be used for learning, education or training". This repository has a collection of specifications to provide a comprehensive suite of e-learning capabilities that enable interoperability, accessibility, and reusability of digital learning objects. These specifications help in creation of well-structured descriptions of learning objects. And the well-structured descriptions will help facilitate the discovery, location, evaluation, and usage of learning objects by students, teachers or learning systems.

Content Model:

Content metadata comprises a hierarchy of elements (as shown in below figure). At the first level there are eight categories, each of which contains sub-elements; these sub-elements may be simple elements that hold data, or may themselves be aggregate elements, which contain further sub-elements. For example: "organisation framework" has sub-elements like board, medium, grade Level, etc. Some of the elements may be repeated either individually or as a group. For example: there can be multiple "attributions" where each attribution is one value (string) and there can be multiple "target frameworks" where each target framework is a group of values (for board, medium, grade Level, etc.).

For more details- https://dev.DIKSHA.gov.in/#/document/open-standard-specification

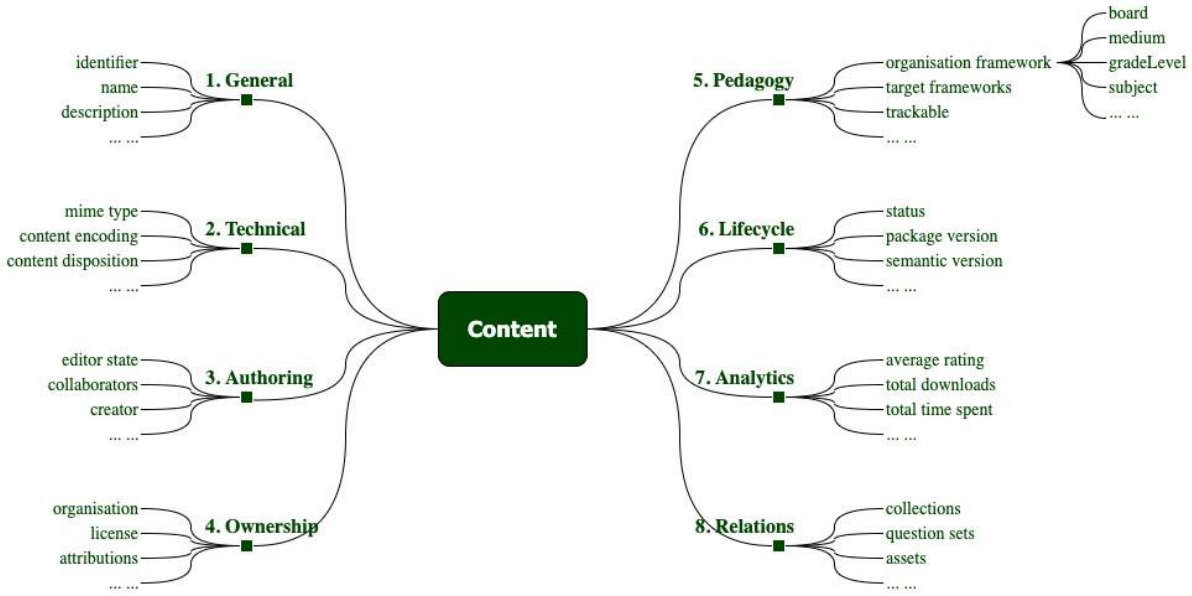


Figure 16: Learning Object Content Model

B1.1.8 SOFIE (Specification for Open Feature Integration and Extensions)

SOFIE (Specification for Open Feature Integration and Extensions) is a specification to integrate different mobile applications for feature extension or integration. DIKSHA mobile application provides the capability to integrate external third-party applications using this specification.

For more details- https://dev.DIKSHA.gov.in/#/document/open-standard-specification

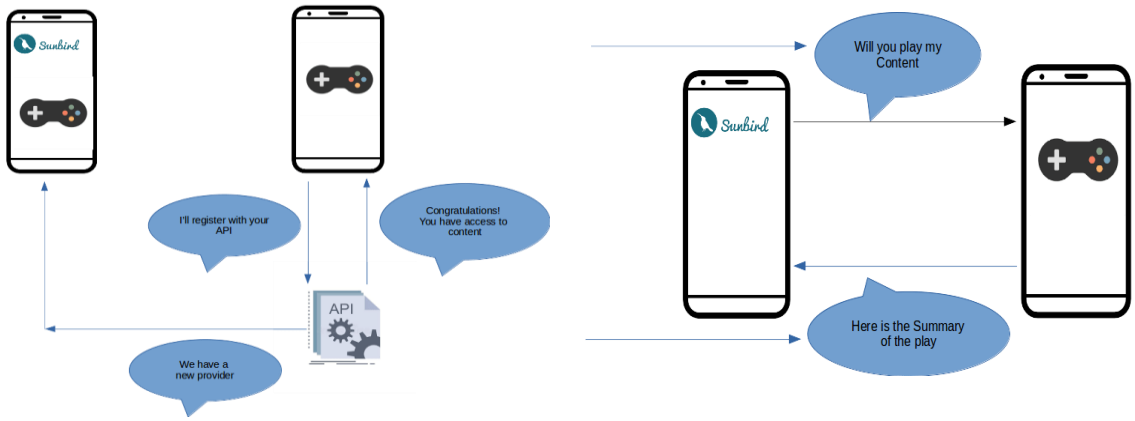


Figure 17: Interaction inside SOFIE model

B2. Standards for Consent Management

The consent of citizens is crucial in ensuring that collection of data is done in a manner consistent with the legal rights of students/ parents. It is also important to ensure that, once collected, the data captured is used and disclosed (in an identifiable or anonymised form) in a manner appropriate in law and preserving the citizen-directed constraints.

Towards these, the standards shown in below table are recommended for designing the systems and workflows required for consent management:

#	Purpose	Applicable Standards
1	Consent Framework for DigiLocker	Electronic Consent Framework (Technology Specifications vl.1) with its subsequent revision(s) published by MeitY
2	Online privacy notices and consent	ISO/IEC 29184:2020 https://gdpr-info.eu/recitals/no-32/ https://gdpr-info.eu/recitals/no-42/ https://gdpr-info.eu/recitals/no-43/

Table 7: Standards recommended for Consent Management

The above standards should be implemented in a way consistent with the applicable laws such as the Information Technology Act, 2000 (and its amendments) and various directions.

B2.1 Electronic Consent Framework for DigiLocker (Technology Specifications vl.1) published by MeitY:

With the advent of Digital India there has been an impetus towards enabling digital service delivery of both government and private services to citizens. Aadhaar based Authentication, eKYC, and eSign have enabled the service providers to onboard customers in a seamless manner. Digi-Locker offers a standardized mechanism to issue government documents to individuals and entities in electronic and printable formats, store them, and make them shareable with various agencies. All these systems require a mechanism for obtaining and preserving user consent to operate effectively and securely.

The technology framework outlined in the ECF document is designed to be open, secure, user-centric, and application-agnostic. Using this framework, data consumers (like Govt departments, employers, lenders, etc.) can access data of users from providers (like Govt departments, banks, etc.) using electronic consent, rather than requiring users to share credentials like passwords or to sign paper documents.

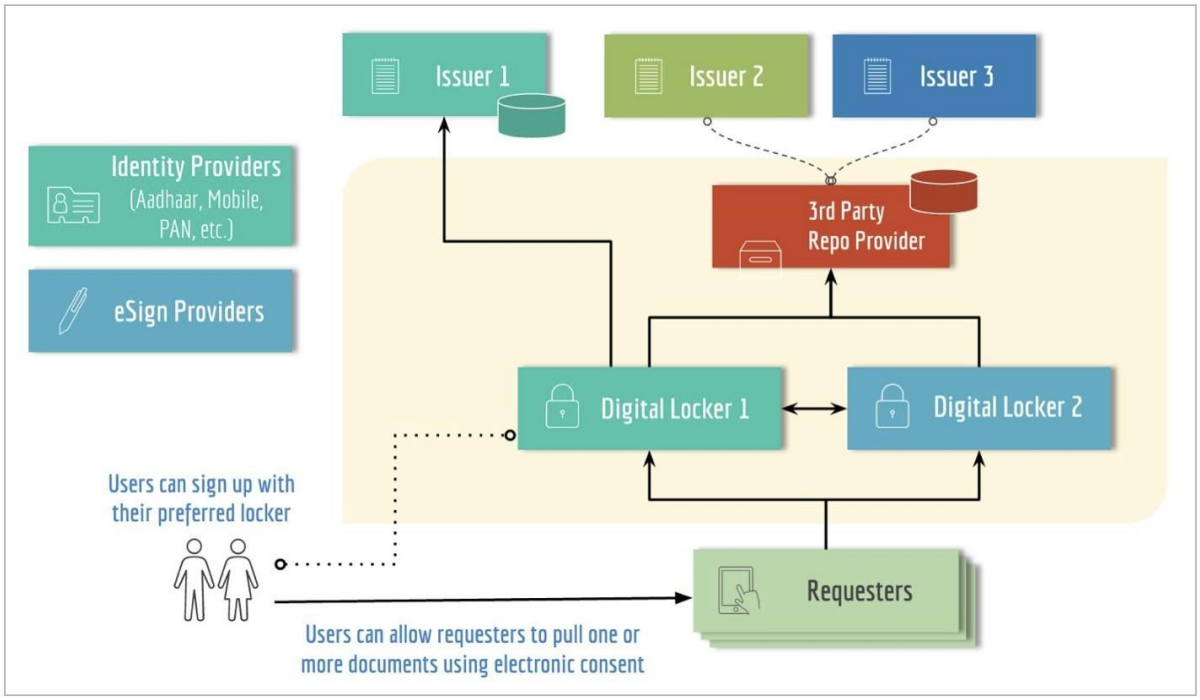


Figure 18: Workflow inside Digi Locker

B2.2 Online privacy notices and consent

These standard shapes the content and the structure of online privacy notices as well as the process of asking for consent to collect and process Personally Identifiable Information (PII) from PII principals. This standard is applicable in any online context where a PII controller or any other entity processing PII informs PII principles of processing.

General Data Protection Regulation standardizes and concretizes consent in by laying the following context:

i. Conditions of consent: Consent should be given by a clear affirmative act establishing a freely given, specific, informed, and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes, or inactivity should not therefore constitute consent. Consent

should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise, and not unnecessarily disruptive to the use of the service for which it is provided.

ii. Burden of Proof and Requirements for Consent: Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

iii. Freely given consent: In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority, and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

B3. Standards for Content

Standards for content comprises two aspects. One relates to core educational elements that groups of students should know, care about, or learn at each grade level and the other relates to quality of the content and content structure, enabling

consistency and manageability across various content. The recommended standards for content are mentioned in the table below:

#	Purpose	Applicable Standards
1	Assessment	Question Markup Language (QuML) Specifications. https://dev.DIKSHA.gov.in/#/document/open-standard-specification
2	Content packaging	IMS Global Content packaging Standards V1.3
3	Content discovery, Exchange	Standards based on Learning Object Discovery and Exchange Project Group (http://www.imsglobal.org/lode/index.html)
4	Virtual Reality Content	ISO/IEC TR 23842 ISO/IEC TR 23843

Table 8: Standards for Content

B3.1 QuML- Question Markup Language

Assessment has always played an important role in education. Most, if not all, types of formal education use some sort of assessment, typically including a final exam to earn a grade, a degree, a license, or some other form of qualification.

Today, assessment is no longer restricted to grading at the end of an instruction (summative assessment), but it has been recognized that assessment is also useful for continuous monitoring & feedback (formative assessment) and guiding of the learning progress (means to learn), without being necessarily used for grading purposes.

Questions for continuous feedback

Formative assessment, including self-assessment, can play a vital role in motivating students since it provides them with a way to judge their own competency level and allows them to track their progress. It also enables students to identify areas where more work is required, and to thereby remain motivated to improve further. Of course, this requires that students receive feedback as quickly as possible.

Formative assessment also provides timely feedback for teachers, both with respect to the effectiveness of the teaching and the performance of the students; it thus helps to identify points that might need clarification.

For both groups, teachers and students, frequent testing is preferable. Infrequent testing makes each exam a “major event”, with students investing much effort into preparation and they may even stop attending class to prepare for the exam. With infrequent tests, students may be unable to determine whether they are studying the right material and with sufficient depth.

Questions from a question bank can be used to create different types of formative assessments. Presenting questions from a question bank has many advantages. Firstly, it can ensure that questions are always fresh, do not become stale and repetitive and the questions can evolve in their precision of measuring the student’s proficiency.

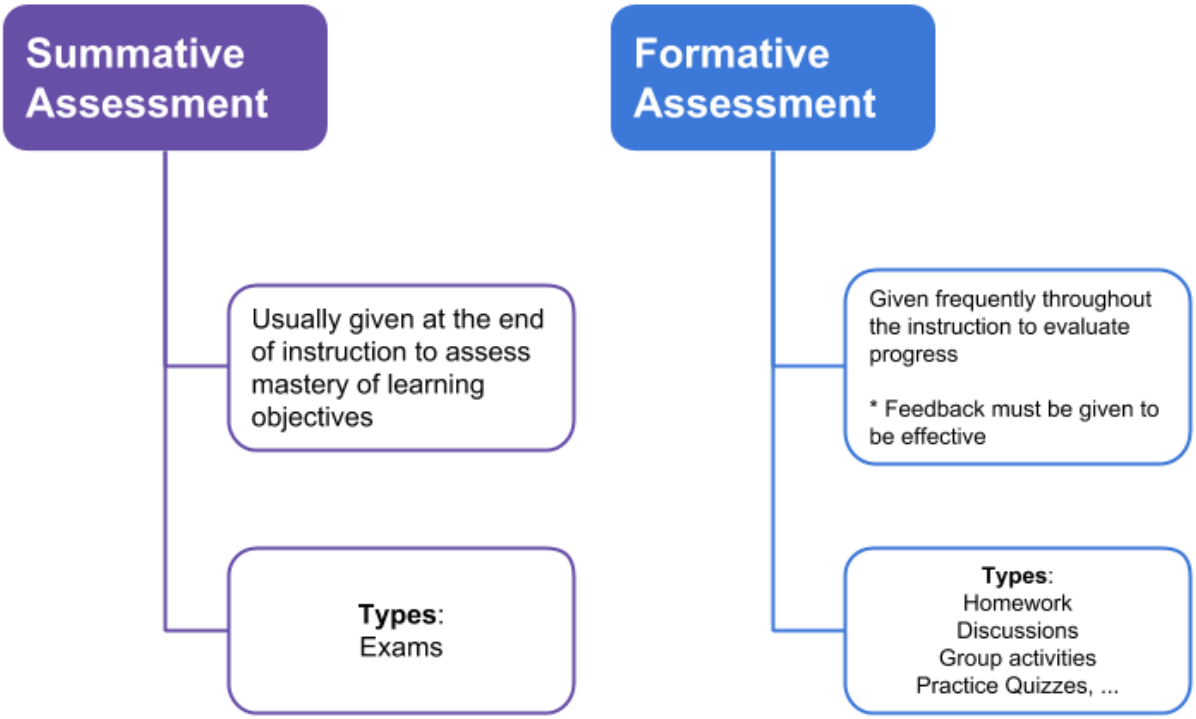


Figure 19: Reference model for assessment type

Questions as a means to learn

Answering questions and solving problems is an effective way to learn. Unlike traditional tests where the questions are used to measure the proficiency of a student, if questions are presented as learning tools, they will encourage students to do a full and meaningful enquiry about the related concepts. In fact, one of the main objectives of questions should be “achieving defined goals”. A student should be asked questions that will require him or her to use the skills that he or she is trying to learn. Such questions should be more about provoking a process of learning than about finding an answer.

If the questions focus on micro-concept level assessment of student’s proficiency, it is possible to identify strengths, areas that need focus & improvement, and recommend the relevant content to the student that specifically address the individual learning needs.

Questions that are tagged with appropriate pedagogic metadata and associated with relevant concepts will enable “questioning” to be used as an effective means to encourage learning.

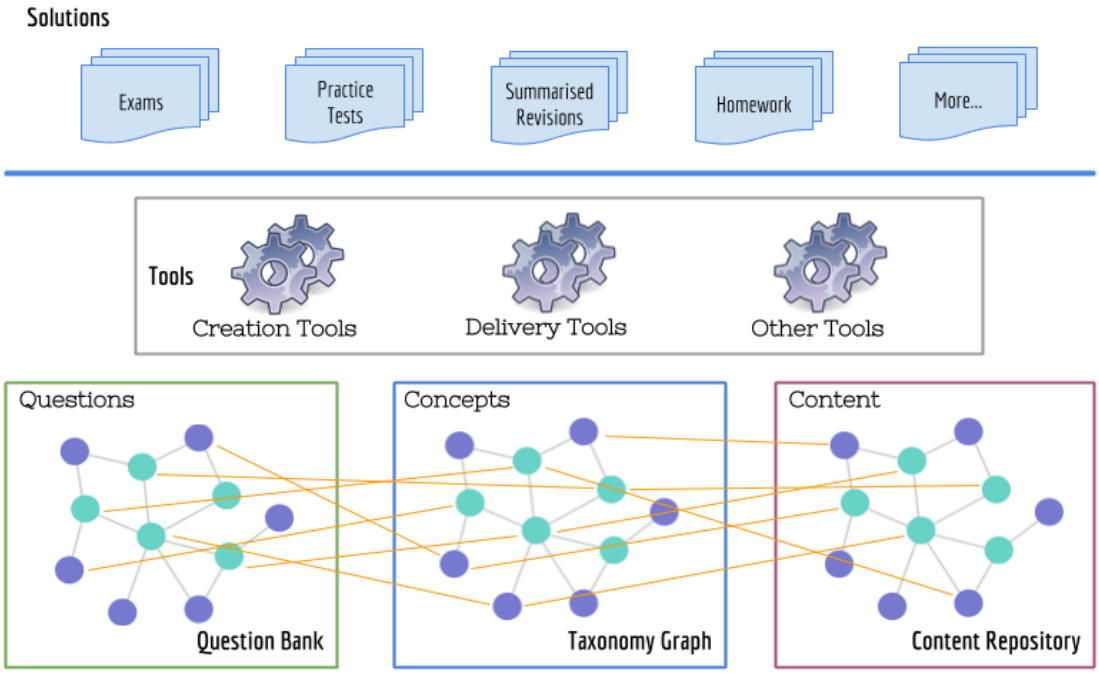


Figure 20: Assessment Design Solution

Need for a common standard

Assessment is always a time-consuming activity for teachers, especially if large numbers of students are to be assessed or, if assessment is frequent. This has motivated the development of technical devices to support assessment, starting with relatively simple mechanical devices and evolving to today’s computer-aided assessment (CAA) or e-assessment.

E-assessment is one of the fundamental elements of e-learning. E-assessments have a number of practical advantages; in particular, scoring can be automated (to most extent). This makes them especially attractive in e-learning settings, as it allows to make assessment available “anyplace, anytime”.

Creating high-quality e-assessments, however, is challenging, especially if they are to assess higher-order cognitive levels, such as application, analysis, synthesis, and evaluation in the traditional taxonomy of Bloom.

Ensuring the reusability, longevity, and platform independence of tests can mitigate the high costs of creation and can help preserve investments and intellectual assets when hardware and software change, thus ensuring sustainability. This requires a standard, platform-neutral, vendor-independent interchange file format for e-assessments.

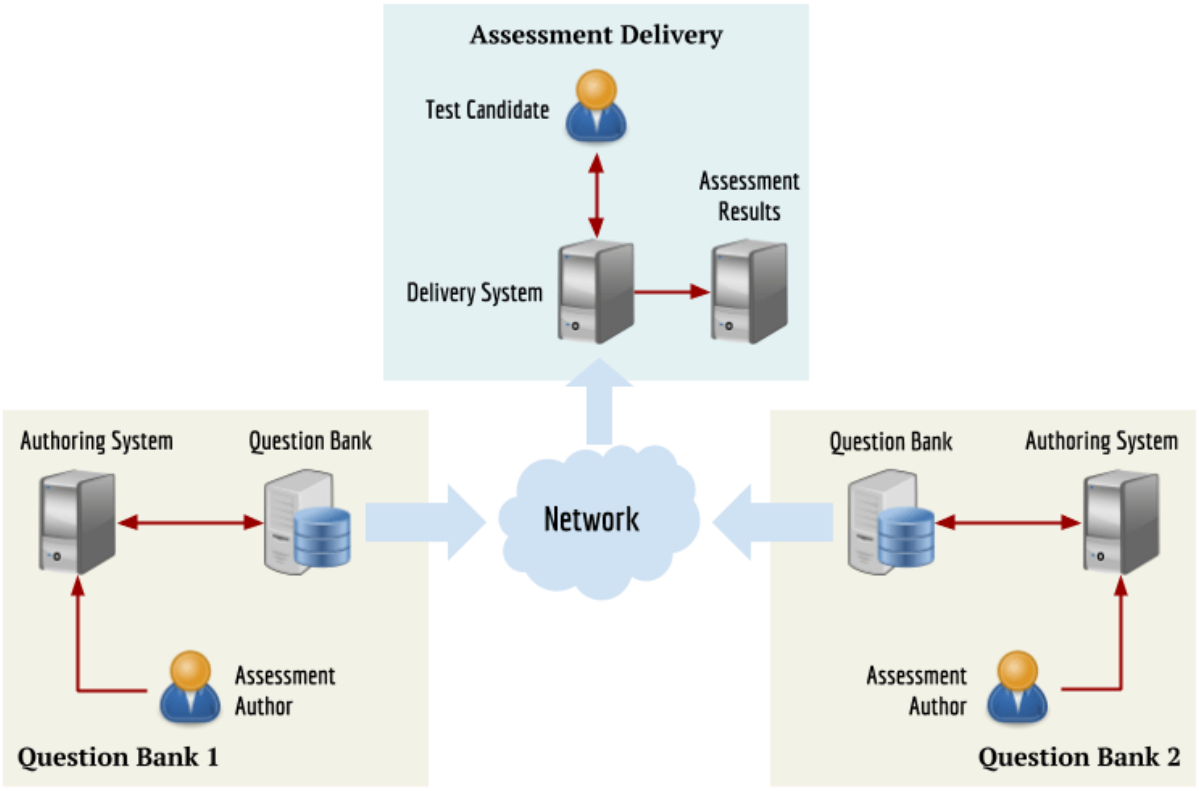


Figure 21: Assessment Design and delivery

QuML Specification

Question Markup Language (QuML in short) is a specification for storage, rendering and distribution of Questions and Tests. QuML allows assessment materials to be authored and delivered on multiple systems interchangeably. It is designed to facilitate interoperability between systems.

This specification enables aggregating questions from a wide variety of existing sources (Question papers, PDFs, documents, teachers, individuals, etc.) into one repository and stored in a common format. With all questions available in a repository and in the same format, the reach and applicability of these questions gets amplified multi-fold. When these questions are available with QuML as the interface language,

multiple applications (which understand & render QuML) can get created to serve a wide variety of use cases and users.

In a nutshell, a microservices architecture centered around “questions”, with different platforms & applications as constituent services, is possible. It allows anyone to offer a scalable, entirely new application that uses QuML questions, effortlessly.

Figure 22: QuML systems and tools

A lot of questions currently exist in PDFs, word documents, as exam papers (soft and hard copies), in the minds of teachers & other creators, in existing question repositories and in many other sources. And on the demand side, teachers, students & parents have access to some of those resources only - mainly because existing systems have access to questions from at most one source. And some of the questions are completely not accessible as there are no systems or services built for them.

If questions from multiple sources are imported into a QuML compliant question repository, multiple systems get access to all the questions. It is possible because systems need to adhere to only one specification (QuML), unlike before, where each question is stored and represented in a different way.

B3.2 Content Packaging

Content packaging refers to defining the content in a way that it is readable on a variety of platforms. It comprises meta data and meta data description in a unified format so that it can be standardized for multi-platform compatibility.

The standards lay down the different types of data structures that can be used to export, import, aggregate, and disaggregate content packages of learning, education, and training content. The specifications under the standards, support the learning activity content, location of the content, arrangement of content pieces for best instructional effect. IMS content packages of instructional content are also used in a variety of software applications.

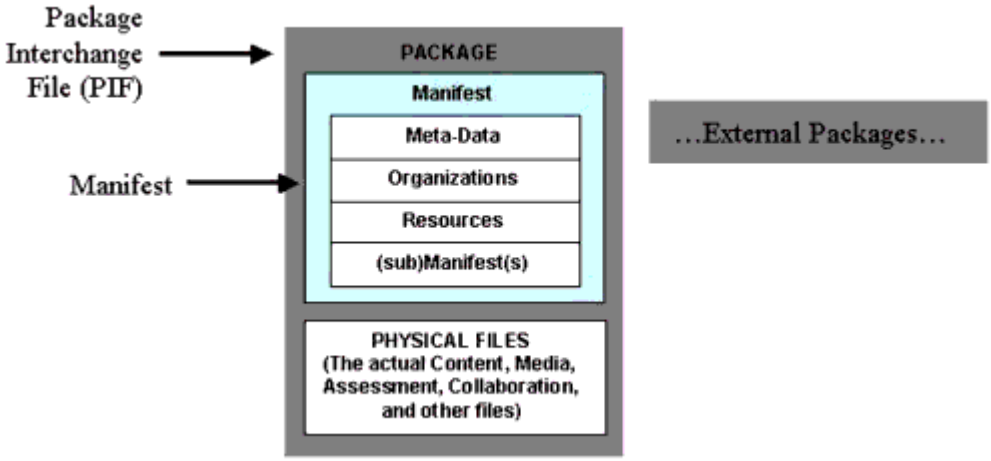


Figure 23: IMS Conceptual Packaging Conceptual Model

With the ever-increasing adoption of IMS Content Packaging, compatibility had to be the main identifier. Backward compatibility laid the foundation of this packaging model thereby ensuring the future growth while regularizing the current growth model. The IMS Content packaging specification allows adopters to gather, structure, and aggregate content in an unlimited variety of formats.

Key Elements of Content Packaging are as follows:

The content package consists of two major elements: a special XML file describing the content organization and resources in a Package, and the physical files being described by the XML. The special XML file is called the IMS Manifest file because course content and organization are described in the context of 'manifests'. Once a Package has been incorporated into a single file for transportation, it is called a Package Interchange File. The relationship of these parts to the content container is described below:

Package Interchange File - a single file, (e.g., '.zip', '.jar', '.cab') which includes a top-level manifest file named "imsmanifest.xml" and all other physical files as identified by the Manifest. A Package Interchange File is a concise Web delivery format, a means of transporting related, structured information. PKZip v2.04g (.zip) is recommended as the default Package Interchange File format. Any ZIP file format MUST conform to RFC1951.

Package - a logical directory, which includes a specially named XML file, any XML control documents it references (such as a DTD or XSD file) and contains the actual physical resources. The physical resources may be organized in sub-directories.

- Top-level Manifest - a mandatory XML element describing the Package itself. It may also contain optional (sub)Manifests. Each instance of a manifest contains the following sections:
    - Meta-data section - an XML element describing a manifest.
    - Organizations section - an XML element describing zero, one, or multiple organizations of the content within a manifest.
    - Resources section - an XML element containing references to all of the actual resources and media elements needed for a manifest, including meta-data describing the resources, and references to any external files.
    - (sub)Manifest - one or more optional, logically nested manifests.
- Physical Files - these are the actual media elements, text files, graphics, and other resources as described by the manifest(s). The physical resources may be organized in sub-directories.

Package - A Package represents a unit of usable (and reusable) content. This may be part of a course that has instructional relevance outside of a course organization and can be delivered independently, as an entire course or as a collection of courses. Once a Package arrives at its destination to a runtime service, such as an LMS vendor, the Package must allow itself to be aggregated or disaggregated into other Packages. A Package must be able to stand alone; that is, it must contain all the information needed to use the contents for learning when it has been unpacked.

Packages are not required to be incorporated into a Package Interchange File. A Package may also be distributed on a CD-ROM or other removable media without being compressed into a single file. An IMS Manifest file and any other supporting XML files required by it (DTD, XSD) must be at the root of the distribution medium.

Manifest - A manifest is a description in XML of the resources comprising meaningful instruction. A manifest may also contain zero or more static ways of organizing the instructional resources for presentation.

The scope of manifest is elastic. A manifest can describe part of a course that can stand by itself outside of the context of a course (an instructional object), an entire course, or a collection of courses. The decision is given to content developers to describe their content in the way they want it to be considered for aggregation or disaggregation. The general rule is that a Package always contains a single top-level manifest that may contain one or more

(sub)Manifests. The top-level manifest always describes the Package. Any nested (sub)Manifests describe the content at the level to which the (sub)Manifest is scoped, such as a course, instructional object, or other.

Resource - The resources described in the manifest are physical assets such as Web pages, media files, text files, assessment objects or other pieces of data in file form. Resources may also include assets that are outside the Package but available through a URL, or collections of resources described by (sub)Manifests. The combination of resources is generally categorized as content. Each resource may be described in a <resource> element within a manifest's XML. This element includes a list of all the assets required to use the resource. The files included in the Package are listed as <file> elements within such <resource> elements.

You can read further about the standards, here-

https://www.imsglobal.org/content/packaging/cpv1p1p3/imscp_infov1p1p3.html

B3.3 Content Discovery Exchange

Learning Object Discovery Exchange (LODE) i.e., Content discovery exchange aims to facilitate the discovery and retrieval of learning material such as text, images, and short videos that are combined in a precise order to provide end-users with meaningful learning experience. Learning content specifications such as IMS Content Package and IMS Common Cartridge make it more interoperable and easily exchanged over OERS and CMS.

The standards proposed by IMS Global proposes three main data models, which are as follows:

- A LODE Context Set for the Contextual Query Language (CQL): a data model for the attributes of learning objects, which can be used for search by expressing educationally meaningful queries.
- A data model, named Information for Learning Object eXchange (ILOX), that organizes sets of metadata on learning objects to be used in data exchange; and
- A data model, named Learning Object Repository Registry Data Model, for learning object collections, to be used in discovering and configuring access to those collections

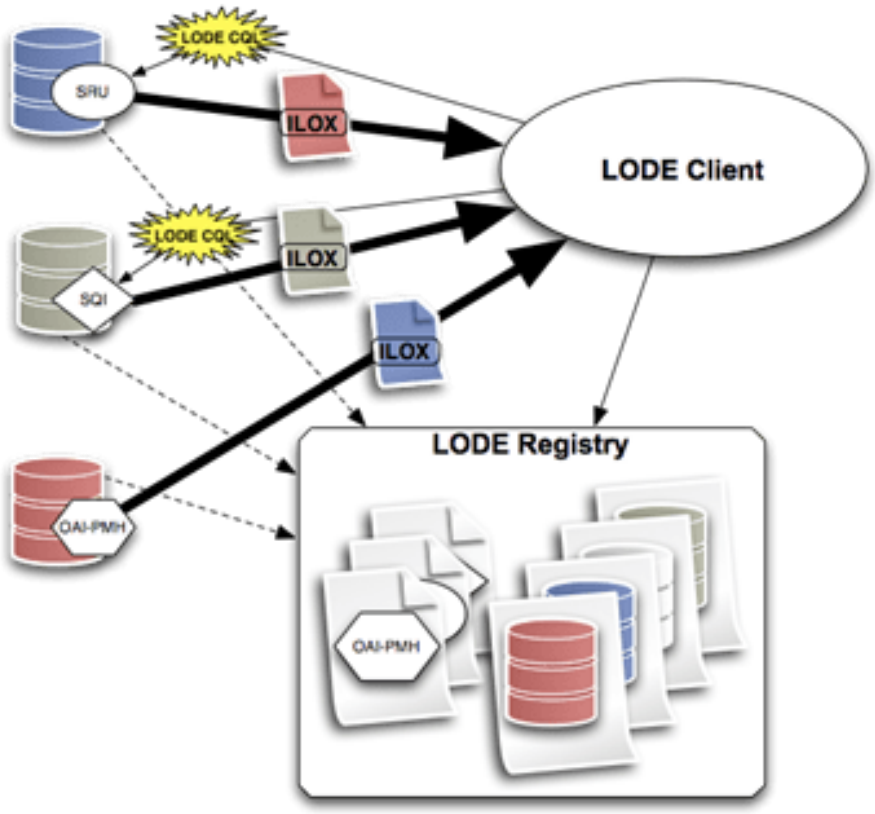


Figure 24: LODE Registry Data Model

The Learning Object Discovery & Exchange (LODE) Learning Object Registry Data Model provides a scheme of description of learning data material, the responsible people for such material, and the available mechanisms for interacting with the same.

Descriptions following this model are intended to facilitate exchange of learning content between different collections. The model provides a consistent framework, independent of local registry configuration, for:

- Collection discovery
- Evaluation and vetting of collections
- Access to collections (e.g., harvesting or searching)
- Automated configuration of access to collections

In order to access collections within repositories, the participants need a common metadata description of their respective collections, including who is responsible for the collections (and will be involved in negotiating the exchange of learning content), how to establish access to the collections, and what are the constraints on access to the collections. Having such metadata in machine-readable form allows content exchange to be substantially automated. Read here more to know in detail about the

LODE Metadata and model - https://www.imsglobal.org/LODE/spec/imsLODEv1p0bd.html

Metadata Standards

The IEEE LOM standard defines a set of meta-data elements that can be used to describe learning resources. This includes the element names, definitions, data types, and field lengths. The standard is known as a multi-part standard and defines both a conceptual model for the meta-data and an XML binding. The standard includes conformance statements for how meta-data documents must be organized and how applications must behave in order to be considered IEEE-conformant.

The IEEE conceptual data schema for meta-data definitions is hierarchical. At the base of the hierarchy is the "root" element. The root element contains many sub-elements. If a sub-element itself contains an additional sub-elements it is called a "branch". Sub-elements that do not contain any sub-elements are called "leaves". This entire hierarchical model is called the "tree structure" of a document

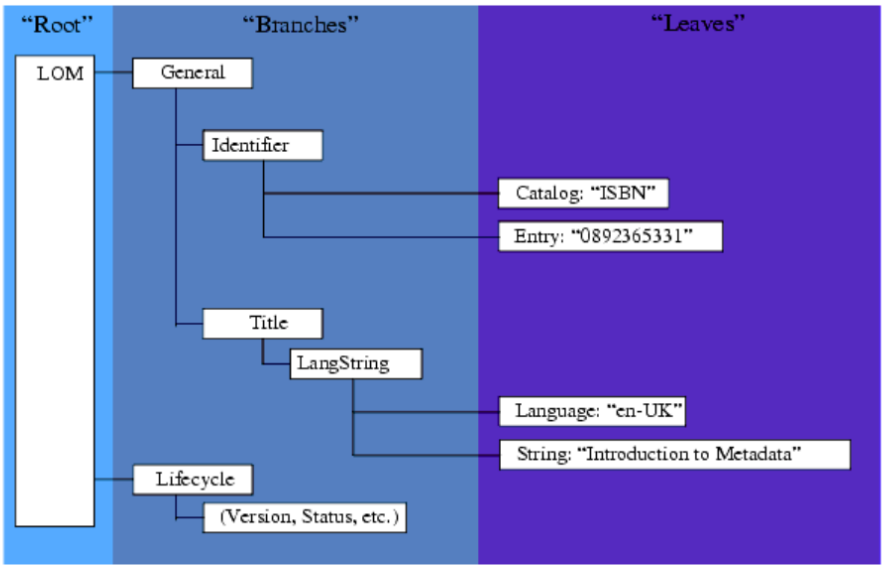


Figure 25: LODE Registry Tree structure

Read here- http://ltsc.ieee.org/wg12/index.html to know more details about the conceptual data scheme.

The conceptual data scheme is in tabular format and shows how all the different elements are divided into nine categories such as General, Life Cycle, Meta-Metadata, Technical, Educational, Rights, Relation, Annotation, and Classification.

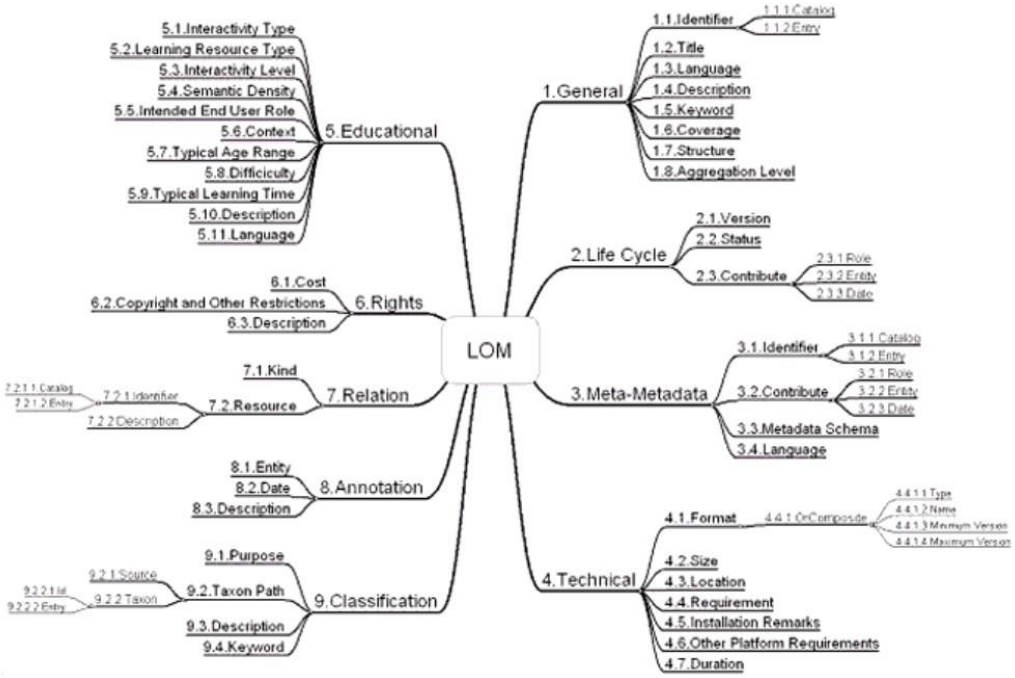


Figure 26: LOM Schema

Each leaf element in the LOM conceptual data schema has a datatype and a value space that defines the encoding of the data for that element. These data types and value spaces sometimes restrict how an element may be used, for example by specifying a restricted vocabulary, and may also provide the facility to encode extra information, such as multilingual entries.

Read more to know more about the data types and value spaces of LOM- http://www.imsglobal.org/metadata/mdv1p3/imsmd_bestv1p3.html#1621637

B3.4 Virtual Reality

Education industry is evolving rapidly, from learning online to integrating virtual reality and augmented reality in the learning modules. Many institutions are using application-dependent methods and simulation for teaching and training. However, from the point of view of ICT integration and information modelling, virtual education and training systems can be developed based on a systematic design approach with standards.

Virtual learning sessions are based on MAR concepts that include VR and AR i.e., computer simulated education and provide empirical learning in immersive virtual environments.

Virtual education is mainly of two types: online and offline, online refers to using computing devices and virtual environments and offline refers to using digital information and virtual environments.

In order to provide the capability to represent and simulate physical sensors in education and training systems, the systems require the following: representation of physical sensors, visual and functional properties of each physical sensor, physical properties of each physical sensor, control of a physical sensor's data stream, and an interface for controlling physical sensors in a 3D scene.

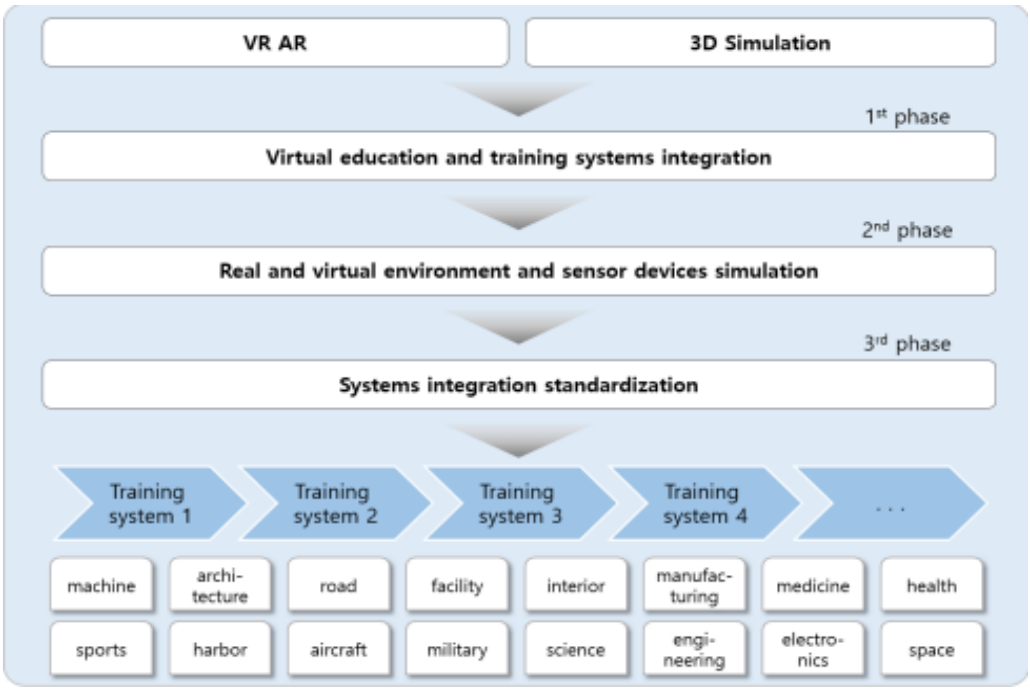


Figure 27: VR, AR, 3D simulation for training systems

The VR education mentioned above has a simulated sensor MAR world, it organizes MAR content with scene composition. ISO/IEC 18038 DIS describes details of the model 2.

Education and training content can be input to the systems via the combination of

a virtual simulation platform and an experience and knowledge database. Simulator software should be provided for education and training. This includes a simulator control management tool, operations management, and evaluation.

When developing virtual education and training systems based on the framework, the following technologies, in addition to VR and AR, are needed:

1. Content creation and manipulation
2. Information modelling
3. Visualization and simulation
4. Sensor representation
5. Real world representation
6. Graphical user interaction

Information modelling using VR and AR is necessary to be defined and implemented for virtual education and training systems so that content in knowledge databases can be simulated in virtual environments. How to define and represent education and training information in relation to VR and AR should be analysed.

- Real world representation should include real world physical objects represented in virtual environments.
- Graphical user interaction should include types and usage of interfaces with virtual environments during education and training.

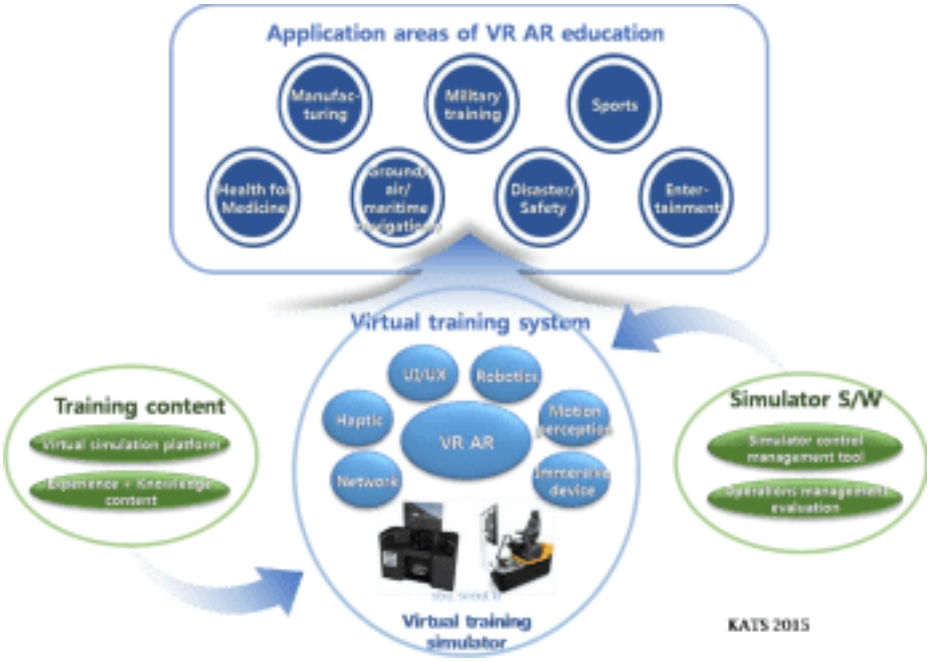


Figure 28: Virtual education and training systems framework

Standard technology for virtual education and training systems

Standard technologies should be integrated when developing virtual education and training systems. This clause describes the classification of the necessary standards and which subcommittees are related to the development of the standards. Details of the standards will be discussed in the next clause. Standard technology should be provided in the following functional areas:

1. Virtual environment representation for virtual education and training
2. Virtual simulation interface with virtual environments
3. Virtual simulation with real world environments and sensors
4. Information transmission, exchange, and interaction
5. Education and training information description and manipulation

Necessary standards	Required functions	VR AR functional type
Virtual environment representation	i. Representation methods of 3D virtual environments for virtual education ii. Application interfaces for virtual education environments	VR AR representation information modelling

	iii. Virtual world information file format	
Virtual simulation interface	i. Simulating algorithms depending on types of education and training ii. Simulating interface for education and training information	VR AR simulation in virtual worlds
Virtual simulation with real worlds	i. Real world simulation in virtual worlds using real world information ii. Interfaces for importing and exporting real world information	VR AR interface with real worlds
Information transmission	i. Multimedia compression and transmission ii. Compressed and secured information iii. Transmission for education and training	VR AR transmission
Education and training information	i. Description and manipulation of education and training information ii. Managing education and training iii. Learning, education, and training methods	Education information modelling using VR AR

Table 9: Classification of standards necessary for virtual education and training systems

Read more about the virtual reality setup in the white paper- "*Guidelines for Developing VR and AR Based Education and Training Systems"*

B4. Interoperability Standards

NDEAR seeks to connect varied systems developed using different technologies and on different platforms by different actors within the ecosystem. The standards should therefore support the integration of all such systems and are necessary to be addressed within NDEAR. Since NDEAR is built on IndEA principles, interoperability recommendations of IndEA also apply. The following are recommended interoperability standards:

#	Purpose	Applicable Standards

#	Purpose	Applicable Standards
1	School Location - Rural and Urban	Metadata & Data Standards - Local Government Directory GIS Mapping standards - ISO 19115, CSDGM (Content Standard for Digital Geospatial Metadata) School Infrastructure and Strengthening of Secondary and Higher Secondary Education (https://cpwd.gov.in/Publication/Compendium_of_Architectural_Norms%20_guidelines_for_Educational_Institutions.pdf) School Mapping https://www.education.gov.in/en/sites/upload_files/mhrd/files/upload_document/Relevent%20provision%20on%20Access%20and%20School%20Mapping.pdf https://www.educationforallinindia.com/universalisation%20of%20secondary%20education%20report%20of%20CABE%20Commuitee.pdf
2	Metadata and Data Standards for School Education	Under Development - STQC http://egovstandards.gov.in/metadata-and-data-standard https://projects.iq.harvard.edu/files/sdpfellowship/files/eimac_education_data_standards_101.pdf Statistical Standards for design of surveys, collection, processing, analysis, review, and dissemination of data - https://nces.ed.gov/statprog/2012/ Technical standards of Interoperability-

#	Purpose	Applicable Standards
		http://egovstandards.gov.in/sites/default/files/Technical%20Standards%20for%20IFEG%20Ver1.0.pdf
3	School Interoperability	Schools Interoperability Framework followed by US, UK etc. (http://specification.sifassociation.org/Implementation/US/2.5/html/index.html)
4	Learning Analytics Interoperability	ISO/IEC TR 20748-1:2016 & ISO/IEC TR 20748-2:2017
5	Metadata for Learning Resources	ISO/IEC 19788-1:2011
6	Metadata for Facilitators of Online Learning	ISO/IEC DIS 23127-1
7	Diversity and Inclusion	https://cpwd.gov.in/publication/harmonisedguidelinesdreleasedon23rdmarch2016.pdf ISO 21542:2011, Building Construction – Accessibility and Usability of the Built Environment

Table 10: Interoperability Standards

B4.1 School Location

a. School mapping - Accessibility

For improving access to secondary education following are the relevant provisions made in the framework with respect to access to the secondary school. In order to meet the challenge of Universalisation of Secondary Education (USE), there is a need for a paradigm shift in the conceptual design of secondary education. The guiding principles in this regard are Universal Access, Equality and Social Justice, Relevance and Development and

Curricular and Structural Aspects. To achieve universal access, situational strategies have been designed to set up new schools where no secondary school exists in the defined habitation, upgrade elementary schools into high schools by adding extra classrooms and other facilities, and providing additional classrooms and other related facilities in the existing secondary schools to accommodate more students.

For effective school mapping and micro planning, GIS standards are recommended practices to facilitate developing, sharing, and using GIS data, GIS software and GIS services. These standards concern the use of any geographic information including data formats, metadata, and services.

In addition to above, Local Government Directory (LD) is one of the applications developed as part of Panchayat Enterprise Suite (PES) under ePanchayat Mission Mode project (MMP) (http://epanchayat.gov.in). LGD aims to keep all information about the structure of local governments and revenue entities online. Main objective of LGD is to maintain up-to-date list of revenue entities (districts/ subdistricts/villages), local government bodies (Panchayats, Municipalities, and traditional bodies) and their wards, organizational structure of Central and State Governments and parliament and assembly constituencies and their relationship with one another.

The main stake holders of LGD are State Panchayati Raj Department, State Urban Department, State Revenue Department, or any other department of states which is responsible for formation of new districts, sub-districts/Tehsils, villages, panchayats, or any other type of local government bodies. The same can be used for school mapping. For more info - https://lgdirectory.gov.in

b. School Infrastructure standards

These standards provide rules for infrastructure support to enhance the access and to provide enabling conditions for quality education by providing access to schools, enhancing the infrastructural quality of classrooms, labs, toilets, hostels etc. and other resources of schools.

B4.2 Metadata and Data Standards for School Education

a. Education data standards

The adoption of Data Standards for use across e-Governance systems will enable easier, efficient exchange and processing of student data. It will also remove ambiguities and inconsistencies in the use of data. The data standard

enables the sharing or exchange of information between multiple users in a way that it guarantees the same understanding of what is represented within that information. When exchanged information consists of structured data, a data standard provides the description of that structure.

The purpose of Education Data Standards is to provide common element names and definitions for local and state education agencies that typically handle student demographic, achievement, staff information, and school program information. The goal of these standards is to increase the accuracy of data exchanged between systems, increase data quality by removing ambiguities in definitions, and provide a common vocabulary for educators, researchers, and other decision makers to understand what the data mean, so they can work together to improve programs and outcomes for students.

b. Statistical Standards

These standards are intended to assist the Department of Education in fulfilling the goal of providing public policy decision makers and the public informative statistical information that is: high quality, reliable, and useful. These standards and guidelines are also intended to present a clear statement for data users regarding how data should be collected in surveys, and the limits of acceptable applications and use.

c. Technology Standards on Interoperability –

Interoperability Framework for E-Governance (IFEG) in India categorizes the technical area for e-Governance applications under 7 broad Domains:

1. Presentation and Archival
2. Process
3. Data Integration
4. Meta-data
5. Data Interchange
6. Network Access and Application
7. Security

B4.3 School Interoperability

The Schools Interoperability Framework (SIF) is a technical blueprint for enabling diverse applications to interact and share data related to entities in the

Figure 29: Interoperability Framework

complete spectrum of School Education (5/Foundational + 3/Preparatory + 3/Middle + 4/Secondary) instructional and administrative environment. SIF is designed to:

- Facilitate data sharing and reporting between applications without incurring expensive development costs.
- Enhance product functionality efficiently; and
- Provide best-of-breed solutions to users easily and seamlessly.

B4.4 Learning Analytics Interoperability

Reference Model and System Requirements

The increasing amount of data being generated from learning environments provides new opportunities to support learning, education, and training (LET) in a number of new ways through learning analytics. Learning analytics is a composite concept built around the use of diverse sub-technologies, workflows and practices and applied to a wide range of different purposes. For instance, learning analytics is being used to collect, explore, and analyse diverse types and interrelationships of data, such as: learner interaction data related to usage of digital resources; teaching and learning activity logs; learning outcomes and structured data about programmes; curriculum and associated competencies.

Learning analytics is an emerging technology addressing a diverse group of stakeholders and covering a wide range of applications. Learning analytics raises new interoperability challenges related to data sharing; privacy, trust, and control of data; quality of service, etc. Through use case collection in the ad-hoc group on learning analytics interoperability, established under JTC1/SC36 in 2014, the following issues were identified and captured as general requirements for learning analytics applications:

For the learner:

- tracking learning activities and progression.
- tracking emotion, motivation, and learning-readiness.
- early detection of learner's personal needs and preferences.
- improved feedback from analysing activities and assessments.
- early detection of learner non-performance (mobilizing remediation).
- personalized learning path and/or resources (recommendation).

For the teacher:

- tracking learners/group activities and progression.
- adaptive teacher response to observed learner's needs and behaviour.
- early detection of learner disengagement (mobilizing relevant support actions).
- increasing the range of activities that can be used for assessing performance.
- visualization of learning outcomes and activities for individuals and groups.
- providing evidence to help teachers improve the design of the learning experience and resources.

For the institution:

- tracking class/group activities and results.
- quality assurance monitoring.
- providing evidence to support the design of the learning environment.
- providing evidence to support improved retention strategies.
- support for course planning.

In addition, learning analytics practice can build upon prior work in LET standardization and innovation but there are several factors that require special attention. These factors include:

- requirements arising from the analytical process.
- data items required to drive operational LET systems are not always the same as desired for learning analytics.
- volume, velocity, and variety of the data collected for analytics indicate different IT architectures, which imply different interoperability requirements.
- Use of learner data for analytics introduces a range of ethical and other socio-cultural issues beyond those which arise from exchanging data between operational systems.

B4.5 Metadata for Learning Resources

The standards specify metadata elements and their attributes for the description of learning resources. This includes the rules governing the identification of data elements and the specification of their attributes. These standards provide principles, rules, and structures for the specification of the description of a learning resource; it identifies and specifies the attributes of a data element as well as the rules governing their use. The key principles stated in the standard are informed by a user requirements-driven context with the aim of supporting multilingual and cultural adaptability requirements from a global perspective.

B4.6 Metadata for Facilitators of Online Learning

The standards specify a metadata structure to store, present and exchange online learning facilitator (OLF) information by specifying the data elements and their attributes to describe facilitator's information on various kinds of online education platforms.

This standard provides a generic information model of OLF to describe relevant information that applies to the facilitation and training services provided online, and includes information about the person offering facilitation, the affiliation of the person, facilitation ability, facilitation practices, the facilitation service offered, learners' reviews and testimonies, and related social network information. The conceptual data model allows the linguistic diversity of OLF information attributes and offers a flexible metadata schema to describe them.

B4.7 Diversity and Inclusion

The standard (BS 76005:2017) provides a framework for holistic approaches to diversity and inclusion that enable an organization to demonstrate its commitment to valuing people in its widest sense. It is intended to facilitate the fairness and dignity of all at work.

This standard provides recommendations for reviewing, assessing, and undertaking a competent and principled approach to diversity and inclusion that encompasses:

- People management and development.
- The evolution of more inclusive policies, procedures, practices, and behaviours within organizations supporting supply chain capability and diversity; and
- The building of productive relationships with others, be they customers or clients or people within communities.

This approach focuses on diversity and inclusion in organizations of all sectors, sizes, types, and stages of development. This standard recognizes that each organization is different, and that decision-makers need to determine the most appropriate approach according to their organization's context. This British Standard is intended to be used by any responsible person(s) involved in organizational leadership and management. It is also relevant to stakeholders, including a directly employed workforce, contracted workers, trade unions or workforce associations and networks, community leaders, customers, clients, and investors.

B5. Assessment and Results

Assessments are tools to understand a student's educational progress and achievement. However, India has multiple Education Boards and assessment systems which are not comparable with each other. So, it becomes difficult to judge the performance of students assessed by one system with respect to another system. There is a need to standardize assessments/ results so that each and every student is assessed through a standardized system, comparable to one another.

#	Purpose	Applicable Standards
1	Credentialing	InDEA 2_0 Report Draft V6 24 Jan 22_Rev.pdf https://www.irrodl.org/index.php/irrodl/article/view/4529/5298
2	Student Education Record (Harmonisation of marks)	Suggested in the NDEAR meeting, it is an academic bank of credit Concept note: https://www.ugc.ac.in/pdfnews/2656827_NAC-BANK.pdf

Table 11: Assessment Standards

5.1 Credentialing

Verifiable Credentials

The government, academic, industry, and other ecosystems today issue many certificates (government and non-government issued), licenses, authorization letters, etc. Unfortunately having all these in paper form creates issues of low trust, information asymmetry, costly verification procedures, and non-portability amongst many others. In addition, authenticity of such documents is not easily verifiable giving rise to fake certificates and fraud. Credentials (various certificates in digitally verifiable form) empower people and entities to make claims about them (e.g., claims about academic degree or work experience) for availing services and the service provider having the ability to verify those claims in a paperless and trusted manner.

In order to achieve its objectives, the electronic credential should enable verifiability, portability, permanence, should be self-describing, consent based and inclusive.

InDEA 2.0 proposes to adopt credential standards and specifications, standards, schema for credential issuance and implement DEPA architecture for data empowerment, the details of which can be referred from InDEA 2.0 report.

In other words, Verifiable Credentials provide standard schemas to implement Verifiable Credentials based on internationally acceptable W3C VC specifications, in the areas of skilling, education, and jobs.

DIKSHA uses this specification to create and issue credentials for users completing the various Courses and Quizzes published on DIKSHA.

Click this link to get the details of Verifiable Credentials.

Click this link to participate in the community discussions.

Open Badges

International Review of Research in Open and Distributed Learning states that an open badge is a digital micro credential that adheres to the open badge infrastructure (OBI) developed by the Mozilla Foundation and currently administered by IMS Global. OBI calls for badges to be formatted as images enriched with metadata (e.g., issuing

organization, badge description, badge requirements, submitted evidence, standards, endorsements) that allow people to
(a) digitally verify that the badge was earned by a particular recipient and
(b) gain deep insight into the actual skills the badge earner possesses.

Open badges are envisioned as
(a) remixable (i.e., they can be mixed, matched, and republished to different audiences for distinct purposes).
(b) controlled by the badge earner, rather than by an institution, in terms of how it is shared, collected, and displayed.
(c) portable across media and thus widely shareable to anyone selected by the earner; and
(d) issuable by any party, to any party, within any learning context.

They also tend to be competency-based and to require evidence of completion in order to be earned. While open badges are primarily a method for recognizing learning, they have been used for a wide variety of other purposes as well, including as
(a) a mechanism for increasing learner motivation,
(b) a means of charting learning routes or pathways, and
(c) a strategy for supporting self-reflection, planning, and learner agency.

B5.2 Student Education Record (Harmonisation of marks)

To facilitate student mobility across the education system wherein the credits can be accumulated and be used at a later point of time for the requirements of partial fulfilment of a degree program. The National Academic Credit Bank may facilitate the integration of campuses and distributed learning systems, by creating student mobility within the inter and intra University system. NAC-bank may help in seamlessly integrating skills and experiences into a credit based formal system by providing a credit recognition mechanism. The academic credits earned by a student in the system can be automatically credited to his/her account and after accumulation of credits to certain level(s) a student can accrue and redeem the credits for any academic program (educational program leading to the award of a degree/diploma/certificate) at any convenient time.
A similar framework for school students may be designed and developed for harmonization of marks.

B6. Standards for Privacy & Security

Preservation of privacy is an important consideration that needs to be incorporated in the overall design and implementation of the NDEAR. The standards and various operational requirements for privacy and data security are specified in the table below.

#	Purpose	Applicable Standards
1	Security	Digital Certificate, TLS /SSL, SHA-256, AES-256
2	Access Control	eSign (http://cca.gov.in/eSign.html)
3	Mobile Security	OWASP Mobile Security Testing Guide
4	Electronic Credential Specifications	Generic credential standard (https://www.w3.org/TR/vc-data-model/ Interoperable Credential Object Model Specifications for use in Skilling, Work, and Education domains https://github.com/INCOMS)
5	Personal Data Access – DEPA	(http://niti.gov.in/sites/default/files/2020-09/DEPA-Book_0.pdf)
6	Personal Data Protection Bill	(https://www.prsindia.org/billtrack/personal-data-protection-bill-2019) or in the form once notified under law
7	Certificates / Assessments Storage in Digi locker	Digital Locker Technology Framework (Version 1.1) (http://dla.gov.in/sites/default/files/pdf/DigitalLockerTechnologyFramework%20v1.1.pdf)

#	Purpose	Applicable Standards
8	Anonymisation	ISO 29100:2011x
9	Special Protection of Children's Personal Data	https://gdpr-info.eu/recitals/no-38/

Table 12: Privacy and Security Standards

In addition, it is important to ensure that data is reliable and verifiable. Provisions and guidelines related to the following should be incorporated in operational aspects of the NDEAR:

#	Purpose	Applicable Standards
1	Immutability	Digital Certificate, TLS /SSL, SHA-256, AES-256
2	Versioning	Design (http://cca.gov.in/eSign.html)
3	Non-Repudiation	OWASP Mobile Security Testing Guide
4	Audit Log	Generic credential standard (https://www.w3.org/TR/vc-data-model/ Academic & Interoperable Credential Object Model Specifications for use in Skilling, Work, and Education domains https://github.com/INCOMS)
5	Parent / Student Control	Parents/ students should be able to access/view their own education records anytime, and control access by others.

Table 13: Data Standards

B6.1 Security

A digital certificate is a file or electronic password that proves the authenticity of a device, server, or user through the use of cryptography and the public key infrastructure (PKI).

Digital certificate authentication helps organizations ensure that only trusted devices and users can connect to their networks. Another common use of digital certificates is to confirm the authenticity of a website to a web browser, which is also known as a secure sockets layer or SSL certificate.

A digital certificate contains identifiable information, such as a user's name, company, or department and a device's Internet Protocol (IP) address or serial number. Digital certificates contain a copy of a public key from the certificate holder, which needs to be matched to a corresponding private key to verify it is real. A public key certificate is issued by certificate authorities (CAs), which sign certificates to verify the identity of the requesting device or user.

What are the benefits of Digital Certification?

Digital certificates can be requested by individuals, organizations, and websites. To do so, they provide the information to be validated and a public key through a certificate signing request. The information is validated by a publicly trusted CA, which signs it with a key that provides a chain of trust to the certificate.

This enables the certificate to be used to prove the authenticity of a document, for client authentication, or to provide proof of a website's credential.

Who can issue a Digital Certificate?

Digital certificates are issued by CAs, which sign a certificate to prove the authenticity of the individual or organization that issued the request. A CA is responsible for managing domain control verification and verifying that the public key attached to the certificate belongs to the user or organization that requested it. They play an important part in the PKI process and keeping internet traffic secure.

Beneficial features of Digital Certificates

Digital certificates are becoming increasingly important, as cyberattacks continue to increase in both volume and sophistication. Key benefits of digital certificates include:

1. Security: Digital certificates encrypt internal and external communications to prevent attackers from intercepting and stealing sensitive data. For example, a TLS/SSL certificate encrypts data between a web server and a web browser, ensuring an attacker cannot intercept website visitors' data.

2. Scalability: Digital certificates provide businesses of all shapes and sizes with the same encryption quality. They are highly scalable, which means they can easily be issued, revoked, and renewed in seconds, used to secure user devices, and managed through a centralized platform.

3. Authenticity: Digital certificates are crucial to ensuring the authenticity of online communication in the age of widespread cyberattacks. They make sure that users' messages will always reach their intended recipient—and only reach their intended recipient. TLS/SSL certificates encrypt websites, Secure/Multipurpose Internet Mail Extensions (S/MIME) encrypt email communication, and document-signing certificates can be used for digital document sharing.

4. Reliability: Only publicly trusted CAs can issue digital certificates. Obtaining one requires rigorous vetting, which ensures hackers or fake organizations cannot trick victims that use a digital certificate.

5. Public Trust: Using a digital certificate provides confirmation that a website is genuine, and that documents and emails are authentic. This projects public trust, assuring clients that they are dealing with a genuine company that values their security and privacy.

Why do we need Digital Certificates?
Digital certificates act as trust documents. It states that you are the one who has transformed the information by digitally signing the information. It helps the recipient in identifying the authenticity of the sender.

The digital certificate can be used for securing email as well as web-based transactions or to identify other participants of the transactions. The Certificate proves the ownership of a domain name and establishes SSL/TLS encrypted secured sessions between the website and the user for the transaction. As a developer, you can use a digital certificate for the authorship of a code and can retain the integrity of

the distributed software programs. The certificates can also be used for filing income tax returns, signing web forms, e-tendering documents, etc.

Servers and clients use the certificate issued by the Certificate Authorities. The certificate binds the public key to the person or to the server. After that, it validates the connection and prevents impersonation.

A TLS/SSL certificate sits on a server— such as an application, mail, or web server— to ensure communication with its clients is private and encrypted. The certificate provides authentication for the server to send and receive encrypted messages to clients. The existence of a TLS/SSL certificate is signified by the Hypertext Transfer Protocol Secure (HTTPS) designation at the start of a Uniform Resource Locator (URL) or web address.

B6.2 Access Control

For creating electronic signatures, the signer is required to obtain a Digital Signature Certificate (DSC) from a Certifying Authority (CA) licensed by the Controller of Certifying Authorities (CCA) under the Information Technology (IT) Act, 2000. Before a CA issues a DSC, the identity and address of the signer must be verified. The private key used for creating the electronic signature is stored in hardware cryptographic token which is of one-time use. This current scheme of in-person physical presence, paper document-based identity & address verification and issuance of hardware cryptographic tokens does not scale to a billion people. For offering fully paperless citizen services, mass adoption of digital signatures is necessary. A simple to use online service is required to allow everyone to have the ability to digitally sign electronic documents.

eSign is an online electronic signature service which can be integrated with service delivery applications via an API to facilitate an eSign user to digitally sign a document. Using authentication of the eSign user through e-KYC service, online electronic signature service is facilitated.

1. Easy and secure way to digitally sign information anywhere, anytime - eSign is an online service for electronic signatures without using physical cryptographic token. Application service providers use e-KYC service to authenticate signers and facilitate digital signing of documents.
2. Facilitates legally valid signatures - eSign process includes signer consent, Digital Signature Certificate issuance request, Digital Signature creation and affixing as well as Digital Signature Certificate acceptance in accordance with

provisions of Information Technology Act. Comprehensive digital audit trail, in-built to confirm the validity of transactions, is also preserved.

3. Flexible and easy to implement - eSign provides configurable authentication options in line with e-KYC service and also records the e-KYC ID used to verify the identity of the signer. The authentication options for eKYC include biometric or OTP of the e-KYC service provider. eSign enables eSign users' easy access to legally valid Digital Signature service.
4. Respecting privacy - eSign ensures the privacy of the signer by requiring that only the thumbprint (hash) of the document be submitted for signature function instead of the whole document.
5. Secure online service - The eSign service is governed by e-authentication guidelines. While authentication of the signer is carried out using e-KYC services, the signature on the document is carried out on a backend server of the e-Sign provider. eSign services are facilitated by trusted third party service providers - currently Certifying Authorities (CA) licensed under the IT Act. To enhance security and prevent misuse, eSign user's private keys are created on Hardware Security Module (HSM) and destroyed immediately after one time use.

B6.3 Mobile Security

Mobile device security refers to being free from danger or risk of an asset loss or data loss using mobile computers and communication hardware.

Importance of Mobile Security

The future of computers and communication lies with mobile devices, such as laptops, tablets, and smartphones with desktop-computer capabilities. Their size, operating systems, applications, and processing power make them ideal to use from any place with an internet connection. And with the expansion of ruggedized devices, the Internet of Things (IoT) and operating systems, such as Chrome OS, macOS and Windows 10, every piece of hardware that's enhanced with this software and capabilities becomes a mobile computing device.

Authentication and authorization across mobile devices offer convenience but increase risk by removing a secured enterprise perimeter's constraint. For example, a smartphone's capabilities are enhanced by multi-touch screens, gyroscopes, accelerometers, GPS, microphones, multi-megapixel cameras and ports, allowing the attachment of more devices. These new capabilities change the way users are authenticated and how authorization is provided locally to the device and the

applications and services on a network. As a result, the new capabilities are also increasing the number of endpoints that need protection from cybersecurity threats.

OWASP Mobile Security Testing Guide (MSTG)

The Mobile Security Testing Guide (MSTG) is a comprehensive manual enlisting the guidelines for mobile application security development, testing, and reverse engineering for iOS and Android mobile security testers.

Security testing of mobile applications has to be done throughout the phase of its development, right up until its release.

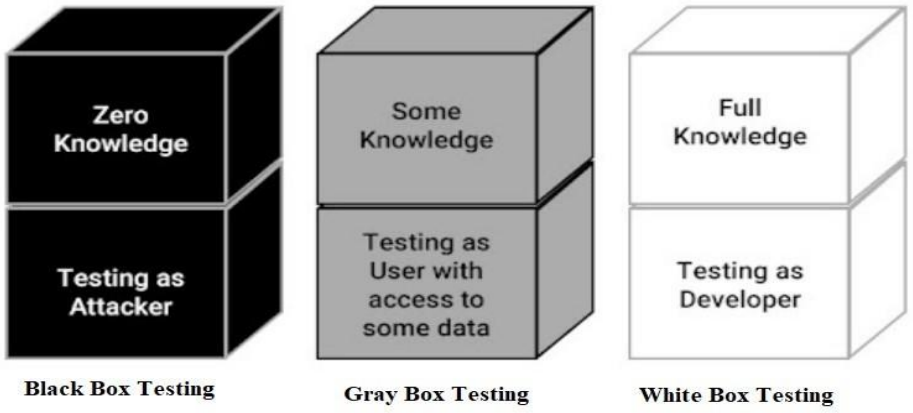


Figure 30: OWASP Mobile Security Testing model

Mobile apps differ from web apps in that they have a smaller attack surface and hence higher protection against cyber threats. To improve mobile app security, we must prioritize data protection on the mobile and the network.

Given below are the key areas in mobile app security.

1. Local data storage - When creating mobile apps, you must exercise extreme caution when storing user data. If an app inappropriately exploits operating system APIs like local storage, it may expose sensitive data to other apps running on the same device.
2. Authentication and Authorization - The endpoint handles the majority of the authentication and authorization logic. Unlike web apps, the users unlock mobile apps using user-to-device authentication capabilities like fingerprint scanning, instead of entering complex passcodes. Security testers must keep in mind the benefits and drawbacks of various authorization systems.
3. Communication with endpoints - Mobile devices provide the door to a wide range of network-based assaults, from simple to complex. Therefore, apps

must use the TLS protocol to establish a secure, encrypted channel for network connection. Maintaining the integrity of information sent between the mobile app and distant service endpoints is critical.

4. Interaction with mobile platform - Mobile operating systems have greater inter-process communication tools (IPC tools), allowing apps to exchange signals and data. These platform-specific capabilities have their own set of drawbacks. If IPC APIs are utilized incorrectly, confidential data may be inadvertently exposed.
5. Code quality and exploit mitigation - Because of the smaller attack surface, mobile apps have a lesser attack surface than online apps. Cross-site scripting is potentially conceivable in some instances on mobile. Therefore, you must follow practices for security, creating secure release builds.
6. Anti-tampering and anti-reversing - Because software protection features are frequently utilized in the mobile app market, security testers must learn how to get around them. Client-side protections have a benefit, provided you implement them with reasonable expectations in mind and are not utilized to substitute security controls.

Strategy for Security Testing

Strategy for Security Testing Security testing, like functionality and requirement testing, necessitates an in-depth understanding of the app as well as a well-defined plan for carrying out the actual testing. Given below are a few strategies for security testing,

- Nature of the app - You have to decide how much security testing is necessary based on the type and purpose of your app. For instance, if it deals with financial transactions, you have to check payment gateways and add a multi-factor or a two-factor authentication. To add an extra layer of security, fingerprint or password login needs to be authorized.
- Time required for testing - You must evaluate how much time you can commit to security testing based on the total time allotted for testing.
- Efforts needed for testing - Security testing is more difficult than other sorts of testing because there are few project rules for it. Therefore, you and your team must define and agree with the testing requirements.
- Knowledge transfer - You might need extra time studying the code or tools to comprehend the app's security and related testing. Devote extra time for this knowledge transfer before making a final testing strategy.

B6.4 Electronic Credential Specifications

Electronic Authentication (or “e-Authentication”) is the process of electronic verification of the identity of an entity. The entity may be a person using a computer/mobile, a computer/mobile itself or a computer/mobile program. Authentication is a way to ensure that the user who attempts to perform functions in a system is in fact the user who is authorized to do so. e- Authentication provides a simple, convenient and secure way for the users to access government services via internet/mobile as well as for the government departments and agencies to assess the authenticity of the users.

Benefits of e-Authentication

Electronic authentication helps to build confidence and trust in online transactions and encourages the use of the electronic environment as a channel for service delivery. In online transactions, data is communicated electronically through internet and mobile applications. With the increased prevalence of online transactions, there is a need to set up suitable e- authentication processes based on an assessment of the risks associated with these transactions.

Overview of e-Authentication Mechanisms

Electronic authentication is accomplished based on the following factors:

- Knowledge - something the user knows (e.g. username, password, PIN, secret questions, and answers, etc.).
- Possession - something the user has (e.g. digital signature, smart card, etc.).
- Be - something the user is (e.g., biometric fingerprint, iris pattern, etc.); or
- A combination of the above.

Utilizing one or more of these factors, there may be three kinds of authentication mechanisms:

- Single Factor Authentication: An authentication mechanism that utilizes only one of the various factors (e.g., a user using username and password for accessing an application).
- Two Factor Authentication: An authentication mechanism where a combination of two factors is used (e.g., a user using username and password as first factor and One Time Password (OTP) as the second factor).

- Multi-factor Authentication: An authentication mechanism where two or more factors are used with one of the factors necessarily being the “Third Factor – ‘Be’” which is something the user is (e.g., a user providing her Aadhaar number (first factor – “Knowledge”) and her biometrics (third factor – “Be”) to authenticate herself).

Key Components of e-Pramaan Framework

1. Identity Management: Identity management is a significant component of e-Pramaan Framework to ensure trusted and reliable online delivery of government services to the authenticated users. Authentication and authorisation should be considered within the context of identity management.
2. e-Authentication : e-Authentication is the process of verifying the identity of an entity.
3. Authorisation: Authorisation is the process of verifying that a known person has the permissions and rights to perform a certain operation in an application. Authentication, therefore, must precede authorisation. An effective access management system incorporates one or more methods of authentication to verify the identity of the user, including passwords, digital certificates, hardware or software tokens, and biometrics. Authorisation governs what a user can access or do within an application. It lets the right users manage the content they have access to and the actions they can perform.
4. Credential Registration: Credential registration is the process which results in issuance of an e-authentication credential, using which an identity can be electronically verified. The credential can be of different strengths, e.g., a password, a token, a digital certificate, or a biometric parameter. The strength of the credential required will be determined by the sensitivity level requirements of the application or transaction. Credential registration process may consist of a combination of the following elements:
    a. Online/Offline process to allow users to register with the required identity and associated information
    b. Creating user entries in an identity directory: The database includes users’ identities and associated information.
    c. Issuing a credential to a user: This credential will be used in the e-authentication process. The directory keeps the details regarding the credentials.
5. Permission Assignment: In order to provide the user access to online services, appropriate permissions need to be assigned to the user as part of the permission assignment process after issuance of the credentials. Permission assignment may be implemented in one of the following ways –

a. As an extension of the credential registration process: Access permissions may be assigned to the user for services delivered by the government departments and agencies as part of the credential registration process.
b. As a separate activity performed at some time after registration: Access permissions may be assigned to the user based on a credential issued by some other agency at a later point of time.

6. Deregistration: Deregistration is the process of de-provisioning a user from a system. As the authority of individuals may change over time, a comprehensive deregistration process helps to manage these relationships accurately.
7. Single Sign-On: Single sign-on is a specialized form of e-authentication that enables a user to authenticate once and gain access to the resources of multiple applications. With this property, a user logs in once and gains access to all systems without being prompted to log in again at each of them.

However, the user may be prompted to provide an additional authentication credential, such as an OTP, a token, a digital certificate, a biometric parameter, etc. in the subsequent applications depending upon the sensitivity level of that application or transaction.

B6.5 Personal Data Access – DEPA

India's Data Empowerment and Protection Architecture (DEPA) is predicated on the notion that individuals should have control over how their personal data is used and shared. It is designed with the belief that agency over data could empower Indians with opportunities to improve their own lives.

DEPA is designed as an evolvable and agile framework for good data governance, given the rapid pace of change in this arena. In a nutshell, it empowers people to access their data and share it with third party institutions seamlessly and securely.

DEPA is a paradigm shift in personal data management and processing that seeks to transform the current organization centric data sharing approach to an individual centric system.

Guiding Principles of DEPA

1. Restoring Agency and User Control: Individuals are empowered actors, not passive targets, in the management of their personal lives (both online and

offline) they should have both the right and the practical means to manage their data and privacy.

2. Informed consent: Consent is an expression of human autonomy. For such an expression to be genuine, it must be informed and meaningful. Personal data should never be shared without consent.
3. Institutional and Data Controller Accountability: While customers are in control and can consent to various uses of their data, individual consent does not absolve institutions holding data (data fiduciaries) of responsibility to protect, manage, and minimize data misuse. They can and will be penalized under governing laws for misusing data, not taking appropriate measures to ensure data security, and misusing the consent framework.
4. Accessibility and Affordability: It is essential that personal data is technically easy to access and use – it is accessible in machine-readable open formats via secure, standardized APIs (Application Programming Interfaces) which can be leveraged by various organizations to present information in a user-friendly and virtual form. DEPA enables the break-down of closed silos enabling personal data to become an important, reusable resource accessible to all with appropriate permissions. Moreover, the objective is to allow for data accessibility and empowerment in a broad and inclusive manner across the population, not just for the wealthiest or the most technologically savvy.
5. Shared open infrastructure: A shared infrastructure and set of standards enables decentralized management of personal data and allows interoperability across the many decentralized players (allowing individuals to change service providers without proprietary data lock-ins). It also makes it easier for companies to comply with tightening data protection regulations.
6. Incentive alignment: For DEPA to be successful, it is critical that the incentives of individuals are aligned with institutions operationalizing their data rights. Under the status quo, data fiduciaries have very different incentives around data use. Therefore, it will be necessary to create new institutions that have incentives more closely aligned with those of individuals, in order to help empower individuals with their data.
7. Reciprocity: Although initial market players will want to only be information users rather than providers, for the ecosystem to thrive players will need to be both information providers and users. Therefore, the DEPA market architecture will function on the reciprocity principle; all data user agencies must also adopt the technology standards required to be information providers to ensure sustainability of the ecosystem.
8. Technology agnosticism & interoperability: The architecture must be technology agnostic. It must be flexible enough to consider evolving technologies and standards of compliance. The technical specifications for

data flows and consent flows moreover will be agnostic to the kind of data that flows (for example, specifications not particular to a sector or type of data).

9. Data minimisation: Data that is processed and shared ought to be minimal and necessary for the purposes for which such data is sought and other compatible purposes beneficial for the data subject.
10. Enabling other data rights: DEPA ought to make it easier for individual users to operationalise (through market structures and technology tools, for example) the right to know how your data is being used, the right to share only purpose-specific data, and the right to be forgotten or to have your data be deleted. However, this is premised on the existence of a legal framework that calls out the importance of these rights.
11. Evolvability: The final principle is that of evolvability. Recognising that this - more than almost any other area of regulation, governance, or service delivery - is an emerging space shaped by rapidly advancing technology possibilities and evolving market dynamics, DEPA's architecture and building blocks must be built to change in order to stay current.

Personal Data Protection Bill

The Personal Data Protection Bill, 2019 was introduced in Lok Sabha by the Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad, on December 11, 2019. The Bill seeks to provide for protection of personal data of individuals and establishes a Data Protection Authority for the same.

1. Applicability: The Bill governs the processing of personal data by:
    a. Government,
    b. companies incorporated in India, and
    c. foreign companies dealing with personal data of individuals in India. Personal data is data which pertains to characteristics, traits, or attributes of identity, which can be used to identify an individual.

    The Bill categorizes certain personal data as sensitive personal data. This includes financial data, biometric data, caste, religious or political beliefs, or any other category of data specified by the government, in consultation with the Authority and the concerned sectoral regulator.

2. Obligations of data fiduciary: A data fiduciary is an entity or individual who decides the means and purpose of processing personal data. Such processing will be subject to certain purpose, collection, and storage limitations. For instance, personal data can be processed only for specific, clear, and lawful purposes. Additionally, all data fiduciaries must undertake certain transparency and accountability measures such as: (i) implementing security

safeguards (such as data encryption and preventing misuse of data), and (ii) instituting grievance redressal mechanisms to address complaints of individuals. They must also institute mechanisms for age verification and parental consent when processing sensitive personal data of children.

3. Rights of the individual: The Bill sets out certain rights of the individual (or data principal). These include the right to: (i) obtain confirmation from the fiduciary on whether their personal data has been processed, (ii) seek correction of inaccurate, incomplete, or out-of-date personal data, (iii) have personal data transferred to any other data fiduciary in certain circumstances, and (iv) restrict continuing disclosure of their personal data by a fiduciary if it is no longer necessary or consent is withdrawn.
4. Grounds for processing personal data: The Bill allows processing of data by fiduciaries only if consent is provided by the individual. However, in certain circumstances, personal data can be processed without consent. These include: (i) if required by the State for providing benefits to the individual, (ii) legal proceedings, (iii) to respond to a medical emergency.
5. Social media intermediaries: The Bill defines these to include intermediaries which enable online interaction between users and allow for sharing of information. All such intermediaries which have users above a notified threshold, and whose actions can impact electoral democracy or public order, have certain obligations, which include providing a voluntary user verification mechanism for users in India.
6. Data Protection Authority: The Bill sets up a Data Protection Authority which may: (i) take steps to protect interests of individuals, (ii) prevent misuse of personal data, and (iii) ensure compliance with the Bill. It will consist of a chairperson and six members, with at least 10 years' expertise in the field of data protection and information technology. Orders of the Authority can be appealed to an Appellate Tribunal. Appeals from the Tribunal will go to the Supreme Court.
7. Transfer of data outside India: Sensitive personal data may be transferred outside India for processing if explicitly consented to by the individual, and subject to certain additional conditions. However, such sensitive personal data should continue to be stored in India. Certain personal data notified as critical personal data by the government can only be processed in India.
8. Exemptions: The central government can exempt any of its agencies from the provisions of the Act: (i) in interest of security of state, public order, sovereignty and integrity of India and friendly relations with foreign states, and (ii) for preventing incitement to commission of any cognisable offense (i.e., arrest without warrant) relating to the above matters. Processing of personal data is also exempted from provisions of the Bill for certain other purposes such as: (i)

prevention, investigation, or prosecution of any offense, or (ii) personal, domestic, or (iii) journalistic purposes. However, such processing must be for a specific, clear, and lawful purpose, with certain security safeguards.

9. Offenses: Offenses under the Bill include: (i) processing or transferring personal data in violation of the Bill, punishable with a fine of Rs 15 crore or 4% of the annual turnover of the fiduciary, whichever is higher, and (ii) failure to conduct a data audit, punishable with a fine of five crore rupees or 2% of the annual turnover of the fiduciary, whichever is higher. Re-identification and processing of de-identified personal data without consent is punishable with imprisonment of up to three years, or fine, or both.
10. Sharing of non-personal data with government: The central government may direct data fiduciaries to provide it with any: (i) non-personal data and (ii) anonymised personal data (where it is not possible to identify data principal) for better targeting of services.
11. Amendments to other laws: The Bill amends the Information Technology Act, 2000 to delete the provisions related to compensation payable by companies for failure to protect personal data.

DEPA's Institutional Architecture

To ensure individual data rights around privacy and portability are protected, a new class of institutions must be created that have economic incentives aligned with those of the users when it comes to the sharing of personal data. Under DEPA, the interaction between an individual, a potential data user, and the data fiduciary holding a user's information will be mediated through consent managers - organizations maintaining the 'electronic consent dashboard' for users. Consent Managers will be in the business of making sure individual data is not shared without user consent.

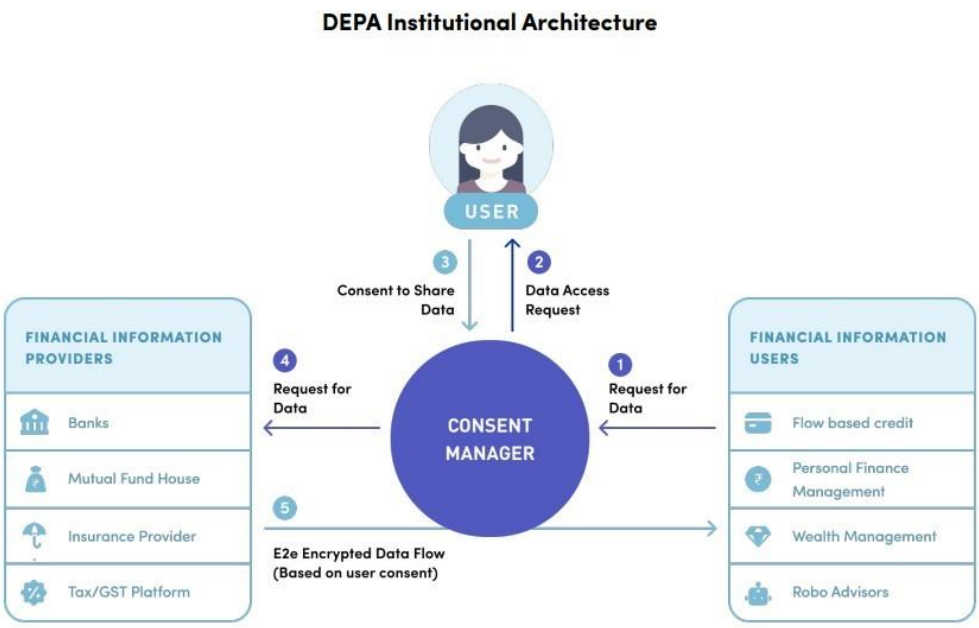


Figure 31: DEPA's Technology Architecture

DEPA's Technology Architecture

In order to enable a thriving ecosystem of data access fiduciaries, a variety of digital public goods have been created:

1. An Electronic Consent Framework, with a specification for a consent artifact managed by MeitY.
2. Data Sharing API Standards to enable an encrypted flow of data between data providers and users
3. Data Information Standard for the launch of DEPA that is sector specific. For the financial sector, this is the Financial Information Standard which explains the required shared elements of a bank statement across institutions for instance.

Critically, these are the basic building blocks of a DEPA technology framework. As DEPA evolves, other technology modules should be added which better preserve privacy and data rights - through a combination of public and private players.

APIs for Data Sharing

Application Programming Interfaces (APIs) enable seamless interaction flow of and encrypted data flow between data providers and data users through a consent

manager. Institutions adopting DEPA APIs can provide data in a machine-readable format to all licensed consent managers. As a result, it is possible to build a centralized dashboard where the individual may grant access and give or cancel permissions for multiple data sources and services. Any service provider can build a consent manager API and enable their service to be connected with the accounts directly.
A standardized Consent Management architecture makes the accounts interoperable and allows individuals to easily switch operators. This is a major element contributing to DEPA's trustworthiness. Interoperability is the core advantage provided by a consent manager, but it is also the core challenge: interoperability within the data management system can be understood as functioning similarly to interoperability in mobile telephone networks. Both systems require a common network that connects distributed nodes.

Data Protection and Processing Standards

DEPA also relies on adoption of related technology standards around data storage and processing techniques. Some of these are outlined in the Personal Data Protection Bill - which for instance states that all processing of sensitive and critical data must occur within India. Further technology standards around data storage, based on the sensitivity of data, ought to be designed and regulated by the forthcoming Data Protection Authority.

B6.6 Certificates/Assessments storage in Digi locker

Digital India aims to transform India into a knowledge-based economy.

The key vision areas under the Digital India Programme are to "provide shareable private space on a public cloud" and to "digitize all documents and records of the citizens and make them available on a real-time basis".

The mechanism of 'Digital Lockers' will greatly improve the citizen convenience and usher in paperless transactions across the entire ecosystem of public services. This entire ecosystem of Digital Lockers for accessing e-Documents via a standard set of interoperable APIs are together covered under this 'Digital Locker Technology Framework'.

Digital Locker Objectives

1. Enable digital empowerment of individuals by providing them with a choice of Digital Locker on the cloud offered by one of the providers.

2. Enable self-signing via e-Sign and make them available electronically.
3. Minimize the use of physical documents.
4. Ensure authenticity of the e-documents and thereby eliminate usage of fake documents.
5. Secure access to various Government issued documents.
6. Reduce administrative overhead of Govt. departments and agencies using electronic documents thus making it easier for the individuals to receive services in a paperless manner.
7. Anytime, anywhere access to their documents by the individuals.
8. Open and interoperable architecture for creating a multi-provider ecosystem providing choice to the issuers, requesters, and individuals. This also allows rapid digitalization across various systems.
9. Architecture to support a well-structured standard document format to support easy sharing of documents across departments and agencies.
10. Ensure privacy and security through user authentication and consented access to documents.

Digital Locker Ecosystem

The following figure depicts the Digital Locker Landscape. Citizens, Issuers, Requestors and Digital Locker are the main components. Digital Locker links various issuer repositories using a set of APIs.

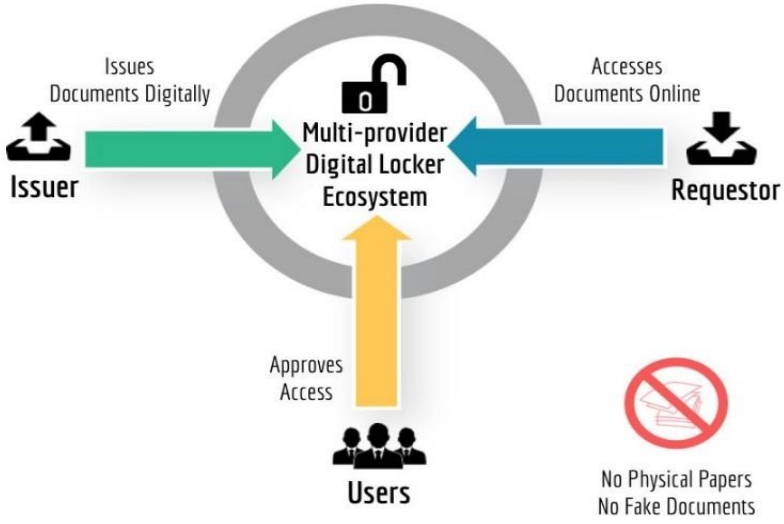


Figure 32: Digital Locker Technology Specifications (DLTS)

Digital Locker Technology Specifications (DLTS)

Digital Locker system consists of e-Documents repositories and Digital Lockers for providing an interoperable, federated, and online mechanism for issuers to store and requesters to access various digital documents in real-time with authorized user consent.

1. Key Terminology
    a. Electronic Document or E-Document – A digitally signed electronic document in PDF or XML format issued to one or more individuals or entities.
    b. Repository – A software application complying with specifications under this framework, hosting a collection (database) of e-documents and exposing a standard API for secure real-time access.
    c. Digital Locker – A dedicated secure storage space assigned to an individual or entity, to store e-documents and/or links to e-documents in repositories.
    d. Issuer – Any public or private sector entity/organization/department issuing digitally signed e-documents to individuals/entities and making them available within a repository for access through a digital locker of their choice.
    e. Requester – An entity/organization/department requesting secure access with user consent to specific e-documents stored across the ecosystem to provide paperless service to end users.

2. Characteristics of Electronic Documents

    To meet the key goals and the solution objectives, architecture should ensure that all electronic documents stored in digital repositories are:

    a. Machine Readable – documents in electronic format should ideally be machine readable (XML, JSON, etc.) instead of formats like PDF eliminating human workflow within the requester system.
    b. Printable – all e-documents should have a printable format attached to it allowing continued printing of certificates for individuals and for backward compatibility with existing paper-based systems.

c. Shareable – users can easily share the documents with other agencies just by providing the unique document URI without having to share photocopies.
d. Verifiable – most importantly, all documents and certificates issued by an issuer can be verified by validating the digital signature of the issuer, thus, eliminating the need for physical verification of the document. In addition, Aadhaar attached documents/certificates ensure only the owner Aadhaar holder can indeed use the certificate, thus eliminating misuse of someone else's certificates.
e. Secure – it is critical that documents in the repositories are secure in terms of storage and access. In addition, specific documents (based on type of document) may only be shareable via owner authentication to ensure sharing and access is authorized by the document owner.

Proposed Architecture

This section covers solution architecture in detail including terminology used, high level architecture diagram, document identification scheme, document issuance lifecycle, document sharing scheme, and some examples.

In the diagram below, the top side represents the issuance part and bottom side represents the real-time access part. Diagram depicts the federated model of document storage via designated dedicated digital repositories. Individuals can sign up for their preferred Digital Locker and use that to obtain consolidated view and also share documents with requesters using electronic consent.

Core Features

a. Multiple electronic document repositories (either issuer's own or 2nd party under the contract with issuers) complying to DLTS specifications allowing rapid digitalization at the issuer level.
b. Storage and access using unique document URIs and by Aadhaar numbers or similar strongly verifiable identity (access using a document URI points to one e-document while access via a verifiable identity(ies) can point to multiple e-documents issued to him/her).
    i. All access via auditable and non-repudiable mechanisms.
    ii. All access within the ecosystem is with user consent. Note that issuers may directly expose documents that are public in nature (e.g., land registration or voter card) independent of the digital locker scheme.

iii. Access via an Aadhaar number or similar universal identity must always be with user authentication to ensure access is authorized by that user (Identity holder).

c. Issuers can also choose to digitize older documents without having a machine-readable representation and allow verifiable and secure access to older (legacy) documents. They can focus on new e-documents in machine readable format while progressively providing digitization of older (existing) documents.
d. Users can also choose to convert their existing documents using a self-signed mechanism and store them in their preferred Digital Locker. Acceptance of such documents will depend on the requester rules.
e. Issuers may provide a printed copy of the document to the individual after storing them in their repository making the e-document verifiable, shareable, accessible, and re-printable.
f. Requesters can dynamically obtain the list of document types defined by issuers by querying the metadata of the repository allowing issuers to add new document types dynamically.

Security & Privacy Aspects

1. Document Security
    a. Proposed solution eliminates the need for all e-documents to be stored in one central repository to minimize the risk of security and availability.
    b. Since e-documents are mandatorily digitally signed and timestamped, NO alteration can be done for misuse.
2. Access Security
    a. Repository and Digital Locker providers must comply with DLTS security and API specifications.
    b. While some e-document types may be available to trusted requesters without electronic authentication and authorization of the owner, some document types may mandatorily require explicit electronic authentication and authorization of the document owner for every access.
    c. Access to repositories is only protected by API license keys, digital signature, secure transport, and access level audits.
    d. If explicit authentication is required for a particular document type, a trusted authentication of the owner is mandated during access.
        i. Architecture allows owner authentication via Aadhaar or other trusted 3rd party authentication schemes.

e. Mandatory audit logs must be maintained both by Digital Locker and repository providers.
f. Repository providers MUST publish anonymized access logs in public for transparency as well as notification subscriptions by the document owners.

API Specifications

A detailed set of API and compliance specifications have been prepared. These API's cover all functions of a service provider within the Digital Locker ecosystem. These include:

1. PushURI: Allow Issuers having strongly verifiable identity (e.g., Aadhaar) seeded documents to push URI's of these documents directly into the Digital Locker of the issuer or account of the User.
2. PullDoc: Allows Users to pull a document from the Issuer repository into the Digital Locker by providing a URI or pull a URI of a document by searching for his/her own document from the repository of the Issuer.
3. FindURI: Allows the user to get all the URIs from various Digital Lockers that are attached to the user's universal Identities such as Aadhaar.
4. FetchDoc: Allows a Requestor to fetch a document for a given URI after having received the user consent.
5. GetLockerToken: and the schema definition of the Consent Token – Electronic consent artifact created and audited as per MeitY's Electronic Consent framework.

The following Meta APIs facilitates seamless integration between ecosystem partner applications:

1. getIssuers: Allows ecosystem partners to fetch all the Issuers registered with the regulator to provide Digital Locker services.
2. getLockers: Allows ecosystem partners to fetch all the Locker Providers registered with the regulator.
3. getDocumentTypes: Allows ecosystem partners to fetch all the applicable Document Types supported by the systems. For e.g, document types are represented by unique alpha based DocumentTypeId of maximum length 5 along with a short description of the document - "Birth Certificate", "Marriage Certificate", "Employment Certificate" etc.,
4. getDocumentLookupAttributes: Each Issuer shall map the documents with unique user attributes for retrieval. For e.g., CBSE maps the documents using Name, Roll Number and Year. This API enables Digital Locker providers to

easily identify the lookup parameters and to pull the documents from Issuer's repository. With the saturation of Aadhaar seeding across issuers repository, Aadhaar may eventually become one such uniquely identifiable parameter.

B6.7 Anonymisation

ISO/IEC 29100:2011 provides a privacy framework which

1. specifies a common privacy terminology.
2. defines the actors and their roles in processing personally identifiable information (PII).
3. describes privacy safeguarding considerations; and
4. provides references to known privacy principles for information technology.

ISO/IEC 29100:2011 is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.

The ISO 29100 privacy framework does not include formal requirements that a company must follow, but it does provide bullet points under each of its proposed principles that discuss what it means to adhere to the principle and many organizations refer to those bullet points as proposed controls. In total, the original version of the ISO 29100 framework proposed approximately 70 controls that fall under (or can be considered subcategories of) the following 11 principles:

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention, and disclosure limitation
6. Accuracy and quality
7. Openness, transparency, and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

B6.8 Special Protection of Children's Personal Data

These guidelines are mainly addressed to the protection of personal's data of children involved in the education system, by providing investigators the knowledge and the

means that are fundamental to guarantee the protection of student/children's personal data and the respect of their privacy.

1. Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.
2. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.
3. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

A minimum standard of security would include the following:

1. Access to central IT servers to be restricted in a secure location to a limited number of staff with appropriate procedures for the accompaniment of any non-authorized staff.
2. Access to any personal data within an organization to be restricted to authorized staff on a 'need-to-know' basis in accordance with a defined policy.
3. Access to computer systems should be password protected with other factors of authentication as appropriate to the sensitivity of the information.
4. Definition of computer protection and of manual files to be kept hidden.
5. Back-up procedure in operation for computer held data, including off-site back-up.
6. All reasonable measures to be taken to ensure that staff are made aware of the organization's security measures and comply with them.
7. All waste papers, printouts, etc. have to be disposed carefully.
8. A designated person should be responsible for security and for periodic reviews of the measures and practices in place.

B7. Standards for Software Design and Development

Software design and development standards shall ensure that software's architecture and design is compliant with common minimum practices and shall enable it to grow as a quality product. Standards will ascertain that software is standardized, compatible and interoperable with other systems. The following are recommended standards:

#	Purpose	Applicable Standards
1	Digital Service Standard	Digital Service Standard, MeitY
2	Open Data Sharing	The Open Government Data (OGD) (https://data.gov.in)
3	Framework for Adoption of Open-Source Software in e-Governance Systems	MeitY Guidelines
4	Quality Management, Assurance and Metrics	ISO/IEC 19796-3:2009 ISO/IEC 40180:2017
5	Mobile Governance	Framework for Mobile Governance, MeitY
6	Telemetry	https://dev.DIKSHA.gov.in/#/document/open-standard-specification
7	Guidelines for Indian Government Websites	https://web.guidelines.gov.in/
8	Web Standards for Accessibility (Web and Mobile)	World Wide Web Consortium (W3C) (https://www.w3.org/)
9	Guidelines for the development of e-Governance Applications	GudApps (https://guidelines.gov.in/gudapps/about.html)
10	Open API	MeitY Guidelines

#	Purpose	Applicable Standards
11	Localisation and Language Support	MeitY Guidelines
12	Geo Spatial Data Product Standardization	ISO 19115, FGDC Content Standard for Digital Geospatial Metadata (CSDGM)

Table 14: Software Design Standards

B7.1 Digital Service Standard

An emerging need has been realized by the Governments to review, rationalize, and enhance the existing e-Services, besides creating a new breed of digital services with a high 'speed-to-market'. The digital services are qualitatively different from the e-Services not only in terms of the new-age design paradigm but also in their goal to create new value at the frontiers, supported by a whole set of new processes. The digital service regime calls for entirely new capabilities both in the service provider community and the consumer community.

The Digital Service Standard is a set of over 170 National and International standards, principles and guidelines organized according to a rational taxonomy, which are easy to comprehend and implement by the Government eco-system. The Vision of the Digital Service Standard is to define a National Standard, the adoption of which ensures Uniformity, Consistency, Comprehensiveness and Excellence in the Definition, Realization, Measurement and Governance of Digital Services.

The Digital Service Standard framework can be applied with benefit to a variety of situations like large green-field digital projects, legacy systems that need to migrate to the digital era, discrete services, and portfolio of services. Digital Service Standard not only provides the principles and guidelines required to be followed, but also provides a framework to measure the performance of digital services; to assess their impact and provides a set of strategies to overcome the challenges which may arise in adoption of this standard.

The vision to graduate to Government 4.0 on the lines of Industry 4.0 would require seamless transition and uptake of the Digital Service Standards by the Central, State and Local Governments. DSS strategies seek to unlock the systemic challenges, overcome the systemic inertia to change and bring about agility in the ecosystem.

Objective:

- Establishment of institutional mechanisms at Central/State levels
- Provide for periodic enhancements to DSS
- Create frameworks for audit and certification of organization
- Facilitate the adoption of DSS

Taxonomy of DSS

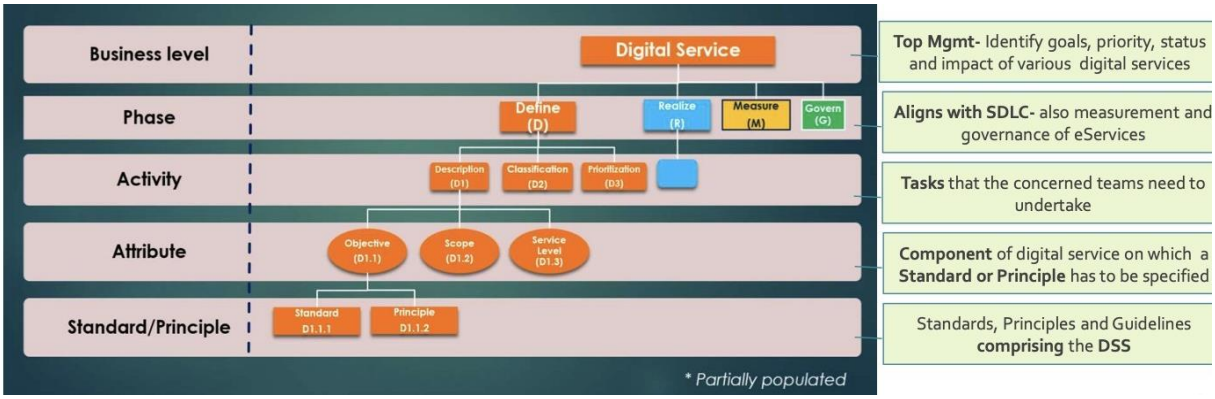


Figure 33: DSS Taxonomy

DSS Certification

DSS Level 1: Must be compliant with the following:

D1.1.2Transparency
D1.3.1 Quantitative Service Levels/KPIs
D2.1.1 Taxonomy of Digital Services
D2.1.2 Service Metadata
R1.1.1 User Needs Analysis
R1.1.2 Process Re-engineering
R1.2.1 User Experience
R1.2.2 User Interface
R1.3.2 Compliance to Standards
R1.3.3 Security & Privacy
R2.1.2 Local Language Interface
R2.1.3 Documentation
R.2.2.1 Change Control

DSS Level 2: Must be compliant with following, in addition to the requirements of Level 1:

M1.1.1 Quality / Outcome KPIs

M1.1.3 Analysis & Dashboards for measurement of Quantity/ Output KPIs
M1.3.1 Cost-effectiveness of the Service
G1.1.1: Institutional Mechanisms
G2.1.1 Change Management
G2.3.1 Capacity Building

DSS Audit

- Establish a process for empanelment of professional companies to undertake audit of digital services projects for compliance with DSS.
- Establish and notify the formats and templates for the DSS audit.
- Audited for adherence to
    - Regulatory requirements applicable to the digital service
    - ISO 9241-171:2008: Ergonomics of human-system interaction: Guidance on software accessibility Data Standards published by MeitY (http://egovstandards.gov.in)
    - Data Privacy & Security
    - Service Level Agreements
    - Infrastructure
    - Security Policy Guidelines
    - Testing
    - Documentation

Institutional mechanism for Governing DSS

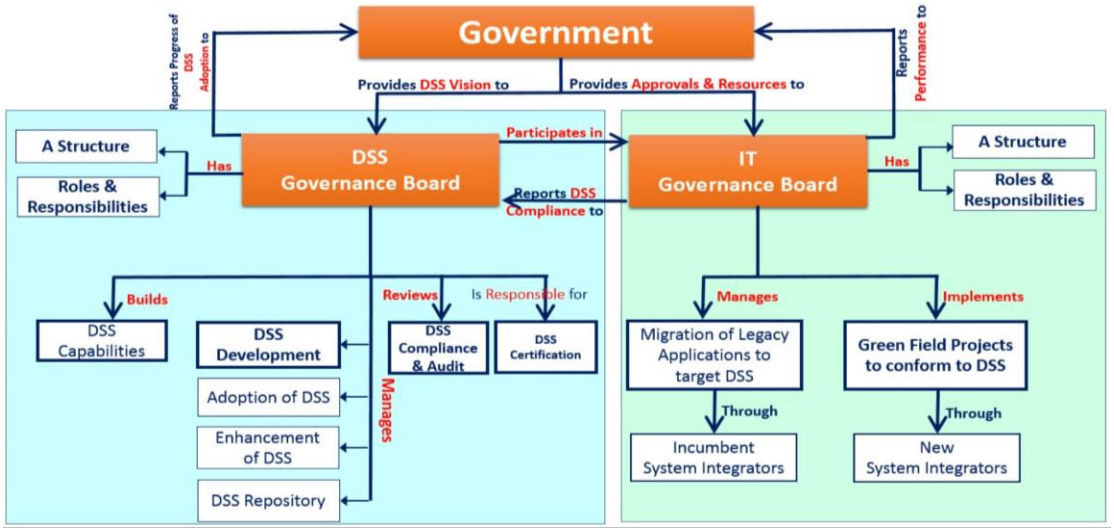


Figure 34: Institutional mechanism for Governing DSS

B7.2 Open Data Sharing

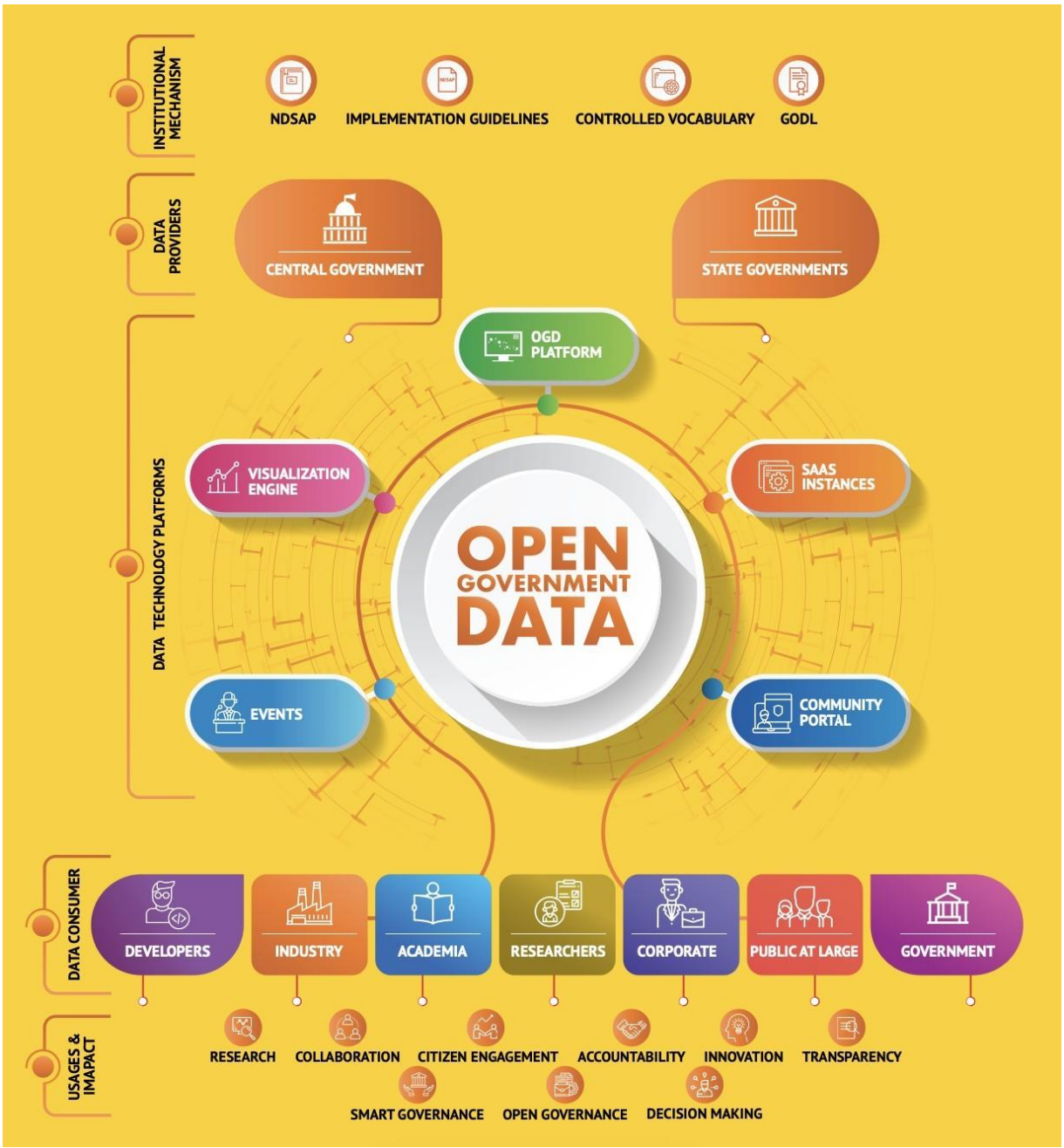
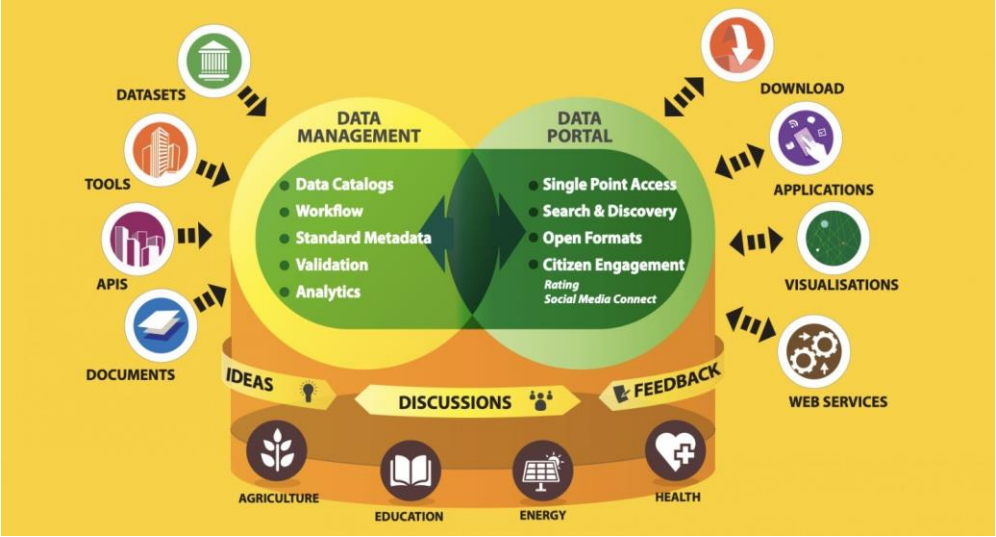


Figure 35: Open Government Data Platform

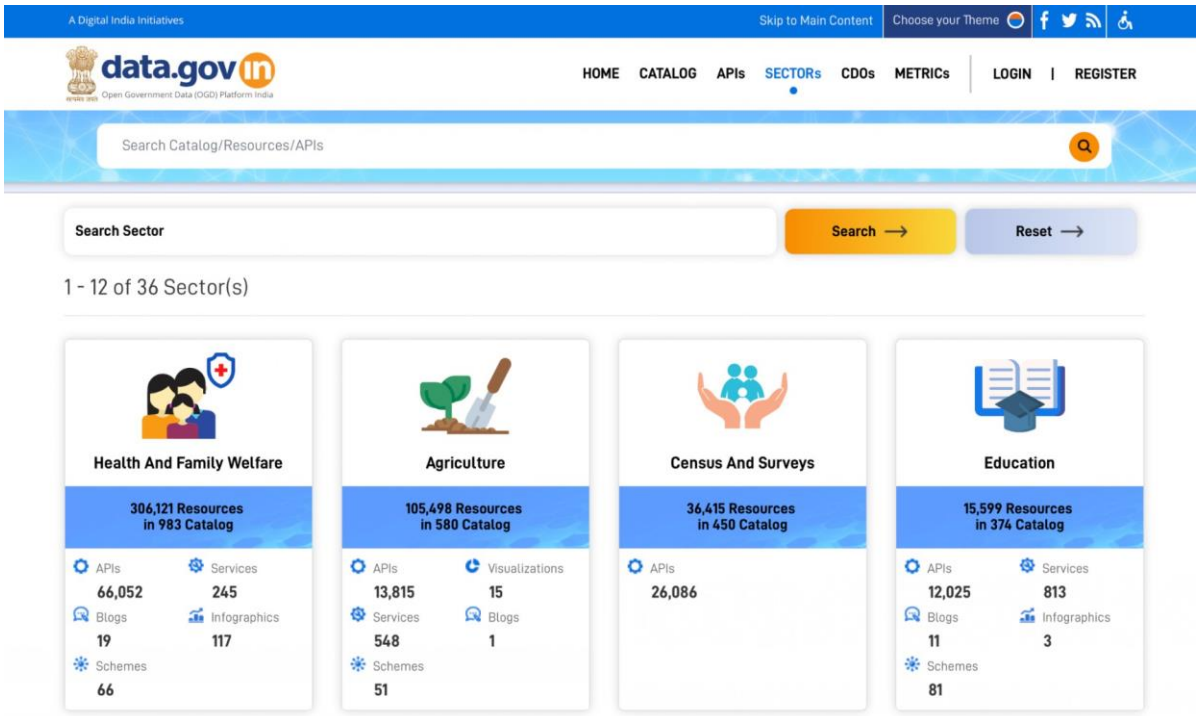
The Open Government Data (OGD) Platform India (https://data.gov.in) has been set-up by the National Informatics Centre (NIC) in compliance with the Open Data Policy (NDSAP) of India. The objective of the policy is to provide proactive access to Government owned shareable data along with its usage information in open/machine readable format, through a wide area of network across the country, in a periodically updated manner, within the framework of various related policies, rules, and acts of the Government. Developed using Open-Source Stack, the project is one of the



initiatives under Pillar 6 (Information for All) of the Digital India initiative.

It facilitates community participation for further development of the product with Visualizations, APIs, Alerts, etc. It has an easy to use and user-friendly interface with dynamic/pull down menus, search based reports, secured web access, bulletin board, based on Dublin Core metadata standards and parametric & dynamic reports in exportable format. The platform reflects how innovative use of information technology has led to a paradigm shift in accommodating the huge data potential of the country.

The Platform has a rich mechanism for citizen engagement, which could help Ministries/Departments/Organizations prioritize the release of Government Datasets.



Besides, enabling citizens to express their need for specific datasets or apps, it also allows them to rate the quality of datasets, seek clarification or information from nodal officers of participating government entities.

The Platform also acts as a knowledge-sharing platform through online communities. Citizens with specific interests are encouraged to contribute blogs and join online forums around various datasets or their domain of interest.

Platform demonstrated its potential to the App Developers' Community through various contests such as 'OGD National Hackathon', Sector specific CDO Workshops', '12th Plan Hackathon', 'In Pursuit of an Idea', 'CMA Hackathon', etc. Out of which '#OpenDataApps Challenge' was launched in association with NASSCOM and 'Code for Honor 2014' was launched with Microsoft.

One of the major parameters for making the Open Data initiative and NDSAP policy a success is to engage with the larger population. Community engagement encourages citizen participation with Open Government Data. A separate Community Portal (http://community.data.gov.in) has been launched to provide a common platform for knowledge sharing through discussion and to contribute through Blogs, Infographics, Visualizations, etc. using data available on the platform. Similarly, a dedicated event portal (https://event.data.gov.in) has also helps in management of workshops,

Figure 36: egov platforms

hackathons, challenges, etc.

B7.3 Framework for Adoption of Open-Source Software in e-Governance Systems

Government of India (GoI) has been implementing the Digital India programme as an umbrella programme to prepare India for a knowledge-based transformation into a digitally empowered society and a knowledge economy. Under the overarching vision of Digital India, GoI aims to make Government services digitally accessible to citizens in their localities and to ensure efficiency, transparency, and reliability of such

services at affordable costs. To meet this objective, there was a need felt to set up a commensurate hardware and software infrastructure, which would have required significant resources. Adoption of Open-Source Software (OSS) has increased worldwide and has led to innovations in implementation of ICT solutions across businesses and Governments. The use of OSS in the key domains of ICT implementation (like application development, internet connectivity, infrastructure, Data Centre and mobile) has helped widespread adoption of open-source technologies across the world. The OSS solutions have matured to a large extent and millions of committed developers are participating in making it conducive to the needs of different areas of ICT implementation. These solutions are now available with the required support services. The increased convergence of computing platforms facilitates the use of OSS together with Open Standards and adoption of web browser as a unified platform for software applications. The socio economic and strategic benefits offered by the adoption of OSS in -Governance have encouraged several Governments and public agencies, to bring out policy framework / guidelines in this area. Compliance to Open Standards brings the twin benefits of interoperability and easy migration to OSS. The Government of India has been promoting the use of open-source technologies and has been keenly encouraging their adoption in the -Governance movement of the country. Department of Electronics and Information Technology (DeitY), Government of India has formulated the "Policy on Adoption of Open-Source Software for Government of India" to enable effective adoption of OSS and encourage the formal adoption and use of Open-Source Software (OSS) in Government Organizations. The policy has been approved and notified. In pursuant to this policy, the department is required to publish a policy framework for rapid and effective adoption of OSS covering the prioritization of the application areas and illustrative list of OSS and OSS stack etc. required for various functional areas. This "Framework for Adoption of Open-Source Software" has been formulated to promote adoption of OSS in e-Governance Systems in India. It lays down a set of recommendations and procedures for promoting, managing, and enhancing the adoption of OSS.

The key objectives of the Framework are to:

(a) Provide guidance to the Govt. departments and agencies in selecting OSS Solutions

(b) Identify the OSS Stack appropriate to the needs of various government departments and agencies.

(c) Enhance & sustain the ecosystem to provide multi-layer support services on OSS for various National & State projects.

(d) Create knowledge-base and build capacity on OSS.

(e) Provisioning the Institutional Mechanism and resources required for promoting OSS on an ongoing basis.

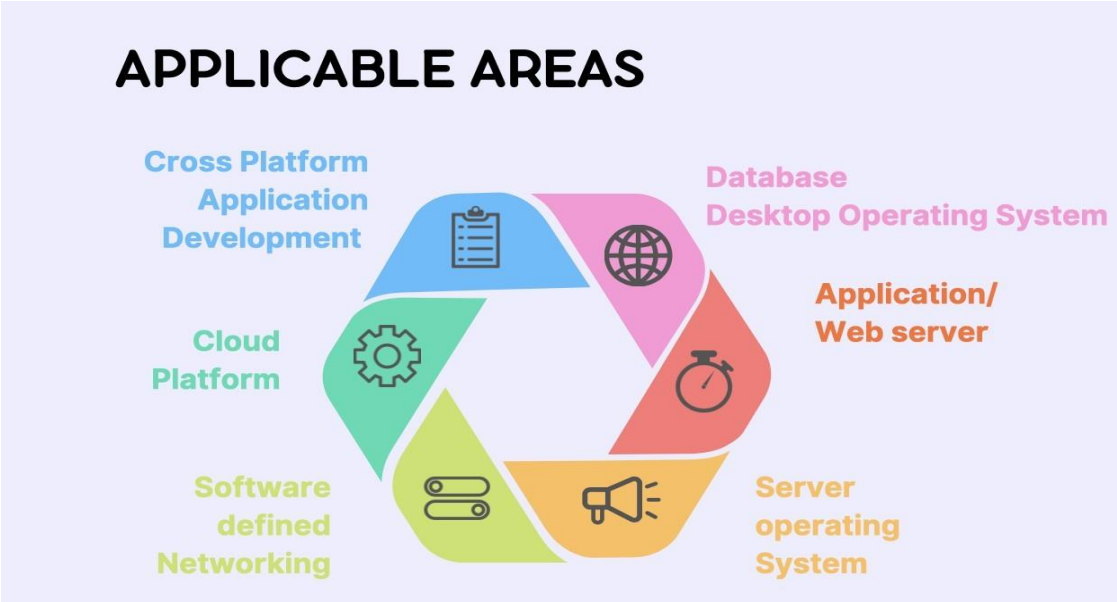


Figure 37: Applicable areas of adoption

Impact of OSS in ICT and non-ICT Domains

OSS framework has a wider perspective than a software development methodology. It not only increases access, ownership, and control of ICT, but also provides a Framework for usage and sharing of intellectual capital. The sharing of knowledge spreads, not only through OSS, but also through other related areas like Open Standards, Open Hardware and Product Designs, Open Process, Open ware Course, etc. This is collectively known as Open Technology (OT). In addition to ICT fields, the tradition of sharing of knowledge spreads in many other sectors as Open Medicine, Open Knowledge base, Open Law, Open Science, Open Music, Open Agriculture, etc.

Interoperability & Open Standards

Open standards play an important role in fostering healthy competition, enhancing the interoperability among e-Governance Systems and better communication among all stakeholders. Open standards are defined by each country or public agency. The

Government of India had also brought out “Policy on Open Standards for e-Governance” to enhance the standardization activities in India.

a) OSS and Open Standard

"Open Standard", in general, refers to a technical specification as a result of consensus during formulation and ratification stages.

OSS refers to the implementation of technical specification by a community using Open-Source licensing and collaborative contributing model; The licensing and contributing model may vary from one community to another.

Though OSS and Open Standard concepts are similar in terms of availability of specification, cooperative development-model but still there are some differences.

b) Significance of Open Standards on OSS

Migration from CSS to OSS and vice-versa is made easier by Open Standard. Mandating Open Standards has a complementary effect on OSS systems, introduces increased competition and facilitates better compatibility between CSS & OSS. The availability of an OSS reference implementation would spur quicker adoption and acceptance of the standards as the implementation of the standard is available for reuse. Examples include HTML5, JavaScript, etc.

Summary of Recommendations for Adoption of OSS Framework

This section summaries the recommendations for the adoption of OSS.

Recommendations for Implementing Agencies for OSS Framework

(a) Preference should be given to select OSS libraries which have liberal and less restrictive license models.

(b) Selecting appropriate OSS stack for development of applications and infrastructure is crucial for performance and sustained support.

(c) Establish Multi-Level Support Services on the adoption of OSS.

(d) Provisioning of application development, staging and deployment environments for the reuse of Open-Source Stacks with support services:

(e) Offer services for preferred areas and provide support.

(f) Continue R&D efforts in OSS in identified thrust areas.

(g) National repositories/ knowledge banks should be created for OSS solutions, technologies, and applications.

(h) Development of two toolkits (one toolkit for rating OSS against another OSS and another toolkit for rating OSS against CSS) should be brought out.

(i) Develop a mechanism/tool to rate the OSS based application based on the criticality of the application.

(j) Transferability of ICT Assets (which facilitate the reuse) within all levels of Government and public agencies without additional expenses should be considered while procuring them.

(k) The distribution of the modified source code and executable of the OSS across various units of the single Government entity should be considered as internal distribution.

(l) Use of OSS in Government Departments along with skill development programs should be encouraged.

(m) The security of OSS solutions under OSS Stacks should be enhanced by creating a two layered internal & external audit mechanism and retrofitting mechanism under the proposed structure.

(n) OSS application development with Indian languages interface should be encouraged.

(o) Simpler & easier Software Development with GUI, Meta-Language and Templates should be

provided, as a RAD environment, to achieve faster adoption of OSS to meet the quick delivery schedule.

(p) The guideline on influencing factors for the adoption of OSS should be brought out by customizing for Indian Scenario.

(q) Enforcement guidelines on Open Standards Policy of Government of India should be brought out to accelerate the adoption of OSS.

(r) The model used by some Indian Institutes may be considered for creating training and learning materials using the community approach.

(s) Development of a community engagement model to encourage internal developers to participate in the open-source community under the appropriate policies and engage with external developers

Recommendation for -Governance Project Implementation Teams

(a) Since many social, economic, and strategic benefits are provided by the adoption of OSS, the OSS options should be considered seriously by the e-Gov planners, architects, and developers.

(b) This Framework should be used to expedite the adoption of OSS in e-Governance in India.

(c) Focus on Preferred areas for adoption.

(d) Since many socio, economic and strategic benefits are provided by the adoption of OSS, OSS should be considered as a preferred option.

(e) Preference should be given to "Pure Open-Source Model" for availing the support service on OSS.

(f) Government Agencies and Departments should seek to avoid vendor lock-in to proprietary IT products and services. RFP (Request for Proposal) documents should avoid using vendor specific product/brand names.

(g) Applications developed by the Government of India should be cross platform and not be locked into a specific platform.

(h) For Government funded software research and developments in India, scientists/ researchers should be encouraged to publish their innovations under Open Source and Open Document licenses, except for security reasons.

(i) Large Projects should be split into smaller Projects for development by different parties/vendors/SMEs and integrated & implemented by the project teams. This will reduce the number of resources required for the smaller project, encourage SMEs participation, reduce the risks in ICT projects and facilitate the adoption of OSS.

(j) Open Web Technology should be preferred to develop once and run the same on all devices. Device Specific Development (Desktop, Tablet, Mobile, etc.) should be discouraged.

(k) Code contribution to the OSS community should be encouraged.

Recommendations related to RFP/Procurement

(a) OSS Solutions should be considered as a preferred option in IT procurements by Government of India. In cases where the merits of OSS and CSS are comparable, contracts could be awarded to OSS solutions in recognition of issues like value for money as well as enhanced strategic control,

security, reuse, cost saving, knowledge society creation, adherence to Open Standards etc. which are hard to quantify.

(b) Vendors must provide justification for exclusion of OSS in their responses to RFPs (Request for Proposals).

(c) Hardware and peripherals procured by Government Agencies and Departments should have support for Open-Source device drivers for ensuring interoperability of systems.

B7.4 Quality Management, Assurance and Metrics

http://egovstandards.gov.in/sites/default/files/QualityAssuranceFramework%20Ver.1.0.pdf

In recent years, governments across the world have been investing considerable resources in applying ICT tools to transform the way in which public services to citizens and enterprises are delivered. This wave has been popularly known as eGovernance.

While transformational in nature, eGovernance projects tend to be complex and costly. Variations in capacity and knowledge within government make these projects highly risky and prone to poor implementation outcomes. Poorly implemented or failed eGovernance initiatives subsequently make it more difficult in future to justify financing for such systems and hamper stakeholder 'buy-in'.

These errors, vulnerabilities and risk therefore need to be managed over the project lifecycle within acceptable parameters. This can be done by putting into place quality assurance mechanisms at relevant stages of a typical eGovernance project life cycle.

Moreover, the Government of India has initiated implementation of the National eGovernance Plan (NeGP) where all eGovernance projects in the country are expected to comply with values and objectives defined in its vision[1]. To translate these values into operational terms, there was a need to evolve a methodology to ensure that eGovernance systems adequately reflect user-centric quality characteristics. For this purpose, a Quality Assurance Framework (QAF) was developed by MeitY.

The principle objective of QAF are:

1. Ensuring system requirements in terms of product processes & services are defined (Definition).
2. Ensuring the system conforms to requirements (Verification)
3. Ensuring user satisfaction with the system, once it goes 'live', (Validation)

The three objectives of quality assurance in an eGovernance project life cycle can be achieved through the identification and application of Quality Gates (QG) at various phases of the project.

Each QG consists of a set of quality baselines relevant to that project phase and is aligned with relevant IS/ ISO standards. QGs can be further divided into two categories: essential and desirable with each project mandatorily required to clear the essential QG regardless of scope or duration.

The essential QGs relate to four key areas:

- Quality Processes in the Organization (Gate 1)
- Software Quality (Gate 2)
- Information Security (Gate 3)
- IT Service Quality (Gate 4)
- Desirable QGs relate to such aspects as project documentation, use of recognised standards and architectures, risk management, business continuity planning etc. Desirable QGs can be incorporated into project planning based on complexity, risk, and resource availability.
  The purpose of the e-governance Quality Assurance Framework is to provide assurance that work products (solutions) and Processes comply with predefined provisions and plans. As a result of successful implementation of this Framework the following will be the expected outputs
    - i) A strategy for conducting quality assurance is developed (through RFP).
    - ii) Evidence of quality assurance is produced and maintained.
    - iii) Problems and/or non-conformance with requirements are identified and recorded.
    - iv) Adherence of products, processes and activities to the applicable standards, procedures and Requirements are verified and
    - v) User satisfaction is measured.
- These are achieved by performing the following activities:
    - i) Process Design & Implementation (Processes for government, project, vendor & user)
    - ii) Product Assurance (Software Application, Hardware & networking components), Process Assurance (Risk management, Asset management, Disaster Recovery ...) and Assurance of management systems (ISMS, ITSM, QMS....) and
    - iii) Measurement of user satisfaction

The Quality assurance framework (QAF) for e-governance is designed to address the requirements of quality assurance namely Definitions, verification & Validation. It is modular in nature to facilitate easy navigation & readability to the user. The structure for Navigation is as follows:

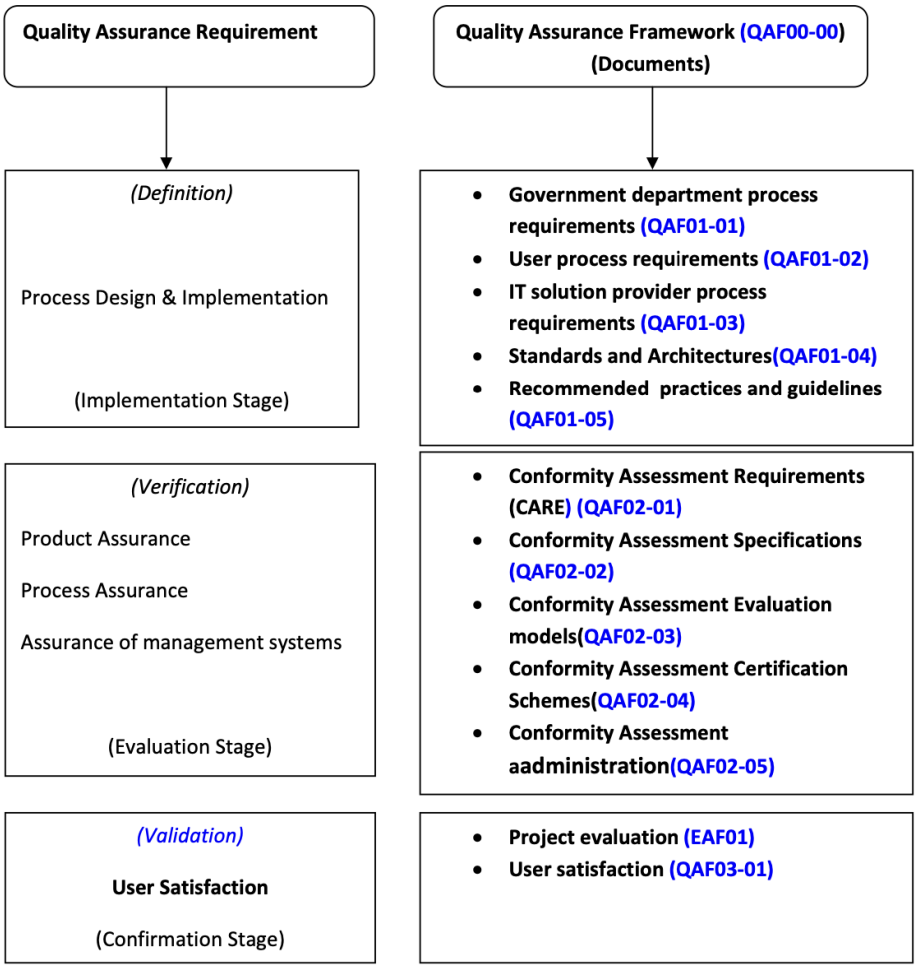


Figure 38: Quality Assurance Framework

The Quality Assurance Framework (QAF) enhances the eGovernance framework conditions in India to support the National eGovernance Plan's vision of providing reliable, cost-effective, and transparent citizen services by applying international good practices and guidelines.

The QAF focuses on three elements of quality:

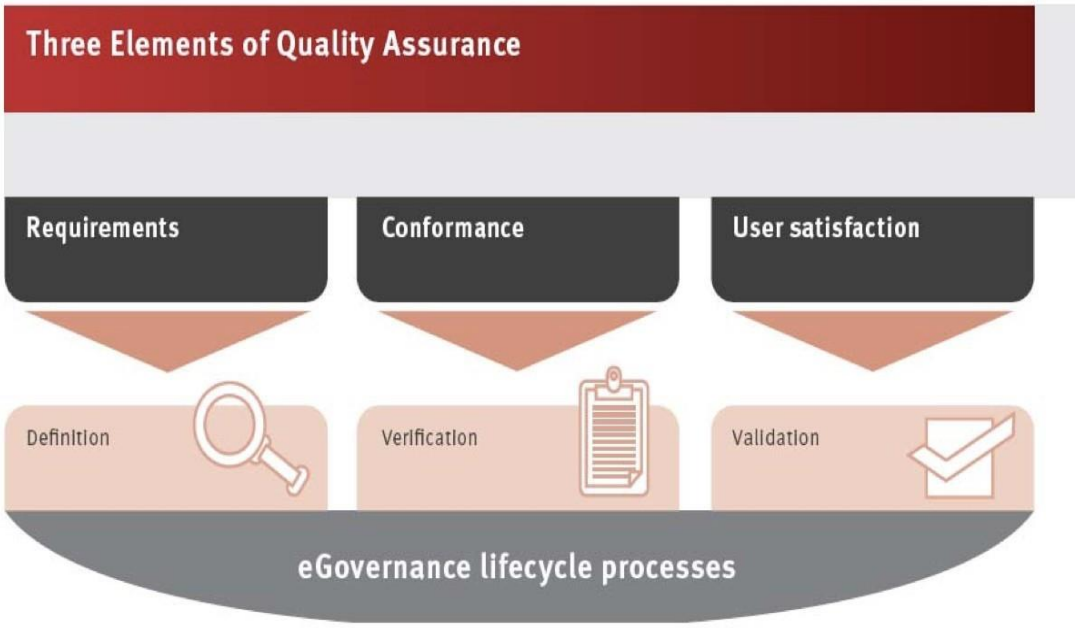


Figure 39: Quality Assessment Framework

1. u
   irements of Processes (For role-based processes i.e., the government agencies, system integrators or solution providers and the users of the eGovernance solution) through its implementation.
2. Conformance (i.e., verification that the ICT solution complies with requirements) through evaluation process.
3. 3. Satisfaction (i.e., validation from users that the system is responding completely and accurately to their requirements) through confirmation.

These three elements cover the interactions between the user, the government, and the solution provider. Through role-based processes, the requirements of the users and government are documented and passed on to the solution provider who is selected through competitive procurement. Once the solution provider has started developing the system, it is the government who must verify that the system is being developed according to

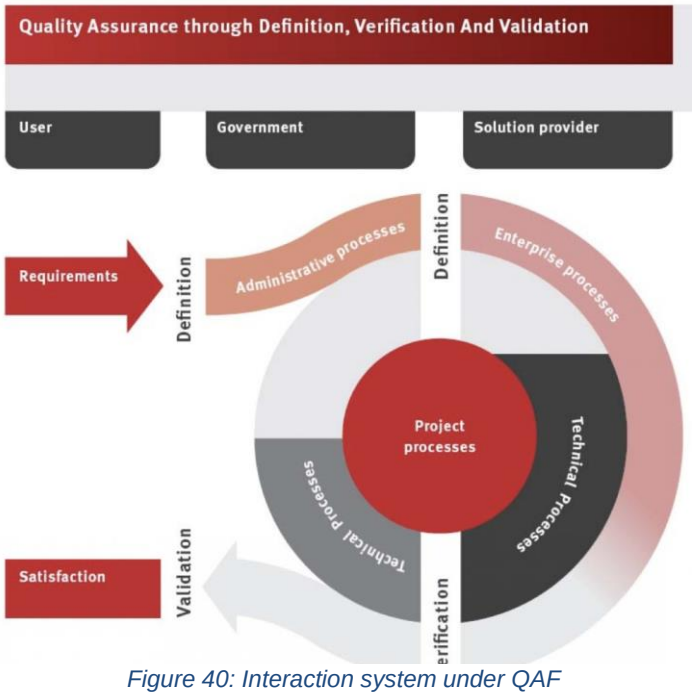


Figure 40: Interaction system under QAF

the requirements defined earlier. Once the system goes 'live', an assessment of the user experience across various user groups, internal and external, is used to validate if the developed system has been able to meet the original requirements and ensure user satisfaction.

Implementation Stage:

The implementation approach refers to the identification and reengineering of processes in the government organization, implementing an eGovernance project. In e-governance system life cycle all the three players (Govt, User & implementing agency) should execute a set of processes. The govt. organization requires implementing these processes (QAF0101) in following groups:

1. e-governance project enablement
2. Acquisition of IT system & outsourcing
3. e-governance project management
4. Technical processes
5. Supply of services to citizens, businesses etc.

The implementing agency /IT solution provider (QAF01-03) in a similar way shall also implement the following processes:

1. Enterprises processes for project enablement
2. Acquisition
3. project management
4. Technical processes
5. Supply of IT services to government

The objective of the implementation approach is to ensure that by implementing a defined process the probability of success of achieving outputs gets enhanced. Each process group consists of a number of processes and each process may be invoked, as required, at any time throughout the life cycle and there is no definitive order in their use. Any process may be executed concurrently with any other life cycle process. Any process may apply at any level in the hierarchical representation of a systems structure. This

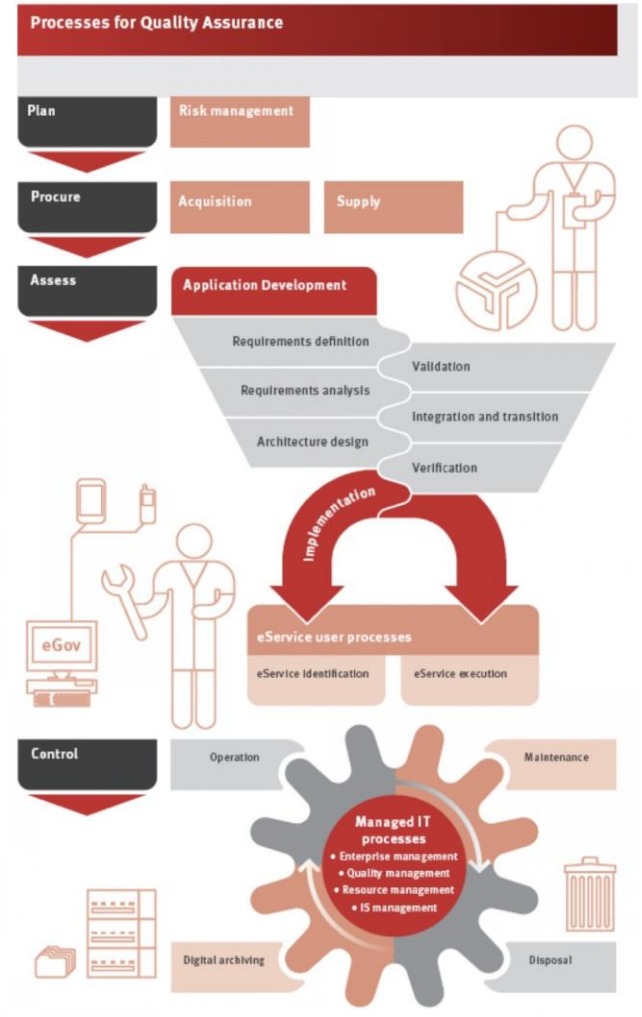


Figure 41: Process for Quality Assurance

continuous interaction between processes is represented by the above figure.

Evaluation Stage

The evaluation approach identifies and applies Quality Gates to assess the quality of the eGovernance system at various stages of the life cycle (QAF0201). The overall objective is to ensure that the eGovernance system responds completely and correctly to the requirement specifications. More importantly, Quality Gates can be used to assess whether (i) the requirements themselves were framed correctly, (ii) which areas need further action to drive the system towards complete conformity with requirements and (iii) which exogenous variables have or are likely to impact the system which cannot be accounted for while defining requirements.

Section 2.3 outlines essential and desirable Quality Gates. The essential QGs relate to quality organizational processes for project design and implementation, software quality, information security and IT service management.

Successful application of QG to each project ensures that quality benchmarks are defined and met consistently, and the overall project outcome reflects a true transition from manual governance systems to a quality eGovernance system

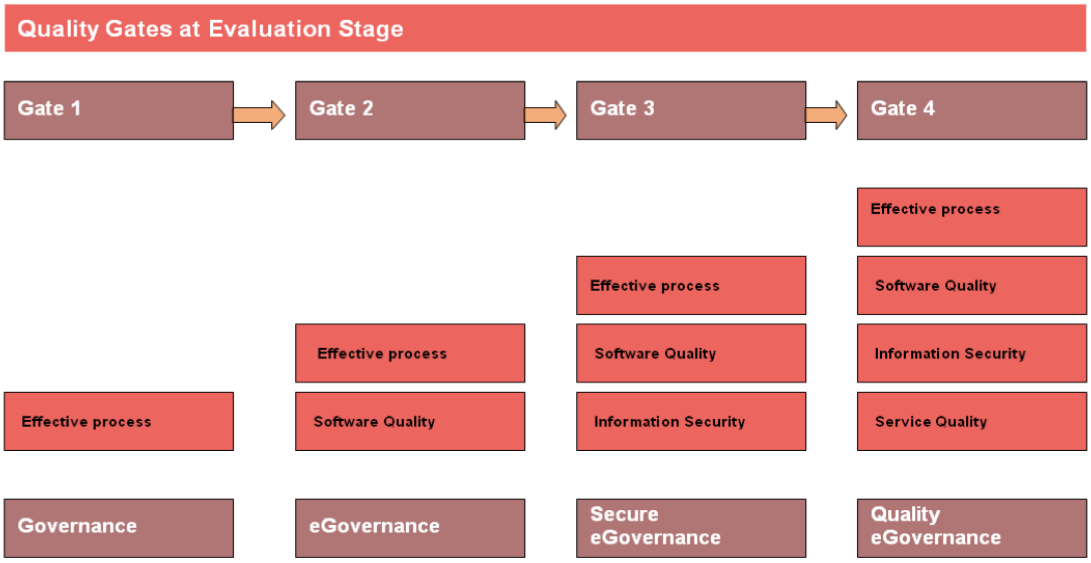


Figure 42: Quality Gates at Evaluation Stage

Confirmation Stage

The first two stages ensure that the requirements from the eGovernance system are correctly documented and verify that the system conforms to these requirements. The true utility of the eGovernance system however lies in the value added to the users of this system.

The confirmation approach to quality assurance completes the chain by validating whether the eGovernance system that has been developed through the project lifecycle is responsive to user requirements and generates confidence that the services delivered would be reliable and quality- assured.

The confirmation approach (QAF0301) sets metrics for the measurement and monitoring of various segments of users and feedback. This is used to track if the system offers functionalities that are of value to the various users and isolate issues and areas for troubleshooting or further improvement.

Figure below illustrates the various categories of users who would be relevant for validating whether the eGovernance system is generating a user experience that is satisfactory for various groups. The first category of users is policy makers and administrators who form the project board and are the owners of the implementation process. Their satisfaction will relate to the extent that the eGovernance system meets the final outputs or outcomes that were conceived at inception, including the financial and economic returns to the financial investment in the project. In other words, the satisfaction of this group would depend on the final outcomes of the eGovernance project and not so much on the inputs and the processes that have gone into the production of such outcomes.

Figure 43: eGovernance User Group Systems

The second category of users relates to other administrators and agencies that form part of the value chain of the bouquet of services delivered through an eGovernance system. This could involve government agencies and personnel at state, provincial and local levels as well as other ministries and departments where cross-cutting services are being delivered. Satisfaction of this user category would

focus mainly on variables related to data security, interoperability, data exchange and system performance.

The third category of users refers to government employees involved in the delivery of the eGovernance service(s). This would consist of relevant department personnel involved in the operations of the eGovernance system, either at the ‘back-end’ agency offices or at the ‘front-end’ staff of public access points such as Common Service Centres. From their perspective, user satisfaction would be determined by variables relating to system performance, user friendliness and impact on productivity and efficiency.

The final category of users would be the citizens and businesses at whom the eGovernance bouquet of services are targeted.

- *User expectations*: There are four key factors which affect user expectations that are important for an organization to consider in relation to service quality: ‘word of mouth’ (promises), personal needs, past experience, and external communications by the service provider. A thorough understanding of the expectations that users bring to the service experience will provide vital information to plan for either managing expectations or targeting areas of improvement.
- *Perceptions of service experience*: It is important for the service provider to understand user perceptions of the service experience in order to identify potential areas of improvement. The issue could be either a difference in perception of a service experience or a bottleneck in actual service delivery. The organization may choose to clarify points of contact by communicating with users or they may redesign their service delivery process to decrease the number of contacts required by the user in order to receive the service needed.
- *Level of importance*: The perceived importance of a service (or its elements) is an essential service variable on two levels: as an antecedent of satisfaction and for planning purposes. As an antecedent of satisfaction, the user assigns a certain level of importance to the service experience. As a user experiences service delivery, his or her perceptions of the experience are filtered by the level of importance attached to that service. Frequency of use is also considered to be a factor that influences the level of importance.

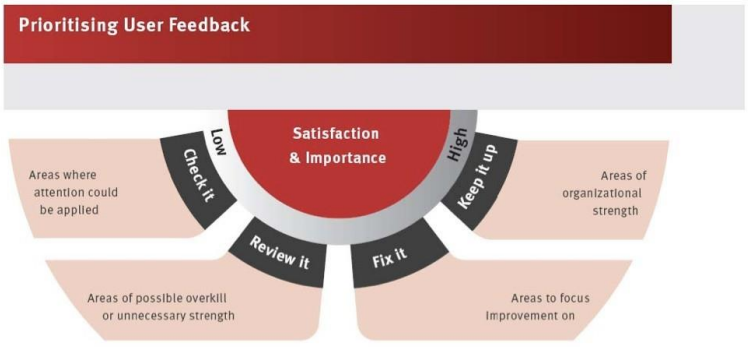


Figure 44: User Feedback flow

- *Level of satisfaction*: Users react to a combination of their expectations - the importance of the service to them and the actual service experience, resulting in an internalized response or perception. Monitoring satisfaction levels can help the project

management to take corrective actions as required or improve on an existing system functionality based on additional feedback.

- *Priorities for improvement*: Information on how important the overall service and individual service items are to users promote well-informed planning decisions. Cross-analysis of satisfaction and importance variables will identify priorities for improvements and thus promote efficient allocation of resources. Figure below provides indicative criteria to prioritize user feedback on quality perceptions and criticality.
- Above Figure provides an indicative approach to classifying and prioritizing user feedback from various groups on eGovernance systems. Implicit in all quadrants is the obvious consideration of cost while deciding the sequence of responses addressing feedback. An important quadrant for policy makers and administrators is the one marked as “Review It”. It checks against eGovernance solution providers in supplying more and more expensive systems which may enhance user experience but are not essential requirements for the services that are being delivered by the system. System integrators, solution providers and assorted vendors have an incentive to ‘over specify’ equipment specifications in large scale, complex eGovernance systems.

B7.5 Mobile Governance

India is rapidly advancing in the technological space. With the growing population and increasing Smartphone penetration, India is going mobile and digital. Smartphones and the internet are not just for the rich and wealthy, but more users are becoming informed by getting access to mobile internet. E-governance is trying its level best to provide e-government services to citizens. But still there is a need to reach these services to individuals at their doorstep. So, looking at the current mobile age there is a need for transforming E-governance services to M-Governance, which promise to bring the “anywhere-anytime-anybody” e-government service vision one step closer.

MIETY under the ambit of Digital India Programme, has initiated several technology-led transformations towards improving ‘Ease-of-living’ for citizens. Mobile governance i.e., providing services through mobile phones is one of the most ambitious initiatives undertaken by the department.

Figure 45: UMANG Mobile App

Umang Mobile app is the official Mobile Governance program which aggregates major government services of the Center, the States, local bodies, and important utility services to facilitate single point access anytime. UMANG supports 13 languages, requires about 30 MB space, helps in discovery of relevant services for a user and bookmarks them for frequent use. All DigiLocker documents are available on the home page and a scanner has been made available for document scanning with applications for a service. Govt. dept. Can integrate with UMANG in just weeks without hiring any agency for development & integration. Core integration of UMANG such as Aadhar, Payment Gateway, DigiLocker, Feedback system, SMS and email gateway are available to all departments. With its vast learning, UMANG is helping departments with GPR (Government Process Re-engineering) and upgradation of their individual platforms. UMANG app has reached a level of more than 3.2 crore downloads and ~2.35 crore registered users while maintaining an average play store rating of 4+ from more than 100k user feedback. On a daily basis, about 25,000-30,000 new users are registering on UMANG.

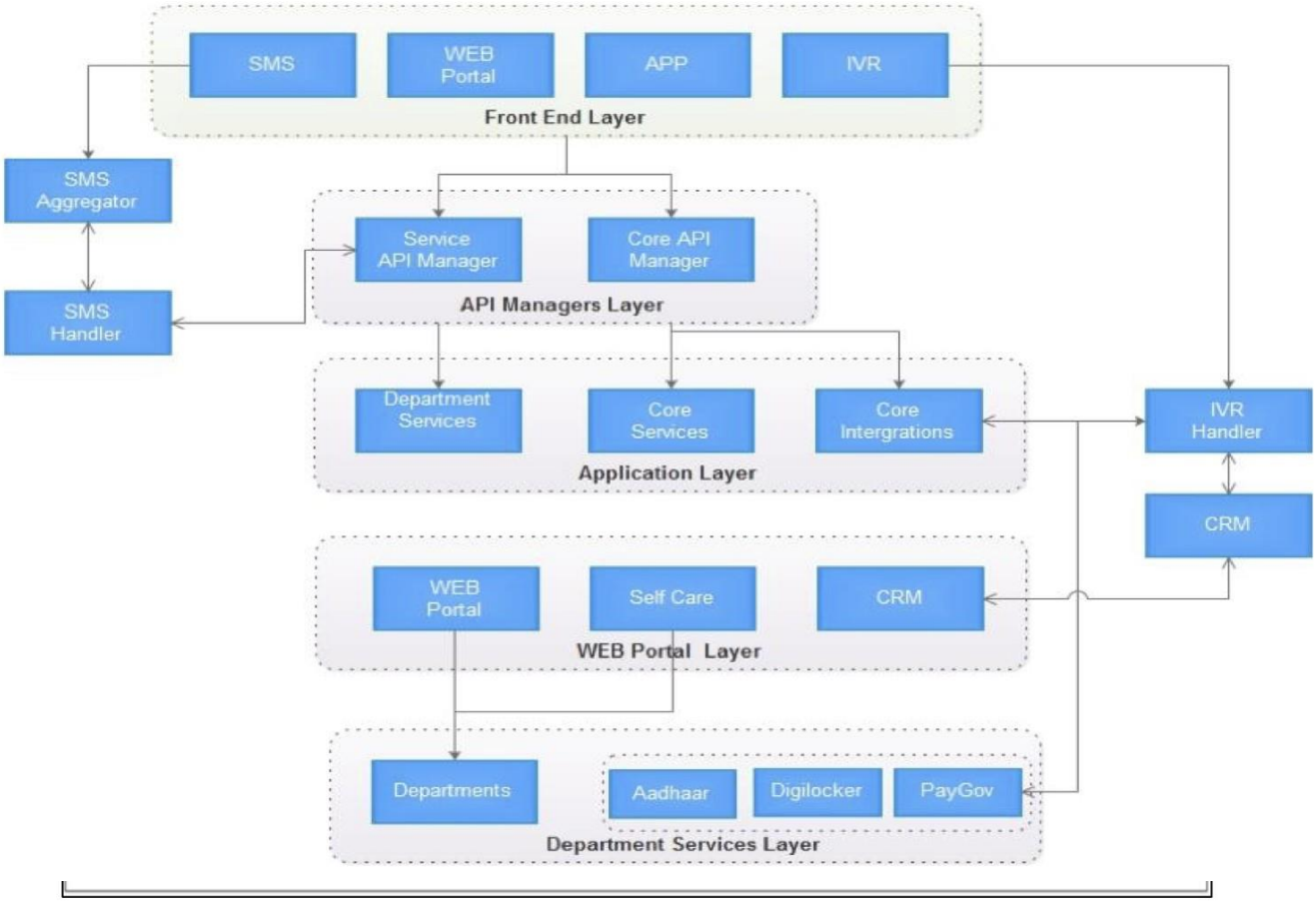


Figure 46: UMANG Architecture Flow

Some of the popular use cases by department includes-

Tribal Affairs - National Fellowship Scheme

Grants fellowship to 750 fresh ST students for pursuing M.Phil. and Ph.D. courses.

Apply for the National fellowship scheme after registration and check the status of your application on UMANG.

Augmenting Writing Skills for Articulating Research (AWSAR)

Ph.D. Scholars and Post-Doctoral Fellows in Science and Technology streams are encouraged to write at least one popular science article during the tenancy of their fellowship, and to participate in a national competition.

Use resource kits, request for webinar registration and submit stories on UMANG.

Innovation in Science Pursuit for Inspired Research - Million Minds Augmenting National Aspirations and Knowledge (INSPIRE Manak)

INSPIRE scheme of Department of Science & Technology is targeting one million original ideas rooted in science & societal applications to foster a culture of creativity and innovative thinking among school children.

Check award sanctions, school-wise awardees, authority contact details & various inspiring videos/FAQs on UMANG.

Central Board of Secondary Education (CBSE)

Locate schools, exam centers and check exam results of 10th & 12th class students every year. Also, Marksheets can be seen through digiLocker on UMANG homepage.

Biotechnology JRF (Junior Research Fellowship)

JRF provides fellowships to biotech students for research, selected through Biotechnology Eligibility Test.

Check status of your application on UMANG.

B7.6 Telemetry

Telemetry is a technology used to automatically record and measure data from real-world use and forward it to systems in a remote location for further analysis and study. Telemetry is used in a myriad of industries from tracking spacecrafts, medical monitoring, tracking wildlife, and so on.

DIKSHA has telemetry that records and measures data up to a minute level of activity such as a button click. DIKSHA uses the Telemetry specifications of Sunbird to capture the data.

Click this link to get the details of the Telemetry specification.

Click this link to participate in the community discussions.

Conclusion

The timing has never been better for using technology to enable and improve learning at all levels, in all places, and for people of all backgrounds. From the modernization of E-rate to the proliferation and adoption of openly licensed educational resources, the key pieces necessary to realize the transformations made possible by technology in education are in place. Educators, policymakers, administrators, and teacher preparation and professional development programs now should embed these standards and tools/resources into their practices. Working in collaboration with families, researchers, cultural institutions, and all other stakeholders, these groups can eliminate inefficiencies, reach beyond the walls of traditional silos set up, and form strong partnerships to support everywhere, all-the-time learning.

No matter their perceived abilities or geographic locations, all learners can access resources, experiences, planning tools, and information that can set them on a path to acquiring expertise unimaginable a generation ago. It is a time of great possibility and progress for the use of technology to support learning.

References

1. MEITY, https://www.meity.gov.in/writereaddata/files/IndEA_Framework_1.0.pdf
2. MEITY, https://www.meity.gov.in/writereaddata/files/InDEA%202_0%20Report%20Draft%20V6%2024%20Jan%2022_Rev.pdf
3. eGOV Standards, http://egovstandards.gov.in
4. http://www.imsglobal.org/lode/index.html
5. IMS Global, https://www.imsglobal.org/content/packaging/cpv1p1p3/imscp_infov1p1p3.html
6. IMS Global, http://www.imsglobal.org/metadata/mdv1p3/imsmd_bestv1p3.html#1621637
7. IEEE, http://ltsc.ieee.org/wg12/index.html
8. IRRODL, https://www.irrodl.org/index.php/irrodl/article/view/4529/5298
9. ABC, https://www.ugc.ac.in/pdfnews/2656827_NAC-BANK.pdf
10. W3.ORG, https://www.w3.org/TR/vc-data-model/
11. DEPA, http://niti.gov.in/sites/default/files/2020-09/DEPA-Book_0.pdf
12. PSR India, https://www.prsindia.org/billtrack/personal-data-protection-bill-2019
13. Digital Locker, http://dla.gov.in/sites/default/files/pdf/DigitalLockerTechnologyFramework%20v1.1.pdf
14. GDPR, https://gdpr-info.eu/recitals/no-38/
15. CCA, http://cca.gov.in/eSign.html
16. Data Gov https://data.gov.in
17. GDPR, https://gdpr-info.eu/recitals/no-32/
18. ITU-T Focus Group Bridging the Gap: From Innovation to Standards, http://itu.int/en/ITU-T/focusgroups/innovation/
19. ISO/IEC JTC1 Subcommittee 36, http://www.sc36.org/
20. IEEE Learning Technology Standards Committee, http://www.ieeeltsc.org/
21. International Digital Publishing Forum, http://idpf.org/epub
22. Advanced Distributed Learning Initiative, http://adlnet.gov/
23. Rustici Software: SCORM explained. http://scorm.com/scorm-explained/
24. IMS, http://imsglobal.org/

Approval By:

1.	Smt. Anita Karwal IAS	Secretary, Department of School Education and Literacy (DoSEL), Ministry of Education, Government of India
2.	Sh. Santosh Yadav IAS	Additional Secretary, Department of School Education and Literacy (DoSEL), Ministry of Education, Government of India

Reviewed by NDEAR Technical Committee:

1.	Sh Rajender Sethi, DDG NIC	Chair
2.	Prof. Amarendra Behera - Jt. Dir., CIET, NCERT	Member
3.	Shri Vinay Thakur - Addl. DG, BiSAG & COO NeGD, MeitY	Member
4.	Dr Pramod Varma - CTO, EkStep Foundation	Member
5.	Shri Jagadish Babu - COO, EkStep Foundation	Member
6.	Dr Naveen E Nicolas, Director, ICT, DoSEL	Member
7.	Sanjeev Yadav, Director Auth-I, Unique Identification Authority of India	Member
8.	Sh Gaurav Singh, Director ICT, DoHE	Member
9.	Prof. K. Srinivas - Head of ICT & Project Management Unit, NIEPA	Member
10.	Shri Saba Akhtar (HOD) - Sr. Technical Director, NIC (DoSE&L division)	Member
11.	Dr Antriksh Johri - Director (IT & Project) & Chief Information Security Officer, CBSE	Member
12.	Kiran Anandampillai, Technology Advisor, NHA	Member
13.	Representative of UIDAI	Member
14.	Representative of IndEA Division, NeGD, MeitY	Member
15.	Sh Rajnish Kumar, Director, DoSEL, MoE	Convener

Support & Assistance for preparation provided by NDEAR DIKSHA Technical Team:

1.	Sh. Rakesh Verma	NDEAR DIKSHA PMU Lead
2.	Sh. Chinmay Chaitanya	Team Member
3.	Smt. Niharika Vasumitra	Team Member
4.	Sh. Sathyaraj Iyer	Team Member
5.	Sh. Sahil Kapoor	Team Member
6.	Smt. Megha Kumar	Team Member