National
Data Sharing Policy

ICTA
ideas actioned

Document Control

Document Title	Report on Data Sharing Policy for Government of Sri Lanka
Abstract	This document provides Data Sharing Policy for Government of Sri Lanka and important related aspects.

Terms, Definitions and Abbreviations

Terms	Definition
Critical Information Assets	Information Assets key to the core operation, performance, capability, viability and credibility of the organization.
Custodian (in the context of the Information Assets)	The recognised officer responsible for implementing and maintaining information assets according to the rules set by the owner to ensure proper quality, security, integrity, correctness, consistency, privacy, confidentiality and accessibility. A custodian will be responsible for specific classifications or categorisations of data.
Government Information	'Government information' includes all reports, documents, data sets and information that Sri Lanka Government organizations collect or produce for statutory purposes or business needs. Information may be stored in a number of information formats. This includes presentation in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, textual or numerical form.
Information	Information is any collection of data that is processed, analysed, interpreted, classified or communicated in order to serve a useful purpose, present fact or represent knowledge in any medium or form. This includes presentation in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, textual or numerical form.
Information and Communication Technology (ICT)	Refers to applications, information and technology.
Information and Communication Technology (ICT) Facilities and Devices	ICT facilities and devices cover computers (including palm and handheld devices); telephones (including mobiles); removable media; radios or other high frequency communication devices; television sets; digital or analogue recorders (including DVD and video); cameras; photocopiers; facsimile machines; printers (and other imaging equipment); electronic networks; internet; email; web mail; and fee-based web services.
Information and Communication Technology (ICT) Resources	Information and communication technology resources for an organization means the resources the organization needs to meet the informational requirements of the organization and its clients, and carry out the organization's operational responsibilities. These include: − *Information obtained, produced or supplied by the organization;* − *The information systems of the organization;* − *Equipment or facilities that support the organization's;* − *Information systems, including, for example, communication;* − *Equipment or software; and* − *The organizations's human resources.*
Information Asset	An identifiable collection of data stored in any manner and recognised as having value for the purpose of enabling an organization to perform

	its business functions thereby satisfying a recognised organization requirement. Data or information that is referenced by an organization, but which is not intended to become a source of reference for multiple business functions is not considered to be an information asset of the organization. This is merely information. Information assets are considered to be associated with one of four standard types: − *Transactional;* − *Analytical;* − *Authored; and* − *Publication.* It should be noted that information content may appear in more than one asset. For example, customer details may exist as a transactional asset, but also be represented in a second analytical asset. In this case there are two assets. It is important to note that an Information Asset may also be considered to be a Public Record if it meets certain criteria. However, not all of an organization's Information Assets will necessarily be Public Records.
Information Asset Owner	The recognised officer who is identified as having the authority and accountability under legislation, regulation or policy, for the collection and management of information assets on behalf of the Governement of Sri Lanka, usually the Commissioner General.
Information Asset Register	A register of information about the significant information assets in the organization's information portfolio. For each information asset, the register holds details including asset name, description, classification, owner and custodian.
Information Systems	The organised collections of hardware, software, equipment, policies, procedures and people that store, process, control and provide access to information.
Classified Information	Official information (National Security or Non-National Security) which require additional security controls in accordance with the risk of compromise to the information. (See also "Non-National Security Information" and "National Security Information")
National Security Information	Any official resource including equipment that records information about or is associated with, Sri Lanka's: − *Security form espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Sri Lanka's defence system or acts of foreign interference;* − *Defence plans and operations;* − *International relations, that relate to significant political and economic relations with international organisations and foreign governments; or* − *National interest, that relates to economic, scientific or technological matters vital to Sri Lanka's stability and integrity.*

Non-National Security Information	Any official information asset that requires increased protection and does not meet the definition of national security information. Most often this will be information about: − *Government or organization business, whose compromise could affect the governments capacity to make decisions or operate, the publics confidence in government, the stability of the market place and so on;* − *Commercial interests, whose compromise could affect the competitive process and provide the opportunity for unfair advantage;* − *Law enforcement operations, whose compromise could hamper or render useless crime prevention strategies or particular investigations or adversely affect personal safety; or* − *Personal information that is required to be protected.*
Owner (in the context of Information Assets)	Information as an asset is owned by the Government of Sri Lanka. The term owner is the recognized officer who is identified as having the authority and accountability under legislation, regulation or policy for the collection of information assets on behalf of the Government of Sri Lanka. Information owners define the policy which governs the information assets of an organization, for example determining the classification of information assets. An owner will often delegate the operational responsibility for information assets to a custodian, who applies controls that reflect the owner's expectations and instructions such as ensuring proper quality, security, integrity, correctness, consistency, privacy, confidentiality and accessibility of the information assets. It is well understood that within government all legal ownership and associated rights and entitlements are vested in the Government of Sri Lanka. However, practically, the Government can only act through the officers of the legislature, judiciary or the public service. Indeed, at an intellectual property level beneficial use delegations do not apply when the public entity represents the Government of Sri Lanka and has the power to deal with assets under its enabling legislation. That is, the public sector owner is deemed to be acting as the Government in relation to assets. For this reason the term owner for the purpose of describing the information architecture is deemed to be the officer through whom the Government, as the ultimate owner, is acting.
Information Field Register	A register (electronic or paper based) that keeps a record of classified information field attributes. The register contains information such as name of information field, the description of the field, the classification level of the field, and the reference to relevant impact assessment carried out.

List of Abbreviations

Abbreviation	*Meaning*
FAQ	Frequently Asked Questions
GoSL	Government of Sri Lanka
IAR	Informational Asset Register
ICT	Information and Communication Technology
ICTA	Information and Communication Technology Agency
IFR	Information Field Register
IPRs	Intellectual Property Rights
ISR	Informational Service Register
IT	Information Technology
LIFe	Lanka Interoperability Framework
MoA	Memorandum of Agreement
MoU	Memorandum of Understanding
SLDSP	Sri Lanka Data Sharing Policy
ToR	Terms of Reference
XML	Extended Markup Language

Table of Contents

1. *Preamble* 2

2. Definitions 4

3. Need, Scope and Objective for Data Sharing Policy 6

4. Journey towards a Data Sharing Policy 10

5. Data Sharing Policy Framework 12

5.1 Data Sharing Principles 13

5.2. Data/Information classification Framework 15

5.3. Service Classification Framework 17

5.3.1. Service Classification Level 17

5.3.2. Service Types 17

5.4.Data Sharing Framework 18

5.4.1. Legal Framework 18

5.4.2. Technical Framework 19

5.4.3. Operational Framework 20

5.4.4. Change Management Framework 21

5.4.5. Governance Framework 22

6. Implementation Roadmap 23

6.1 Stage 1- "Define" 25

6.2 Stage 2: "Design" 28

6.3 Stage 3: "Implement" 33

6.4 "Monitor and Evaluation" 36

6.5 Implementation Timeline 39

7. Way Forward 40

8. Annexures 43

8.1. Annexure 1: Data Classification Flowchart 44

8.2. Annexure 2: Data to Service Classification Mapping 45

8.3. Annexure3: Guidelines for Security Framework 46

8.4. Annexure 4: Information asset security classification controls 47

8.4.1 SECRET 47

8.4.2 CONFIDENTIAL 48

8.4.3 LIMITED SHARING 50

8.4.4 PUBLIC information 51

8.5. Annexure5: Guidelines for Data Migration 53

8.6. Annexure 6: Change Management Framework 54

1.Preamble

1. Preamble

The statement that "Data is the power to drive future" can hardly be debated. The inherent capability of the value of information is widely accepted across and can reap numerous benefits to the society and leading to "Open Government" by reducing corruption, enabling rational debate, better decision making and use in meeting civil society needs.

1. It is therefore imperative to create an ecosystem where data sharing is promoted, harnessed and delivered to the public and with other government departments. Through this ecosystem, each individual or department shall have necessary access to all the information which is deemed sharable and held by Government. Once this is achieved, the individuals and departments shall be empowered by using the *"**Right Information at Right Time**"*.

2. The principles on which data sharing and accessibility shall be based include:
   - *Transparency*
   - *Protection of Intellectual Property*
   - *Protection of Data Privacy*
   - *Interoperability*
   - *Legal support and mandates*
   - *Formal responsibility to enable and promote data sharing*
   - *Accountability of completeness and correctness of data*
   - *Technical and Operational efficiency*

Benefits of Data Sharing

Government

- *Enhanced efficiency in Government service delivery, improved policy development and decision-making through easy access to data collected and generated by various other government departments, ministries and agencies.*
- *Strengthened agility and responsiveness of Sri Lankan government to meet changing needs, more efficient use of public funding through reduction in repetition of tasks associated with information management such as; collection, authentication, validation and storage and*
- *Enhanced communication across government and related sectors.*

Citizens

- *Improved accountability and transparency for citizens, providing them with a better idea of how government manages their information and its business.*
- *Easier public access to government services*
- *Citizens' contact details can be updated by one department and shared with others, saving time in having to register in multiple locations for government services.*

Business

- *Enhanced business opportunities due to access to public data*
- *More transparency into government functioning leading to economic reforms*
- *Cost Optimization as same data shall not be collected and maintained at different places thereby increasing accuracy*

2. Definitions

2. Definitions

Data:*Data in this document refers to all structured collection of numerical compilations and observations, documents, facts, maps, images, charts, tables and figures unless otherwise noted.*

Information:*Data that is processed, organized, structured or presented in a given context so as to make it useful, it is called Information. In other words a structured or processed data is called information. Words "Data" and "Information" have been interchangeably used in the document*

Information asset:*An identifiable collection of data stored in any manner and recognized as having value for the purpose of enabling an organization to perform its business functions thereby satisfying a recognized organization requirement. Information assets are considered to be associated with one of four standard types: Transactional, Analytical, Authored and Publication. It shall be noted that information content may appear in more than one asset. For example, customer details may exist as a transactional asset, but also be represented in a second analytical asset. In this case there are two assets.*

Information Field Register: *A register to record the unique information fields and their respective classifications. The IFR shall ideally be maintained in a central location and shall cover all unique information fields of an organization, thus be readily accessed and referred to by data owners and other users.*

Information Asset Register: *A register to record the classification of information assets (collection of informational fields). The IAR shall ideally be maintained in a central location and shall cover all security classified information assets of an organization, thus be readily accessed and referred to by the data owners and other users.*

Service Classification Register: *Organizations shall establish and maintain an SCR to record the classification of services. The SCRshall ideally be maintained in a central location and shall cover all services (inbound and outbound) provided by the department and it shall be readily accessed and referred to by the data owners and other users.*

Information Life Cycle:*Information life cycle refers to the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.*

Metadata: *This is data about data. It summarizes what, how, where, for whom and when a particular datum or set of data is collected, the data content and sources.*

Standards - *Any application that embeds data handling functions (e.g., data collection, management, transfer, integration, publication, etc.) and operates on data in a manner that complies with data format and data syntax specifications produced and maintained by open, standards bodies.*

Policy: *Is a deliberate plan of action to guide decisions and achieve rational outcome(s). Policies are used to guide consistent actions, i.e. predictive enough to guide stakeholders that are most involved in achieving the desired outcome.*

3. Need, Scope and Objective for Data Sharing Policy

3. Need, Scope and Objectivefor Data Sharing Policy

Background

The issue with the current state of affairs is that there is a lot of information residing within various government ministries, departments and agencies in silos. A significant amount of resources is required to maintain, and this information do not necessarily provide a complete picture of the type of services the public and government departments use or require. This is exacerbated by the absence of national standards for the storage, use and handling of information. There is a requirement to provide seamless exchange and integration of information residing in silos.

In this backdrop, a project has been commissioned to develop an Information and Service classification framework that would define a process of providing integrated information and services in a holistic manner. The framework would seek to identify a common approach for identifying the sources, owners, level of sensitivity, level of security required of information and services. Also, it would facilitate the sharing of data and information between government organizations to improve productivity and transparency. The framework aims to provide an integrated platform for creation of a nationwide policy for sharing that data.

Scope

The Data Sharing Policy defined in this document is applicable to all data created, generated, collected or archived by the Government of Sri Lanka through its associated departments/ ministries/ agencies using public funds. The data may be in electronic form or in form of manual records.

The policy shall ensure accessibility to data as per the security classification assigned to the data by the Data Classification framework of Government of Sri Lanka. The data classified as shareable by Data and Service Classification frameworks shall be made uniformly accessible to those who need and are authorized to use it. In the event where the data is sensitive, the data would be shared with authorized agencies/people with appropriate controls as defined in the data and service classification framework for the Government of Sri Lanka.

Objective of the Policy

The objective of the policy is to define a set of guidelines and principles to help create an ecosystem for the enhanced access to the sharable data to relevant stakeholders protecting the rights of the information provider and the seeker. The policy shall define a framework that would facilitate pro-active sharing of periodically updated sharable data with Government of Sri Lanka. The policy shall be applicable to all data whether electronic or in the form of manual records.

"create an integrated platform to enable seamless sharing of information to the right people at the right time in a secure, reliable manner to promote mutual benefits to individuals, civil society and the country"

The policy intends to achieve the following outcomes

1. **Seamless sharing of data within the departments and the public**

   With seamless sharing of information, a single window to deliver citizen centric services shall be created to serve the citizens in the most convenient and efficient manner. The policy is not only aimed at sharing data with public, but also will promote data sharing between the departments (on authorized or restricted access). This would be a key enabler for the departments using the same data for providing the services. In this case, the departments may not be required to collect the information again but can use the information available with other departments.

2. **Creation of Integrated e-Service delivery**

   The project would also support implementation of 'e-Sri Lanka' where multiple stakeholder partnerships would be developed between the public sector, the private sector and the civil society, to 'take the dividends of ICT to every village, to every citizen, to every business and to transform the way the government thinks and works'. One of the key success factors to this enablement is the presence of an integrated service delivery platform which cannot be achieved without sharing of information based on appropriate classification levels.

3. **Data is provided by Public**

   The data with government has been generated by public funds and hence as long as sharing of data is not harmful to the public interest or the national intrests, it shall be made readily accessible to all.

4. **Considerable percentage of data may not be sensitive**

   A large percentage of the data generated with government may not be sensitive and hence restricting the dissemination of such data only prevents the use of it for scientific, research, social and economic development purposes. Therefore the national level policy would help the sharable data to be used for such purposes, with appropriate controls.

5. **Avoid duplication and data integrity issues**

   Various government departments and agencies require relevant data covering a broad range of economic and social indicators for planning and monitoring social and economic activities. In the absence of data sharing within the government, the same data gets generated separately for each department leading to the duplication of effort and wastage of time and public funds.

6. **Protect the interests of all stakeholders**

   To promote sharing of data, it is imperative that necessary standards and safeguards are put in place in the form of a Data Sharing Policy to protect interests of both the data provider and the seeker.

7. Promote Open Government Data principles(*opengovdata.org)*:

a) *Promoting interoperability standards – Integration with LIFe*
b) *Classification of Information as an Asset*
c) *Providing controls for completeness of the data*
d) *Ensuring the timely delivery of the data accessible to the right people*
e) *Processing of data in machine readable format – Data digitization and processing*
f) *Sharing of data in non-proprietary formats*

8. Promote Open Government principles(*www. opengovpartnership.org*):

a) *Providing Access to public Information*
b) *Information access leading to reduction in corruption and inefficiencies*
c) *Financial transparency in the system*
d) *Bringing more accountability to provide information and to maintain its accuracy*
e) *Integrated window for public services*
f) *Promoting national level governance and citizen partnership*
g) *Giving more access to departmental mandates, laws & insights into Government functioning*
h) *Open data would lead to faster closure of service requests and public grievances based on time bound services and provide higher accountability*

9. Creation of a governance framework

The policy also aims to create a governance framework to monitor and evaluate the implementation of data sharing framework in the government departments/ministries. Some of the steps include;

a) *A dedicated person must be designated to respond to people trying to use the data.*
b) *A dedicated person must be designated to respond to complaints about violations of the principles.*
c) *An administrative or judicial provision to review whether the agency has applied these principles appropriately.*

The details of this are mentioned in the sections below.

10. Guidelines for the creation of legal, technical, operational and change management frameworks for data sharing

The policy also aims to provide guidelines for the creation of legal, technical, operational and change management frameworks for the implementation of data sharing framework in the government departments/ministries. A summary of guidelines to be mentioned under this section is mentioned here while details are mentioned in the sections below:

A. **Legal** - Security Policies , Intellectual Property Rights (IPRs) and Privacy Guidelines
B. **Technical** - Delivery Mechanism, Connectivity, Data standards and records digitization
C. **Operational** - Implementation Plans and Risk management
D. **Change Management** - Trainings and Awareness Programs

4. Journey towards a Data Sharing Policy

4.Journey towards a Data Sharing Policy

Creation of a National Data Sharing Policy is an important step towards achieving Open data concepts and Right To Information in Sri Lanka. This National Data Sharing Policy receives its basis from the Service Classification framework which in turn is based on the Information/ Data Classification framework with the empowerment through Right To Information. The Department level Data Sharing Policy is derived from the National Data Sharing Policy and shall be in conformance to the same.

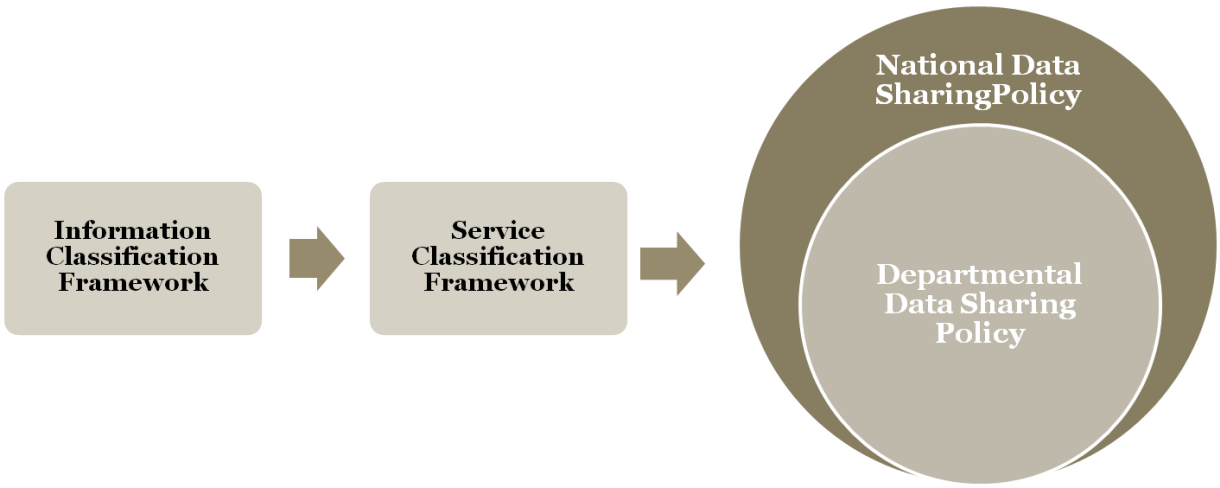
The key components of data sharing policy include:

Data Classification Framework –Data classification is based on the impact of sharing of information with different stakeholders. Based on the impact and findings, appropriate controls are identified.

Service Classification Framework –Service classification framework evolves from information/ data classification framework and aims to share Information Assets (Collection of data elements) as a service. The services are shared as either "*Data Services*" or "*Verification Services*" and can be shared at three levels – *Open, Authorized and Restricted*.

The security classification assigned to a service must at least be the same as the highest security classification of the data being shared or transferred during the course of service delivery.

Data Sharing Policy – The data sharing policy has been created based on the data/services classification frameworks. Within the ambit of the National Data Sharing policy, data sharing policies specific to the departmentsmay be created which would provide the legal, operational, technical and change management frameworks to implement controls which needs to be placed for the effective sharing of information.



5. Data Sharing Policy Framework

5.Data Sharing Policy Framework

The following section describes the data sharing policy framework based on the global best practices and Sri Lanka Data & Service Classification frameworks.

5.1 Data Sharing Principles

Data sharing by government of Sri Lanka ministries, departments and agencies must adhere to the following principles:

A. Transparency

The data sharing policy must be aimed at bringing more transparency into the departmental functions. The department shall provide for sharing of data with respect to internal working of the department (unless specified by departmental mandate), the process for key services, contacts ofimportant people and the escalation procedures. The department shallalso provide time bound procedures for theservices offered on a transparent basis.

B. Protection of Intellectual Property

The department sharing the data shall protect the Intellectual property rights of both the department and the individuals. The data sharing policy for the department shall not bypass right to preserve the IPRs (Intellectual Property Rights) for the provided dataset and any changes to IPR policies for the department mandate shall be carried out in accordance to the rules and regulations that govern the departmental operations.

C. Protection of Data Privacy

Before sharing of information, the data privacy shall be considered well in advance. Currently Sri Lanka does not have any national policy on data privacy; however, consent of the information originators need to be taken before sharing their information. Similar arrangements are required for inter-departmental data sharing as well. However, data subject to privacy shall supersede the data sharing policy

D. Interoperability and linking to LIFe

Electronic data is stored in a multitude of formats of which large number of formats is mutually undecipherable. Thus, one government department saving its documents in a proprietary format may not allow for other departments/citizen to interact efficiently with those data sources. For such reasons, certain set standards shall be used by all government departments. To support this, an interoperability framework, LIFe (Lankan Interoperability Framework) has been defined by ICTA which governs the mechanism for providing data sharing standards. The data sharing policy for department shall be compliant to LIFe to facilitate nation wise adoption of LIFe.

E. Legal support and mandates

The department shall assume responsibility for supporting the data sharing through legal procedures and mandates. The department shall own the changes required to facilitate data sharing with other departments and public. The required changes may include:

- Changes for IPRs and Data Privacy
- MoU/MoA with different departments

F. Formal responsibility to enable and promote data sharing

The department shall assume formal responsibility to enable and promote data sharing. To facilitate data sharing, all the necessary process, teams and supporting technology shall be setup by the department.

G. Accountability of completeness and correctness of data

It is important to note that completeness and correctness of data is very important, therefore all necessary steps shall be taken by the department to maintain the integrity of the data. Inaccurate open data, such as weather information may lead to catastrophic effects and therefore it is important to ensure the accuracy of data.

H. Technical and Operational efficiency

The department shall make all efforts to share the data through technically and operationally efficient mechanisms. This shall mean that department shall make use of optimal techniques and guidelines so that data sharing does not become an additional burden on the departmental functioning. The department shall make necessary modification for optimization of processes for the seamless data exchange with minimal human effort.

I. Machine readable formats

It may be noted that not all open standards (such as PDF) are 'machine readable' so that that the data can be manipulated, reprocessed, visualized, mashed up with other data, or even made interactive. While it is desirable to have information organized in in open standards, it is also desirable for them to be in machine readable formats (such as well defined XML). In this regards the departmental policy shall mandate sharing of information in machine readable format.

J. Pricing

All data, metadata and statistical products declared as official statistics shall be FREE to ALL Users or applicable cost shall not be more than the recovery amount to cover reproduction or distribution costs.

Data which has to be shared under restricted and authorized access may be shared at a price decided by the government department or agency which is the owner of the data as per the policies of the government of Sri Lanka. The owner agency is the one which has created, generated or collected the data. All such costs must be communicated and published on websites; bulletin boards etc by concerned government departments in advance.

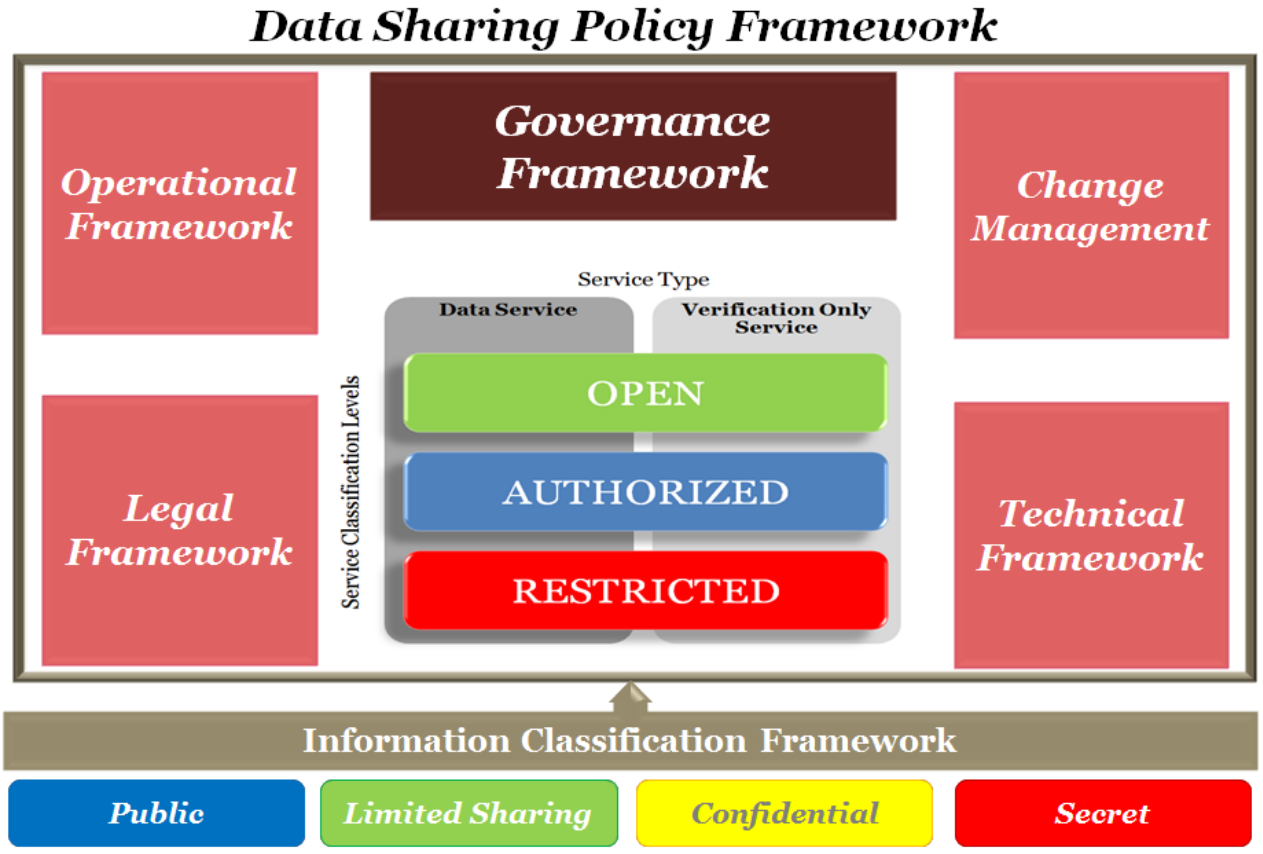
K. Maintenance of Data Quality

For ensuring the quality, integrity and authenticity of data good statistical compilation and dissemination practices must be adopted by the departments owning the data. Observance of procedures for data compilation and dissemination ensures high standards of professionalism.

Note: The department above refers to any organization/body/ministry / etc involved in the process of data sharing as either an information provider or an information seeker.

5.2. Data/Information classification Framework

Data classification is the first step in moving towards a data sharing paradigm. Through this framework, the data elements are identified and classified based on the sensitivity and impact of the sharing of that information. The classification model has following elements:



The major components in the framework include the following:

- **Classification Levels** –A Classification Level represents confidentiality rating (or security rating) that must be applied to the informational assets.Four main levels of security classification markingshave been defined as part of the Information Classification framework; ***"Public", "Limited Access", "Confidential" and "Secret".***

- **Dissemination Limiting Markers (DLM)** – Dissemination Limitation Markers supplement the security classification system for identifying official information. DLMs are markings for information where disclosure of information may be limited or prohibited by legislation or where it may otherwise require special handling. Departments/agencies are responsible for determining the appropriate protections to be applied to information bearing DLMs. DLMs have been categorized in the following four categories:***Sensitive, Sensitive: Personal, Sensitive: Legal, andSensitive Government.***

- **Caveats** – Caveats are warnings that specify or limit the people who can have access to the information. Use of caveats with information signifies that the information has special requirements in addition to those indicated by the protective marking. Information bearing agency specific caveats are to be re-labeled or appropriate procedures agreed up before the release or the transmission outside of that agency. The prior agreement of the originating agency—in other words, the agency that originally placed the caveat on the material—is

required to remove a caveat. If the originating agency does not agree to the removal of the caveat, then the information cannot be released. The requirement to obtain agreement of the originating agency to release the material cannot be the subject of a policy exception under any circumstances.The following categories of security caveats are used: ***Eyes Only (EO), Permission Required (PR), When completed (WC), Do not release Until (DNRU).***

Based on these elements, a framework has been defined encompassing methodology, process and necessary tools for data classification. A broad level flow diagram for the assignment of classification ratings to data elements is mentioned in **Annexure 1** for reference. For further details on how to perform data classification, please refer the "*Data Classification Framework*" document.

5.3. Service Classification Framework

The sharing of data is done via services and therefore a separate service classification framework has been defined based on the data classification framework. The model has also been aligned with the data sharing policy and defines the following key components.

5.3.1. Service Classification Level

Based on the type of security classification assigned, the access to the datamay be regulated and limited to a selected group of individuals or operational units. While providing access it shall be noted that all government data is generated by using public funds and hence as far as possible access to the sameshould be unrestricted, easy, timely and user-friendly as long as the security and privacy requirements are preserved. Access provided to data held by government can be of following types.

1. **Open Access**

Data that may be accessible freely by any individual / agency and the access is provided without any process or registration / authorization is referred to as open data and is freely available to all.

2. **Authorized Access**

Access to data is restricted when data sets are accessible only through a prescribed process of registration / authorization by respective departments / organizations. Data having restricted access shall be made available to only the recognized institutions / organizations / public users, through defined procedures. The requester of such data may need to authenticate his / her identity and provide a valid reason to access the data in question by producing the correct documentation and authorizations.

3. **Restricted Access**

Data declared as restricted shall be accessible only through and under authorization to selected individuals or organizations based on a need to know basis.

5.3.2. Service Types

This refers to the information types being shared through the provided services. The service types are categorized into two broad categories as mentioned below:

1. **Data Service**

Some or all data elements within the data "*Asset*" can be shared depending on the derived sensitivity of the data Asset

2. **Verification Only Service**

Given a set of inputs, an answer as of Yes/No may be provided after the proper verifications are carried out in the source data bases.

Based on these elements, a framework has been defined encompassing a methodology, process and the necessary tools for Service classification. A broad level flow diagram for assignment of service classification based on data classification has been mentioned in **Annexure 2** for reference. For further details on service classification, please refer the "*Service Classification Framework*" document.

5.4.Data Sharing Framework

5.4.1. Legal Framework

Any data sharing shall happen within the legal framework of Sri Lanka, its national policies and legislation as well as the recognized international guidelines. It is imperative to prevent misuse of data and assure security, integrity and confidentiality of data. Objective of the legal framework is to ensure that the privacy, confidentiality, intellectual property rights and the associated security requirements are formally protected.

Data Ownership

Data shall remain the property of the agency/department/ ministry/ entity which generated/collected it.Access to data under this policy shall not be in violation of any acts and rules of the government of Sri Lanka in force. Legal framework of this policy shall be aligned with various acts and rules covering the data.

The acquiring organization/ individual shall always cite the original data source and assume all responsibilities as to the use, analysis and interpretation of the data being provided. Once data has been provided, the government of Sri Lanka and associated departments / ministers / agencies shall not vouch for any analysis performed on the data, or for the quality of the data.

All data being shared must ensure compliance to guidelines for legal, security, IPR, copyrights and privacy requirements.

Memorandum of Understanding or Agreement

The data owner shall sign a MoU/MoA, to document the terms of the arrangement and treatment of the data so that confidentiality is not compromised during the process of sharing. It is suggested that Legal and privacy experts be consulted as part of the MoU/MoA process. The MoU shall consider the information security and privacy during:

- *Data Storage*
- *Data Handing/Processing*
- *Data Transmission*
- *Data Destroy/Dispose*

5.4.2. Technical Framework

The technology framework shall be formulated to enable and facilitate data sharing within the government and with citizens. For data to be seamlessly shared it is required that the data collection, generation, storage and transfer follows same technological standards.The consistent application of relevant standards give assurance to users and providers that the information is 'fit for purpose' and implies a certain level of quality. The application of standards fosters an environment of trust and dependability across government, providing a reduction in duplication of effort and re-work.

"Provide technical platform to enable creation of information in a way that supports downstream information processing and dissemination activities"

Security Framework

Departments shall create a comprehensive security framework for the protection of data assets and unauthorized usage of the information. This is extremely important to mitigate theeffect of illegal usage of data that may lead to national level impact. It is therefore important to create a clear policy for controls related to Confidentiality, Availability and Integrity (CIA) of the data. A draft guideline for the creation of a security policy is mentioned in **Annexure3**. ICTA has already developed an Information Security Policy which shall be used as a basis.

Sharing data through e-delivery

Departments shall deliverservices through electronic mediums providing single-point access to information assets and applications published by given departments. All sharable data shall be available through the e-delivery channels for enabling rational debate, better decision making and use of civil society.

Use of machine-readable and open formats

Departments shall use machine-readable and open formats for information as it is collected or created. While information shall be collected electronically by default, machine-readable and open formats must be used in conjunction with both electronic and telephone or paper-based information collection efforts.

Build information systems to support interoperability and accessibility

The system design shall be scalable, flexible, and facilitate extraction of data in multiple formats and for a range of uses as internal and external needs change, including potential uses not accounted for in the original design. The data shall be consistent with existing policies of departments and must use standards in order to promote data interoperability and openness. This policy mandates the use of LIFe while defining the departmental policy for interoperability *(one of the components of the data sharing policy)*.

Records Digitization and Migration

A considerable amount of data with government still resides in manual records, files etc which are not easily and uniformly accessible to all. Hence digitization of all government data is a key step towards creating an open data environment. A recommended step during the process of data sharing policy is to determine if a parallel programme to digitize data may be taken up. Such a program would be helpful in sharing information currently existing in manual form or proprietary formats (in legacy systems).

5.4.3. Operational Framework

Creation of an implementation plan

Task 1 - Identification of dependencies: Once the dependencies are identified, they shall be refined ensuring that any constraints on the implementation plans are identified. There are several key dependencies that may be taken into account, such as dependencies on existing processes and implementations and existing information systems / services or changes to them. Dependencies are required to be documented and used for determining the sequence of implementation and identifying the coordination that would be required. A study of the dependencies of groups and activities are required to create a basis for the projects to be established. Once this is done, relevant projects are examined to verify whether incremental approachesare viable.

Task 2– Determine constraints: Through this step, all constraints related to business, data, application and technology are collated and documented. This is an essential step in the overall planning and would help to identify the boundaries in which the project has to be executed.

Task 3- Identify projects for execution: The activities shall be logically grouped and prioritized based on requirements, dependencies, business benefits and the constraints within the environment.Once the packages are defined, these are grouped into portfolios and projects taking into consideration the dependencies and the strategic implementation approach.

Task 4 – Evaluate implementation: The department shall evaluate implementation strategy alternatives and select an implementation strategy. The departmental teamshall explore the different methods of implementing the future transformed environment along with the associated risks, timing, duration, costs, benefits, barriers, and enablers. Once the approach and acceptance criteria for implementation have been defined, the various components of the current and planned future environments are analyzed to determine which specific actions are required to enable a successful migration and implementation plan. From this analysis, the approaches and policies that shall constitute the implementation are defined including:

- *Whether to use **cutover ('big bang'), pilot, parallel running or a phased or staged approach** to 'go-live'*
- *The **associated measurement criteria** for the items that shall constitute the successful migration and its acceptance*

A detailed implementation plan shall be made for the project which shall be the guiding document for the program management office and the implementing agencies during project execution. The implementation plan shall specify:

- *Approach containing different phases for the implementation of the project,*
- *Implementation time frame for the complete system rollout of the project*
- *Standard processes to be used to measure the quality and consistency of the output*

Implementation Risk management

During the planning and implementation phases of sharing data, a comprehensive approach towards risk management shall be adopted by the departments. The department shall adhere to the following process for risk management throughout the execution of the project.

Each of these steps is undertaken based on the defined framework and may often lead to the mitigation of risks; a template for this is illustrated below:

Risk ID	Risk	Preliminary Risk			Mitigation	Residual Risk		
		Effect	Frequency	Impact		Effect	Frequency	Impact

The departments would create a separate risk register to manage the risks involved during the implementation of the project.

5.4.4. Change Management Framework

To develop a data sharing culture in the government officials and functionaries, a comprehensive change management initiative shall be undertaken by the departments. The change management shall not only educate people of the importance and the ways of data sharing but shall also cater to the necessary frameworks and legal aspects.

- **Training**

  To ensure a consistent application of the data sharing framework, guidelines and information management principles need to be formulated. It is also imperative that Data Sharing Champions are identified within each government department and agency. They must be given trainings on standards and frameworks. The training shall also emphasize on the benefits that would result in to both government and citizens by adopting the data sharing principles. An education program can be developed for government employees involved in the information lifecycle, such as policy developers, analysts and information custodians etc. The program would need to cover standards and practices for information management and sharing. The education plan shall also cover details about privacy, licensing and copyright, legislative requirements and technology.

- **Recognition and rewards**

  Recognition and rewards for those who actively participate in information sharing shall provide an extra stimulus for government agencies/ departments to create an open data culture in their organizations. The rewards shall recognize individuals as well as an organization's commitment towards data sharing.

- **Awareness Programs**

  Awareness about the data sharing policies of the Government of Sri Lanka, intended benefits and steps required to create an open data environment in Sri Lanka needs to be created. Information on government websites, organizing events, messages in government publications, advertisements in media can help build a sense of responsibility towards data sharing in Government employees and awareness in citizens.

A brief guideline on change management framework has been mentioned in **Annexure 6** for ready reference. The departments shall make necessary modificationbased on departmental requirements and use for training of its employees and other stakeholders.

5.4.5. Governance Framework

Compliance

The department shall undertake the following steps for ensuring compliance to the data sharing policy

- *A dedicated person must be designated to respond to people trying to use the data.*
- *A dedicated person must be designated to respond to complaints about violations of the principles.*
- *An administrative or judicial provision to review whether the agency has applied the principles (mentioned in section 5. 1) appropriately.*

It is necessary to review the outcome of the data sharing policies created by Sri Lankan government and deliberate on the need to any updates required in the policy. The evaluation plan and appropriate tools need to meet the expectations of all stakeholders, and is vital to the success of the data sharing. There shall be a requirement for constant monitoring, reporting and reviewing of data sharing polices and principles endorsed by the government.

Details of the governance are mentioned in the sections below; under the “Monitor and Evaluate” Phase.

6. Implementation Roadmap

6. Implementation Roadmap

The implementation roadmap consists of three main stages, namely:

Define: This is the first stage in the implementation roadmap and it primarily deals with the identification of data and services to be shared. Furthermore, during this stage, data to be digitized from manual records and legacy systems which has to be migrated to the new systems (with data sharing) shall also be identified. A broad level implementation roadmap for the execution should also be created at this stage.

Design: Once the data has been identified for classification, the classification process is applied to arrive at the appropriate classification levels. The classification process is applied to both information and then services. Based on the classification, a departmental level policy needs to be defined having information on control points, data digitization strategy, adoption of security framework and creation of change management framework for identification of changes to people, process and technology due to these changes.

Implement: The final stage in the implementation deals with the development of data sharing technologies by sharing the data through the departmental websites or equivalent delivery mechanisms. Furthermore, upon classification process for data sharing, signing of agreements (MoU/MoA) needs to be initiated to protect the information security. To support the larger cause of the project, this stage also deals with the provision of training to all staff members and other key persons for better system acceptance of the information classification process.

Monitor and Evaluate: This is the first stage in the implementation of information classification and starts with the mobilization of the *"Data sharing team"*. This teamshall be responsible for end to end implementation of data sharing (andrelevant processes related to classification etc). In this stage, the objectives of the engagement are verified through regular compliance checks. Based on the checks and feedbacks, the information classification policy may be revised. The necessary changes are also required to be applied to the data sharing process.

6.1 Stage 1- "Define"

Step 1: Creation of the data sharing team

To effectively manage the data sharing, it is suggested that a dedicated team with representation from the following (can be expanded /contracted based on departmental requirements) be created:

- *Head of departments and (or) ministries*
- *Chief Information Officer of the department*
- *Public Relationship Officers*
- *Program managers for all IT initiatives*
- *Record Keeping staff*
- *Legal team within department*

The recommended size for this team is four or five (and no more than ten) permanent members.A recommended Terms of Reference (ToR) for this team shall be as follows:

- *Define departmental specific data sharing policy based on generic policy defined by ICTA*
- *Define inventory of information assets to be classified*
- *Define Memorandum of Understanding (MoU) / Memorandum of Agreement(MoA) for data sharing across departments and public*
- *Define appropriate controls for classified data based on different classification. The controls would span across entire information life cycle i.e. from creation to disposal*
- *Establish a training calendar to educate different stakeholder on the classification, its impact, risks and actions to be taken*
- *Conduct periodic checks to verify the compliance*
- *Create change control board to review and update the information classification policy and suggest any changes required at National level*

Departments must ensure that roles and responsibilities are clearly designated for the promotion of efficient and effective data release practices across the agency and that proper authorities have been assigned to execute related responsibilities.

Role of ICTA

ICTA shall provide overall oversight and guidance from an advisory perspective for the implementation of this policy. It shall provide advice on:

- *Creating enabling environments for ensuring equitable access to data for users. ICTA may release advisories in this respect.*
- *Review and update the data sharing policies periodically*
- *Endorsement of the Data Sharing Policy*
- *Providing oversight for the review of prices to be charged for applicable data products and Services to ensure that they are based on cost recovery basis.*
- *Taking charge of change management and communication program for promoting data sharing at national level.*

Role of Department Chief Information Officer/ Chief Innovation Officer / Information Champion

- *Ensure that a comprehensive up to date listing of available data are posted on an accessible channel*
- *Publish all publicly shareable information assets on departmental e-delivery channel*
- *Specify type of access and pricing for restricted information*
- *Organize trainings, education and awareness programs for data sharing at department level*
- *Ensure that data controls are applied consistently and appropriately*

Role of Departmental Users

- *Awareness about data sharing and classification process*
- *Report incidents and issues for violations of departmental policy*
- *Provide timely feedback to department on the quality and usage of its data*

Step 2: Identify Information to be classified:

The foremost step during the implementation phase is *identification of information to be classified*. This process has to be done in several steps as mentioned below:

1. ***Identify data sources*** *– From where the data has to be extracted*
2. ***Identify all data elements*** *– Input, Processing and Output*
3. ***Create a collection of unique data elements*** *as same data elements may be used during input, processing and output stages.*

The following information may be required to be identified for classification:

Information Sources – ***Ministry/Department/Agencies generated Internal Data*** – ***Ministry/Department/Agencies generated data for public*** – ***Citizen data recorded/retained by Ministry/Department/Agencies*** – ***Data for private organizations recorded/retained by Ministry/Department/Agencies***	**Information stored in** – **Government Orders and Files** – **Policies, Advisories, File Notes and Minutes of meetings** – **Fact Sheets and Statistical reports** – **Cabinet Notes, Planning and Execution documents** – **Tenders, RFPs, Contracts and many more** – **Personal Information, Health Information**
Information content types – ***Structured –such as date of birth, gender, bank details*** – ***Semi Structured –such as Name, Address*** – ***Unstructured – such as policies, advisories etc.***	**Information categories** – *Relatively fixed –Organizational charts, FAQs etc.* – *Dynamic – Contact numbers, present address etc.* – *Transactional – Payment Information etc.* – *Archived – Backup data, old files etc.*
Information available on – ***Hard copies and files*** – ***Electronic mails*** – ***Electronic documents*** – ***Databases and business applications*** – ***Other media such as hard disks, floppies***	**Data classification to be undertaken for** – *Original Documents* – *Compiled Documents /Reports* – *Derived /Analytical Reports*

Step 3: Identify Information Services:

Along with the information elements, broad services to be provided to citizens and departments shall also be identified. These services shall further be elaborated in stage 2 under service classification, but it would help the departments to identify them here to understand and collate the services they intend to deliver in the context of the available information.

Step 4: Identify Information to be digitized and migrated

As explained above,a large amount of information in manual form needs to be digitized and migrated from manual and legacy systems. Under this stage, the data from various sources has to be identified for the purpose of digitization and migration. The digitization and migration shall be done in a phased manner and prioritization of the digitization process for various types of data needs to be carried out to avoid the flood of digitization requests.As not all departments may not be required to digitize all the available historical data, this step may be carried out at the discretion of the department on a selected set of data..

Step 5: Identify roadmap for data sharing

Large transitions are typically done in a staged and planned manner due to inherent risks involved with such projects. Therefore, a roadmap for data sharing shall be developed based on priority and complexity of the tasks. This is typically carried out by spreading the transitions across multiple timeframes for implementation. The department shall undertake necessary steps to create a roadmap for the department and get this approved by the higher management.

6.2 Stage 2: "Design"

Step 1: Apply Data Classification

Once the data elements are identified, a data classification framework shall be applied on the data fields. The data classification rests on the following classification model

- **Classification Levels –**Confidentiality rating (or security rating) that must be applied to the informational assets in one of four levels ***"Public", "Limited Access", "Confidential" or "Secret".***
- **Dissemination Limiting Markers (DLM) –** Dissemination Markings for information where disclosure of information may be limited or prohibited by legislation or where it may otherwise require special handling. DLMs have been defined in the following four categories: ***Sensitive, Sensitive: Personal, Sensitive: Legal, and Sensitive Government.***
- **Caveats –** Warnings that specify or limit the people who can have access to the information. Use of caveats with information signifies that the information has special requirements in addition to those indicated by the protective marking and fall into one ***Eyes Only, Permission Required, When completed, Do not release Until***

For each of the data elements, an impact assessment is carried out based on a template as mentioned in below table.

Areas of Impact	Information Classification			
	Public	Limited Access	Confidential	Secret
Overall Impact	**Minor Adverse Effect** on operations, assets, finances or individuals **Nil Adverse Effect** on national security, foreign relations	**Damage** to operations, assets, national security, foreign relations finances or individuals	**Serious damage** to operations, assets, national security, foreign relations finances or individuals	**Exceptional damage** to operations, assets, national security, foreign relations finances or public
Impact on Internal Stability	No impact on internal stability	Damage to internal stability	Serious damage to internal stability	Exceptional damage to internal stability
Impact on operational effectiveness or Security of Sri Lankan forces	No impact on operational effectiveness or Security of Sri Lankan forces	**Damage** to operational effectiveness or Security of Sri Lankan forces	**Serious damage**to operational effectiveness or Security of Sri Lankan forces	**Exceptional damage** to operational effectiveness or Security of Sri Lankan forces
Impact on National Infrastructure	No impact on national infrastructure	Significantly disrupt national infrastructure	Shut down / substantially disrupt significant national infrastructure	Exceptional damage to national infrastructure
Impact on Foreign Relations	No impact on foreign relations	**Damage** diplomatic relations	**Seriously Damage** relations with other governments	**Exceptional damage** to relations with other governments
Internal Security or Intelligence Operations	Impede the investigation or facilitate the commission of serious crime	Damage to effectiveness of valuable security or intelligence operations	Serious Damage continuing effectiveness of highly valuable security or intelligence operations	Exceptional damage to the effectiveness of extremely valuable security or intelligence operations
Financial Impact	**Work Substantially Against** national finances or economic and commercial interests	**Damage** to Financial Stability	**Substantially Damage** national finances or economic and commercial interests	**Severe Long-Term Damage** to Sri Lankan Economy
Impact to Individuals/ Private Information	Endanger individuals and private entities	Damage to Individuals/ Private Information	Threaten life directly	Lead directly to widespread loss of life

Using the table above and the process mentioned in **Annexure 1**, the classification rating for each data elements is identified. Subsequently, classifications ratings of these elements arelisted in following registers:

Information Field Register (IFR):A suggested template to be used for the IFR is given in Annexure B of the Information Classification Framework.At a minimum, the IFR shall include:

- *Unique information fields;*
- *Description of information field (i.e. what is it about)*
- *Classification of Information filed;*
- *Reference to the Impact Assessment; and*
- *List of information assets that utilize the particular information field.*

Informational Asset Register (IAR):A suggested template to be used for the IAR is given in Annexure C of the Information Classification Framework. At a minimum, the IAR shall include:

- *Name or unique identifier of asset or group of assets*
- *Description of information asset (i.e. what is it about);*
- *Location of information asset, including the device on which it is stored;*
- *Information owner and information custodian;*
- *Classification of information asset;*
- *Date of classification with details of authority of classifier*
- *Reason for classification of information asset (particularly important to support review and reclassification of the information asset at a later time –shall include legislative, regulatory, policy or other reference where applicable, or a copy of the impact assessment made); and*
- *Date to review classification (if known).*
- *Users and usage of the information;*
- *Number of copies in circulation and their location; and*
- *Disposal details where information has been disposed of.*

For further details, please refer the ***Information Classification Framework*** document.

Step 2: Apply Service Classification

Oncethe data classification process is completed, service classification process shall be carried out. A service has been defined as ***"a single or multiple information assets that are collectively used in the delivery of a service"***.

The Service Classification is a system encompassing principles, methodology, tools and framework for designating different categories to services based on impact and value of the information assets that are used in the delivery of a particular service. Based on the type of security classification assigned to the data access to data can be regulated and limited to selected group of individuals. A service can have following sharing mechanisms:

Access Types

Open Access

Data that may be accessible freely by any individual / agency and the access is provided without any process or registration / authorization is referred to as open data and is freely available to all.

Authorized Access

Access to data is restricted when data sets are accessible only through a prescribed process of registration / authorization by respective departments / organizations. Data having restricted

access shall be made available to only the recognized institutions / organizations / public users, through defined procedures. The requester of such data may need to authenticate his / her identity and provide a valid reason to access the data in question by producing the correct documentation and authorizations.

Restricted Access

Data declared as restricted shall be accessible only through and under authorization to selected individuals or organizations based on a need to know basis.

Service Types

Data Service–Some or All data elements within Data Assets can be shared depending on the derived sensitivity of the data asset.

Verification Only Service–Given a set of input, an answer as Yes/No may be provided. This is required mostly for services where verification requests are responded to.

A broad level flow diagram for assignment of service classification based on data classification frameworkhas been mentioned in **Annexure 2** for reference. The output of this stage is a ***ServiceClassificationRegister***. A suggested template to be used for the SCR is given in Annexure A of the Service Classification Framework. At a minimum, the SCRshall include:

- *Name or unique identifier of service;*
- *Service owner and Description of service asset (i.e. what is it about);*
- *Information assets used within the service;*
- *Classification of the information assets; and Service classification level;*
- *Reason for the classification of the information asset (particularly important to support review and reclassification of the information asset at a later time –shall include legislative, regulatory, policy or other reference where applicable, or a copy of the impact assessment made); and*
- *Date to review classification (if known).*

For further details on how to perform service classification, please refer the **"*Service Classification Framework*"** document.

Step 3: Define security controls and adoption of security framework for the Information Assets

Appropriate controls shall be applied to ensure that protection is given to information assetscommensurate with the security classification level that has been determined. These shall be established to ensure information shared within government departments and other entities are secure and consistent with the sensitivity of information that is obtained, stored and transmittedto provide the service. The controls for security and overall security guidelines are mentioned in **Annexure3** for reference. The departments shall also refer to national level information security policy during the creation of controls for security.

Step 4: Create Departmental Data Sharing Policy

The department shall develop a data sharing policy for the department, based on the information classification framework, service classification framework and the national data sharing policy. Following factors (but not limited to)could influence the policy:

- *Size of the department*
- *Departmental mandate and Legislation*
- *Current policies and organizational hierarchy*

- *Processes and systems maturity*

Important: Once information has been classified, any changes to the classification policy at national level due to changing needs, regulations etc may impact existing classification and retro fitment exercises need to be carried out for impacted datasets.

Step 5: Design a change management and capacity building framework

Please refer to Section 5.4.4 Change Management Framework for more details.

6.3 Stage 3: "Implement"

Step 1: Share data through e-delivery channels

The department shall at this stage start sharing the data with citizens and other departments. It is assumed that the data sharing is done through departmental e-delivery channels.

During the sharing of data, following checks shall be maintained:

- *The data is up to date, complete and accurate*
- *All data being shared must ensure compliance to guidelines for legal, security, IPR, copyrights and privacy requirements*
- *The shared data is in machine readable format*
- *The data promotes "Open Standards"*
- *The shared information complies to Lankan Interoperability Framework (LIFe)*
- *The terms and conditions of usage of information is made available to Information seeker*
- *For all public data, the information is provided free of cost. Data which has to be shared under restricted and authorized access may be shared at a price decided by government department or agency which is the owner of the data as per the policies of government of Sri Lanka*

Step 2: Imparting necessary trainings

The department shall impart necessary trainings to the different stakeholders. The various stakeholders who need to be trained include (but not limited to):

- *Chief Information Officer of the department*
- *Head of departments & ministries*
- *Public Relationship Officers*
- *Record Keeping staff*
- *All departmental staff*
- *Support desk and GIC*
- *Programme managers for all IT Initiatives*

The training programme shall include protection of information assets and its classification during the entire life cycle of information i.e. capturing to disposal. The training shall also include the incident raising and management policy to deal with any violations that may arise due to non fulfillments of processes. The training shall be done in batches followed by refresher courses so that necessary policies are always followed. It is also important to identify and train the "change agents" who can be helpful in spreading the awareness regarding importance of the Information Classification and Security. A detailed framework on change management and capacity building is mentioned at **Annexure6** for reference.

Step 3: Data Digitization and Migration

Another important step during the implementation is to perform data digitization and migration. As mentioned above, this is a ***recommendatory stage only***. A draft digitization process is as follows:

1. *The department prioritizes the records to be digitized and based on the priority, the department undertakes the activity to digitize the records*
2. *It must be ensured that the digitized and non-digitized files are marked separately to avoid duplicity of work.*
3. *A tracking "excel" cum signoff sheet shall be created by the department containing details under the following heads:*
    a. *Record number*
    b. *Number of scanned documents*
    c. *Data verified by verification officer*
    d. *Other important data*
4. *Department shall update the tracking excel with appropriate comments as when a record is digitized. In case of any missing details, the same shall be recorded against the record number. Upon completion of each record, the verification officer shall verify and approve the digitized data.*
5. *Backup of the digitized data shall be maintained on another identified system to prevent data loss. The backup shall be taken at the end of every day and shall be done under the supervision of the verification officer.*
6. *Department shall transfer the backup data locally. The backup data shall be checked for data retrieval from a different machine.*
7. *The verification officer shall provide a sign-off against each case file that is digitized.*
8. *Upon completion of the digitization process, the department shall transfer the backup data in an external Hard Disk Drive or DVD for data migration. A copy of the signoff letter shall also be provided to department head.*

Upon completion of digitization process, the data shall be migrated to new systems. A draft guideline for data migration process is mentioned in **Annexure 5** for ready reference. The migrated data would then become available for the classification process and further sharing by the department.

Step 4: Create MoA/ MoU for data sharing with the departments

While considering data classification and subsequent data sharing, it is essential to understand that sharing departments may not always classify the data in the same manner. This may happen due to different legislations and the mandates of different departments and sensitivities of data across them. Therefore, the owner of the information i.e. department, to which data belongs shall preferably sign a MoU/MoA, to document the terms of the arrangement and treatment of the data so that confidentiality is not compromised during the process of sharing. Through these agreements, the necessary importance can be given to avoid data leakages and prevent misuse of information. The MoA/MoU shall cater to the following controls and shall also include the legal processes for sharing the data as well as any issue arising due to non compliance of terms and sharing of agreements.

Control	Description
Physical Storage	Keep classified information in a secured storage area in accordance with the level of protection specified, whether on department premises, in transit, or at off-site locations (e.g., laptops, other location, and backup storage).
Disposal	Dispose any copies of information in accordance with approved procedures designated by the owner of the data and/or the business function, and in compliance with any regulatory requirements pertaining to its disposition. Employ approved procedures or technology that shall erase department proprietary software and owned data files from all storage media before being sold, reassigned, returned to lease company or for warranty replacements, or discarded. Ensure that erased data cannot be recovered.
Release	Do not disclose or release classified material, including any firm, client, or third party information held by or on behalf of department, whether data or applications held on individual equipment, shared equipment or external storage media (e.g., USB devices, external hard drives, tapes cartridges, CD-ROM's) unless there is a 'need to know' and only with specific authorization from the information owner. Do not leave messages containing classified material on unprotected answering machines since unauthorized persons may replay these.
Retention	Classified material shall only be held for the minimum time necessary after which it shall be destroyed or downgraded in accordance with relevant Data Retention policies
Reproduction	Do not reproduce, reprint, disclose, distribute, transmit electronically or remove information unless the owner grants permission in written. The client engagement team shall be contacted to review the terms of engagement with regards to transmission of client information as this may vary and is binding upon the firm to abide by these agreements. Printers must not be left unattended if classified information is being printed or shall soon be printed. Use of outside services for reproduction/printing requires the third party to sign a non-disclosure agreement.
Fax	If faxing private or secret documents, ensure that the recipient is waiting to accept the fax or ensure relevant controls are applied (e.g. encryption). If recipient shall be receiving the fax via email, then the relevant email controls apply for the corresponding data classification level.
Physical Transport	Sending hard copy or electronic media/disks/CDs via mail, courier, hand delivery, or via registered, certified, or recorded delivery requires the sender to determine the most appropriate method based upon the need to ensure delivery and protect information from disclosure. The sender is required to package the media to prevent physical damage or, when applicable, according to the manufacturer's specifications. In exceptional cases, use special controls, such as locked containers, tamper-evident packaging, and separate packaging delivered via different routes or carriers. When applicable and practical, encrypt the data using the most appropriate technique.
Removal	All information developed by or for the firm, or received during one's employment by the firm, remains the property of department and cannot be removed by staff members, consultants, or contractors unless specifically contracted otherwise.

Third party Interactions	Unless it has specifically been designated as unclassified, all departmental internal information must be protected from disclosure to third parties, including outsourcing arrangements. Third parties may be given access to departmental internal information only when a demonstrable need-to-know exists, when such a disclosure has been expressly authorized by the relevant department Information Owner, and with a signed non-disclosure agreement which includes restrictions on the subsequent dissemination and usage of the information.
Unauthorized disclosure	If classified information is lost, is disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, the Information Owner and IT Security Group must both be notified immediately
Classification markings	Classification is to be marked on every page or system.
Classification labels	Labels to be applied to external storage media (e.g. USB devices diskettes, tapes).

The broad level ToC for MoA/MoU shall contain at least (but not limited to):

- *Data sharing mechanism*
- *Terms and conditions of MoA/MoU*
- *Control points (as mentioned above) for data sharing and protection*
- *Frequency of sharing information – Periodic, adhoc etc*
- *Compliance process for protection*
- *Preservation of IPR and data privacy*
- *Obligations of information provider and consumer*
- *Financials for sharing information (in case price is attached to information sharing)*
- *Liquidation damages*
- *Dispute resolution process and arbitration process*

6.4 *"Monitor and Evaluation"*

Step 1: Conduct compliance Reviews

The compliance review is a very important step to identify whether the implementation meets the desired processes and output. The outputs from the compliance review provide the department with decision making capabilities and provide guidance during the implementation stage. The compliance process is required for:

- *Supporting overall governance*
- *Establish link between implementation and strategic vision of the department*
- *Catch errors at early stage*
- *Application of best practices at work*
- *Identify where policy might need modification*
- *Indicate readiness of the project*

Timing:

The compliance review shall be held at appropriate project milestones or checkpoints in the lifecycle of data sharing i.e. during policy formulation, design of checklists and implementation. The review shall be held as soon as practical, at a stage when there is still time to correct any major errors or shortcomings, with the obvious proviso that there needs to have been some significant development in order for there to be something to review.

The following are key steps during each compliance review:

- *Determine scope of review*
- *Schedule compliance review meeting*
- *Analyze filled checklist*
- *Prepare review report and present to the data sharing team*

Dispensation Process:

During a compliance review process, a deviation may be recorded. In this case, either

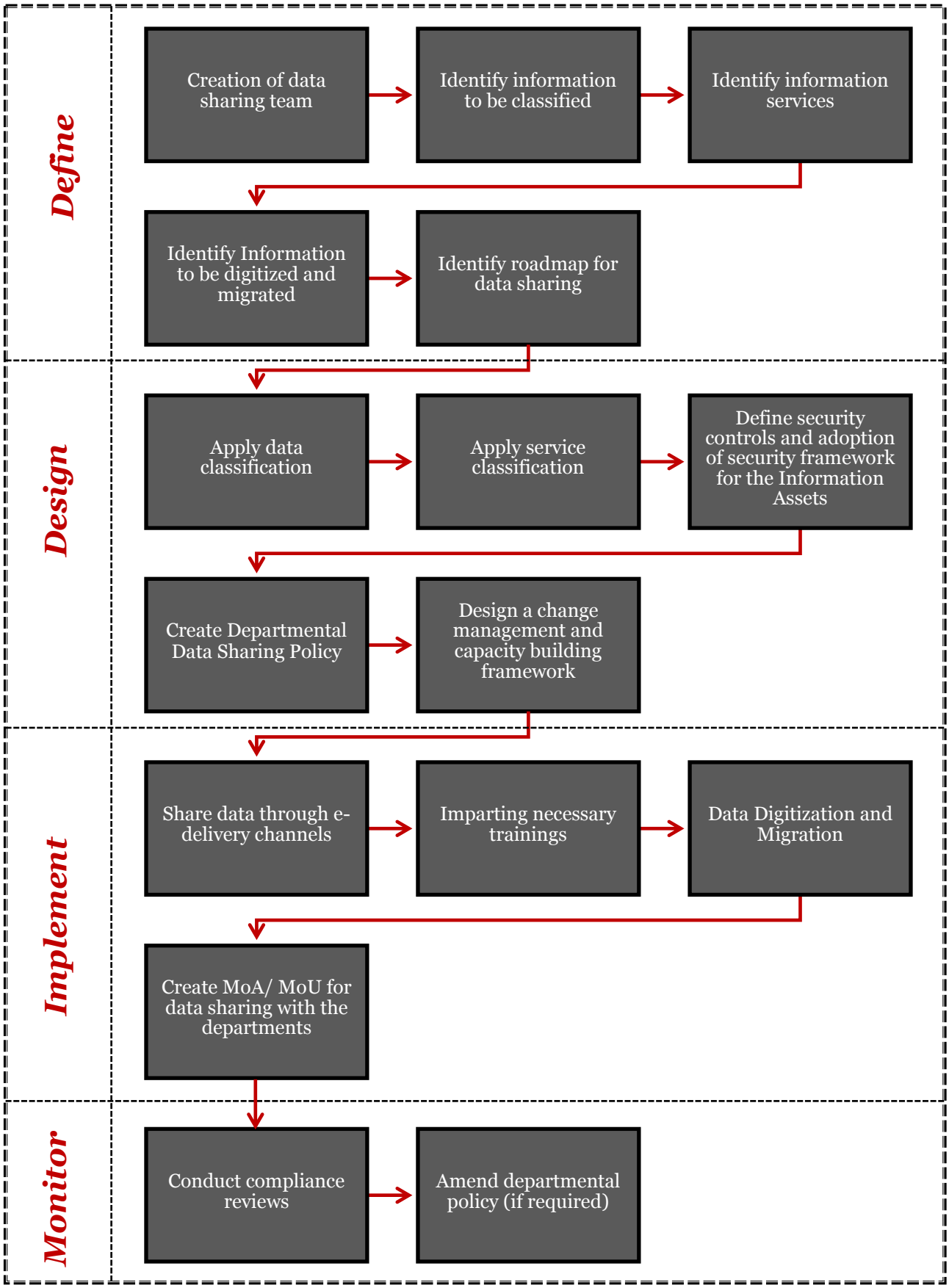
- *Make corrections at appropriate control point or*
- *Request a dispensation*

A dispensation in an alternate route to manage non compliances recoded during the compliance review process. These shall be granted for identified time duration and conditions under which the service shall operate during the lifespan of the dispensation. The dispensations shall not be granted indefinitely, but to provide level of flexibility in implementationand timing. Each of the dispensation shall be presented and approved by the data sharing team.

Step 2: Amend departmental policy(if required)

Based on the feedback and regular updates to the policy and the changing environment, the departmental policy shall be amended from time to time. Alternative the policy shall be reviewed by the data sharing team once every 6 months.

Following diagram summarizes the *Data Sharing Policy Implementation Framework*. This may be used as a reference and a high level guidance to the implementation of the sharing policy.



6.5 Implementation Timeline

Following timelines may be adhered with respect to data sharing:

#	Activity	Time Frame
Stage 1: Define		
1.	Identify Information to be classified	T+1 Months
2.	Identify Information Services	T+2 Months
3.	Identify Information to be digitized and migrated	T+2 Months
4.	Identify roadmap for data sharing	T+2 Months
Stage 2: Design		
5.	Apply Data Classification	T+6 Months
6.	Apply Service Classification	T+8 Months
7.	Define security controls and adoption of security framework	T+8 Months
8.	Create Departmental Data Sharing Policy	T+9 Months
9.	Design a change management & capacity building framework	T+4 Months
Stage 3: Implement		
10.	Share data through departmental websites	T+12 Months
11.	Imparting necessary trainings	T+6 Months onwards
12.	Data Digitization and Migration	T+4 Month onwards
13.	Create MoA and MoU for data sharing with the departments	T+11 Months
Stage: Monitor and Evaluate		
14.	Creation of data sharing team	T+1 Months
15.	Conduct compliance Reviews	Every 2 months or whenever deemed appropriate
16.	Amend departmental policy (if required)	Every 6 months or whenever deemed appropriate

T = Commencement date

7. Way Forward

7. Way Forward

To implement data sharing policy, efforts in right direction need to be taken by ICTA and various other government departments and agencies. This section describes the recommendations for ICTA to support the data sharing initiative.

The recommendations here in this section are done for three broad areas – **People, Process and Technology.**

People

A. Conducting National/Regional Level trainings

To facilitate such large scale national level projects, it is essential to conduct several trainings in area of data and service classification. The departments operate under different levels of maturity and therefore all of them need to be trained on data and service classification process to ensure consistency of the implementation. Therefore, ICTA (or through a representative body) may like to conduct national/regional level training programs to facilitate the building of capacities within the department.

Process

B. Policy on RTI

Data sharing policy recommends guidelines to make all government data easily, freely and uniformly accessible to all. But in order to make governance totally transparent, data sharing must be made a legal obligation for all government departments and agencies. A citizen must have a right, protected by the law of the land, to demand information from government agencies. The law must make it compulsory for government to provide as much information to the public at regular intervals through various means of communication, including internet. Formulation of such a Right to Information Act by Sri Lankan government shall showcase its ultimate commitment towards creation of open Government environment.

C. Data Privacy Policy

The data sharing by practice brings an inherent risk of data privacy for which currently, Sri Lanka does not have any legal policy. In absence of this policy, data which may be deemed public can be shared without enough attention to the data privacy. Therefore it is essential to draft a clear cut policy on data privacy so that a consistent definition of data privacy can be adopted across all departments and used during the process of data and service classification. This shall also help to protect the rights of the individuals and organizations whose data is being shared.

D. Amendments to IT Act

The IT Act of Sri Lanka may be required to be amended to cater to issues related to IPRs, data privacy and implementation plan as mentioned in data sharing policy. The national level policy support is extremely important to facilitate data sharing through accepted delivery channels and well defined processes. A legal team may be deputed along with technical experts and other relevant teams to make necessary amendments to IT Act of Sri Lanka.

E. Facilitate funding support to department for implementation

While ICTA is Nodal Agency for ICT initiatives, such initiatives would require financial support from the Government of Sri Lanka for smooth implementation of this project. The departments may have to provide for investment into People, Process and technology to enable smooth sharing of data and single windows for e-Service delivery. The lack of funding may hamper the department's willingness to scale up and share the data with department and the public.

The policy owner may like to evaluate and finalize a policy decision on who shall bear the cost of development of ecosystem (people, process and technology) for sharing data. Based on the decision, the pricing of the information can be done appropriately. The decision shall also clarify whether the cost shall be borne by the department who would share the data or who consumes it.

Technology

F. Formation of National Data Portal

Considering the fact that every department may not have a fully functional data portal to share its data, a national level portal to meet such needs shall expedite the process of data sharing. An open source data sharing platform is available under the Open Government Platform (OGPL). The platform provides Content management System, Data Management System (DMS) and Visitor Relationship Management (VRM) features along with query visualization and other important features. ICTA may consider the creation of national level data sharing portal and promote that as single place for all government data.

G. Establishment of National/District Data Centers

As mentioned above, the departments may not have provision or capacity to host a self sustained data center where e-delivery channels can be hosted for sharing of information. In this regards, ICTA may facilitate establishment of necessary infrastructure (Data Centers, Disaster recovery, connectivity etc.) to provide hosting services to the various government departments within Sri Lanka.

H. Expansion of datasets available under LIFe

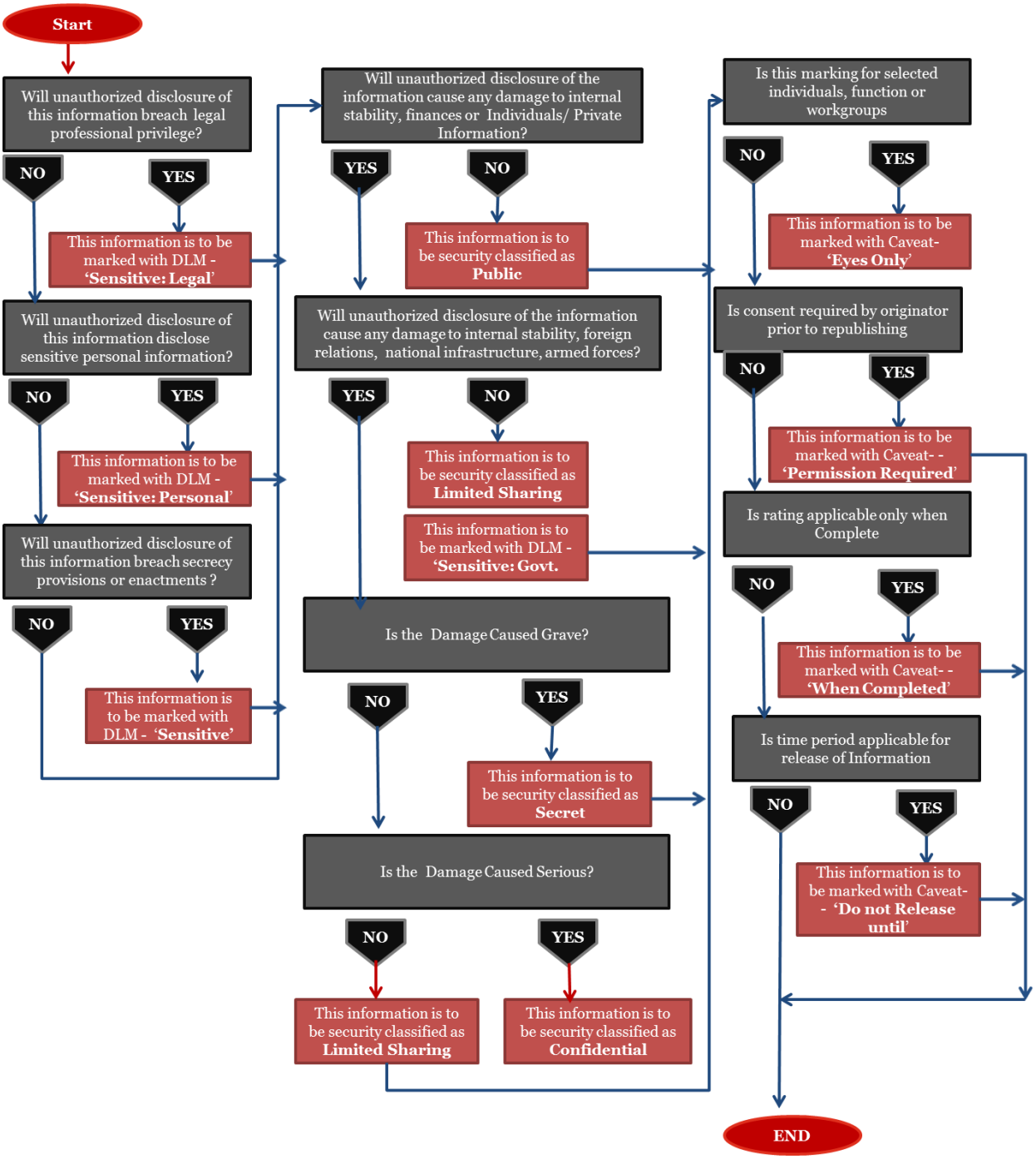
As mentioned above, one of the success factors of the project lies on the interoperability framework used for sharing. In this regards, the Lanka Interoperability Framework (LIFe) has been created and covers following domains:

- *Personal domain – Completed and approved*
- *Project coordination domain – Completed and approved*
- *Land domain – Completed and approved*
- *Vehicle domain– Completed and approved*

To facilitate the data sharing, the number of data sets needs to be enhanced to include more domains. ICTA may like to assume responsibility (directly or through a designated authority) to expand these datasets for departments use a common language for data sharing. In absence of this, real benefits of the program may get limited.

8. Annexures

8.1. Annexure 1: Data Classification Flowchart



8.2. Annexure 2: Data to Service Classification Mapping

Information Classification	Dissemination Limiting Markers and Caveats											
	No DLM or Caveat	No DLM	Se: Private	Se: Legal	Sensitive	Se: Gov	No DLM	Se: Private	Se: Legal	Sensitive	Se: Gov	CAVEAT
Public	x											
Limited Sharing		x	x		x			x	x	x	x	x
Confidential		x	x		x			x	x	x	x	x
Secret							x	x	x	x	x	X
Service classification level	**OPEN**	**AUTHORIZED**					**RESTRICTED**					

8.3. Annexure3: Guidelines for Security Framework

The security of the information systems starts with a strong security policy that defines the freedom of access to information and dictates the deployment of security in the network. The policy shall cover at least:

- **IT Organization -** To ensure that the department has a well-defined Information Technology Function, structured appropriately to enable effective application of IT to business needs, both operational and strategic.
- **Physical and Environmental Security -** To establish adequate measures to prevent unauthorized access, damage and interference to IT assets and services and possible interruption to business activities. The policy consists of physical security, environmental security, power supplies, cabling security, physical security of desktops/ laptops, clear desk and clear screen.
- **Personnel (Human ware) Security -** The objective of personnel security policy is to reduce the risks of human error, theft, fraud or misuse of facilities. The policy consists of Security in job definition, user responsibilities / accountability and Security awareness orientation sessions.
- **Computing Environment Management (CEM) -** The objective of CEM is to develop appropriate operating procedures and incident management procedures. Effective management of the computing environment would ensure the correct & secure operation of information processing facilities. The policy consists of identification of hardware, information handling and security, documented operating procedures, change control, incident management, separate development and operational facilities, security of system documentation, media handling and security, computer virus control, disposal of media, upload anddownload capabilities.
- **Logical Access Controls -** The objective of logical access controls is to control access to computer systems and networks in order to eliminate unauthorized use.The policy consists of user access management, user responsibilities, PC / laptop logical security, emergency procedures / privileged ID's, usage of sensitive system utilities.
- **Network Security-** The objective of network security policy is to ensure the security and continued availability of network facilities and the supporting infrastructure, and their correct and secure operation. The policy consists of network management controls, network devices, remote access and network diagnostic tools.
- **Internet Security -** To define a coherent internet specific information security policy that shall help to protect information systems from attacks through the internet. The policy consists of firewall security, internet use, E-mail security, public web-site security, virtual private network security.
- **Compliance -**The objective of compliance is to ensure compliance to avoid breaches of any criminal and civil law, statutory, regulatory or contractual requirements. The policy consists of Use of unauthorized software, purchasing and regulation of software use and standard version of software.

Note:*The departmental information security policy shall be compliant to IT security policy published by ICTA and is available at ICTA Website.*

The following represents the control points for the preserving the security which shall be customized as per departmental needs.

8.4. Annexure 4: Information asset security classification controls

This section contains summary details of the controls relevant for the various information classification levels.

8.4.1 SECRET

Information assets that require a substantial degree of protection as their compromise could cause serious damage to the Government, commercial entities or members of the public. For instance, compromise could:

- *threaten life directly;*
- *seriously prejudice public order; or*
- *substantially damage government finances or economic and commercial interests.*

The HIGHLY PROTECTED category and the marking should be used sparingly.

Preparation and handling

Markings

Distinct markings on document or information asset. Centre of top and bottom of each page, in capitals, 5mm (20 point) bold and red if possible.

Page numbering

Essential. Numbering should be of the form 'Page n of x' where x is the total number of pages. Copies should be numbered.

Filing

Must be placed in appropriate file without delay. File in distinctive file (RED). Use file reference and folio numbering. Use appropriate file cover sheet.

Electronic information

Prepare in drive or electronic document and records management system with restricted access or on standalone equipment.

Printing

Printer is not to be left unattended while SECRET documents are being printed.

Copying, storage and disposal

Copying

- May be prohibited by information owner.

- To be kept to a minimum in accord with operational requirements.

- Copies should be numbered.

Physical storage

- 'Clear Desk' policy.

- Stored in a vault or safe.

Electronic information storage

Restrict logical access based on need-to-know.

Manual transmission

Within a single location

- Single opaque envelope indicating classification.

- Uncovered by hand directly between authorised members of staff in discrete office environment.

- Must not be left unattended on recipient's desk.

Between locations

- Double enveloping (i.e. sealed inner envelope indicating classification placed within a single opaque outer envelope that does not indicate classification); or

- Single opaque envelope that does indicate classification and secured in a lockable container and delivered by an authorised messenger.

- Receipting required.

Electronic transmission

Data transmission

Basis of 'need-to-know'.May be passed over appropriately classified internal networks.Must be encrypted when being sent between organizations using cryptographic protocols.

eMail

Basis of 'need-to-know'. Email should be the last resort for the distribution of SECRET documents unless the document is separately encrypted to an appropriate standard. Email is to contain the classification in the 'Subject' line. The 'Prevent copying' option in the 'delivery options' is to be checked.

May be passed unencrypted over appropriately classified internal networks.Must be encrypted when being sent between organizations.

Fax

Required that someone attend the receiving facsimile to receive the material, and that receipt or non-receipt of the document is advised. Encrypted communications systems must be used to discuss or transmit SECRET information.

Archive and disposal

In accordance with authorised retention and disposal schedule by department mandate or applicable legislation.

Paper waste - Drafts, working papers and copies must be shredded

Electronic media and equipment - Media to be destroyed or sanitized

8.4.2 CONFIDENTIAL

Information assets whose compromise could cause damage to the Government, commercial entities or members of the public. For instance, compromise could:

- *endanger individuals and private entities;*
- *work substantially against government finances or economic and commercial interests;*
- *substantially undermine the financial viability of major organisations;*
- *impede the investigation or facilitate the commission of serious crime; or*
- *seriously impede the development or operation of major government policies.*

Preparation and handling

Markings

Distinct markings on document or information asset. Centre of top and bottom of each page, in capitals, 5mm (20 point) bold and red if possible.

Page numbering

Desirable.

Filing

File in distinctive file (YELLOW). Use appropriate file cover sheet.

Electronic information

Prepare in drive or electronic document and records management system with restricted access.

Printing

Printer is not to be left unattended while CONFIDENTIAL documents are being printed.

Copying, storage and disposal

Copying

- *May be prohibited by information owner.*
- *To be kept to a minimum in accord with operational requirements.*

Physical storage

- *'Clear Desk' policy.*
- *Stored in a vault or safe.*

Electronic information storage

Restrict logical access based on need-to-know.

Manual transmission

Within a single location

- *Single opaque envelope indicating classification.*
- *Uncovered by hand directly between authorised members of staff in discrete office environment.*
- *Must not be left unattended on recipient's desk.*

Between locations

- *Double enveloping (i.e. sealed inner envelope indicating classification placed within a single opaque outer envelope that does not indicate classification); or*
- *Single opaque envelope that does indicate classification and secured in a lockable container and delivered by an authorised messenger.*
- *Receipting required.*

Electronic transmission

Data transmission

Basis of 'need-to-know'.May be passed over appropriately classified internal networks.Should be encrypted when being sent between organizations.

eMail

May be passed over appropriately classified internal networks.Must be encrypted when sent between organizations.

Fax

Required that someone attend the receiving facsimile to receive the material, and that receipt or non-receipt of the document is advised. Encrypted communications systems must be used to discuss or transmit CONFIDENTIAL information.

Archive and disposal

In accordance with authorised retention and disposal schedule by department mandate or applicable legislation.

Paper waste - Drafts, working papers and copies must be shredded

Electronic media and equipment - Media to be destroyed or sanitised

8.4.3 LIMITED SHARING

Information when compromised may lead to minor probability of causing limited damage to Government, commercial entities or members of the public, including causingminor distress to individuals or private entities.

Preparation and handling

Markings

Not required, though helpful in distinguishing LIMITED SHARING information assets from poorly labelled public information and information that has not been classified.

Page numbering

Optional, but generally helpful.

Filing

File in accord with normal records management practices.

Electronic information

Prepare in drive or electronic document and records management system with restricted access.

Printing

Unless otherwise secured, Printer not to be left unattended.

Copying, storage and disposal

Copying

- *May be prohibited by information owner.*
- *To be kept to a minimum in accord with operational requirements.*

Physical storage

- *'Clear Desk' policy.*
- *Lockable cabinet.*

Electronic information storage

Restrict logical access based on need-to-know.

Manual transmission

Within a single location

- *Single opaque envelope indicating classification.*
- *Uncovered by hand directly between authorised members of staff in discrete office environment.*

Between locations

- *Single opaque envelope that does not indicate classification.*
- *Receipting at discretion of information owner.*
- *Delivered by hand or authorisedmessenger including Sri Lankan Post.*

Electronic transmission

Data transmission

Basis of 'need-to-know'.May be passed over appropriately classified internal networks.Should be encrypted when being sent between organizations using cryptographic protocols.

eMail

Basis of 'need-to-know'.May be passed unencrypted over appropriately classified internal networks.Should be encrypted when sent between organizations.

Fax

Required that someone attend the receiving facsimile to receive the material, and that receipt or non-receipt of document is advised. Encryption desirable but not mandatory.

Archive and disposal

In accordance with authorised retention and disposal schedule by department mandate or applicable legislation.

8.4.4 PUBLIC information

Any information which is easily available to the public, government employees, organizations, regulators, project managers, support staff and contractors including information deemed public by legislation or through a policy of routine disclosure can be classified as "Public". This type of information requires minimal or no protection from disclosure.

Whilst there are no requirements to ensure confidentiality of public information, steps should be taken to ensure that the following attributes of PUBLIC information is maintained with adequate controls:

- ***Integrity**: PUBLIC information should not be tampered with or subject to unauthorized modification.*
- ***Availability**: Public information should be available when needed, thus controls should be in place to ensure continuous availability.*

Preparation and handling

Markings

Not required, though helpful in distinguishing PUBLIC.

Page numbering

Optional, but generally helpful.

Filing

File in accord with normal records management practices.

Electronic information

Prepare in drive or electronic document and records management system with restricted access.

Printing

No special requirements.

Copying, storage and disposal
Copying

To be kept to a minimum in accord with operational requirements.

Physical storage

May be stored in unsecured cupboards or cabinet.

Electronic information storage

- *Common access drive or directory*
- *Restrict logical access based on need-to-know.*

Manual transmission

Within a single location

- *May be passed uncovered by hand.*
- *Passed by internal mail in a use again envelope.*

Between locations

- *Passed by internal mail in a use-gain envelope.*
- *Passed by external mail in an opaque envelope.*

Electronic transmission

Data transmission

Basis of 'need-to-know'.May be passed by data transfer using internal or external networks including the internet with controls to ensure integrity and availability.

eMail

Basis of 'need-to-know'.May be passed by data transfer using internal or external networks including the internet with controls to ensure integrity and availability.

Fax

Public information assets may be passed in the clear (unencrypted).

Archive and disposal

In accordance with authorised retention and disposal schedule by department mandate or applicable legislation.

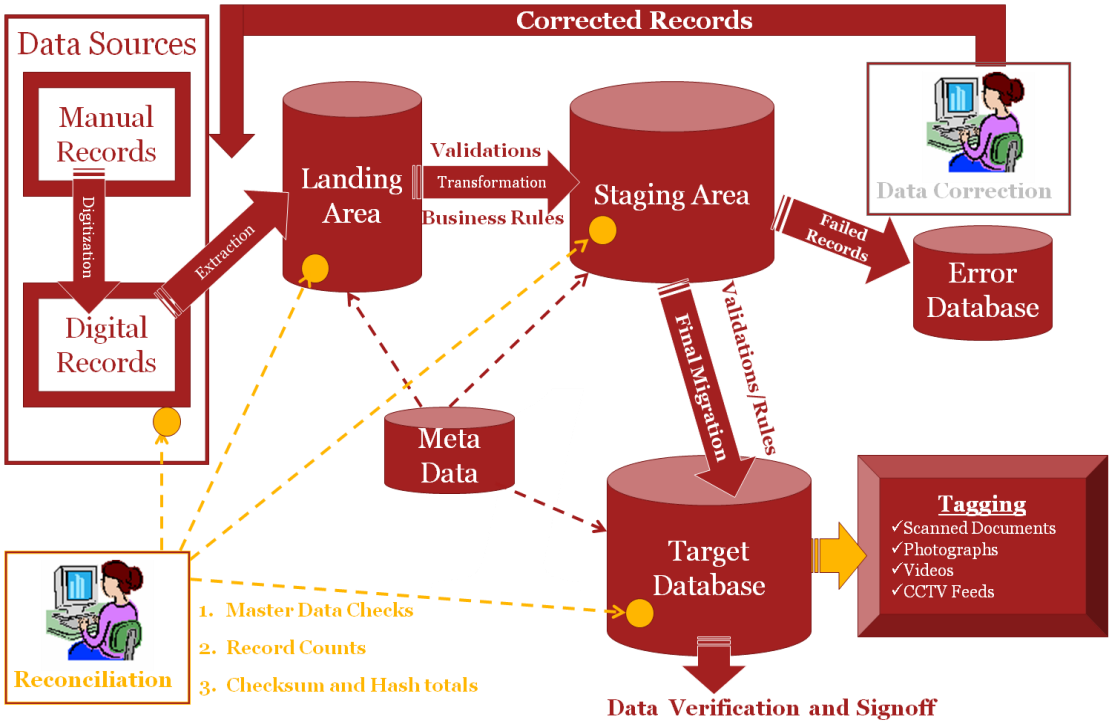
Paper waste - Drafts, working papers and copies may be recycled or may be discarded with general paper waste.

Electronic media and equipment - Media may be reused or disposed of as per paper waste.

Paper waste *- Drafts, working papers and copies may be recycled or shredded*

Electronic media and equipment *- Media may be reused or disposed of using methods equivalent to paper waste advice.*

8.5. Annexure5: Guidelines for Data Migration



A properly defined data migration strategy report shall typically contain

Pre Migration Activities

a. *Migration Plan*
b. *Roles and Responsibilities*
c. *Define set of Activities*
d. *Estimate Time required for migration*
e. *Fallback Plan*
f. *Business Continuity and Downtime planning*
g. *Requisite Software/Hardware for Data Migration*
h. *Data to be migrated*
i. *Data Digitization*
j. *Training/Handholding*
k. *Define Acceptance Criteria*

Migration Activities

a. *Data Quality Assessment and Data Cleansing*
b. *Master Data Migration*
c. *Transaction Data Migration*

Post Migration Activities

a. *Verification*
b. *Error records Handling*
c. *Sign Off*

8.6. Annexure 6: Change Management Framework

Large and complex Information and Communication Technology (ICT) projects should see **vast changes in terms of people, process and technology** which would require a strong inititutional mechanism. The implementation of new solutions and new processes should significantly impact the functioning of departments. One of the major challenges of this initiative would be to **empower and support the workforce in understanding, learning, and adopting the new way of working** to fully realize the potential benefits of this fundamental change.

It is apparent that change management along with capacity building is the need of the hour, and is vital to the success of this project. To manage a large scale implementation, a comprehensive and well-structured change managment framework is required. change management framework would include **paradigms related to change in perception, creating awareness and sensitisation, capacity building and continuous improvement** along with availability of requisite infrastructure and resources to support the entire program

Approach for Designing a Change Management framework

A well-planned and well-designed framework has to be followed to ensure smoother transition of employees and other stakholders into their new roles and to ensure comfort with the new processes and technology. It is necessary to formulate a change management strategy and to plan appropriate interventions for capacity building, training and stakeholder communications at the very onset of the project so as to effectively implement and manage the change.

While conducting the assessment study the department shall prepare a **change readiness questionnaire** to evaluate the needs of the various groups of stakeholders. The data collected during the field study would be **brainstormed and analysed** to understand the need for change and resistance to change. Based on the field study, interviews, current status assessment and To – Be process review, the framework and implementation approach would be designed and recommended. The following steps are required during change management:

- **Phase A: Plan Change**
  - *Defining a plan and implementation of road map;*
  - *Creating a Change Management Institutional structure;*
  - *Identifying Change Catalysts / levers;*
  - *Designing Reward & Recognition Plan;*
  - *Designing Training Content; and*
  - *Designing Communication & Awareness plan.*

- **Phase B: Manage Change**
  - *Conduct Change Management Workshops (National, Regional, District/ Zone level);*
  - *Conducting Trainings;*
  - *Create Communication & Awareness; and*
  - *Manage Change dashboards at State and District levels.*

- **Phase C: Sustain Change**
  - *Performance analysis through periodic examinations, evaluating performance on job, ability to create awareness and motivate team members to sustain the Change Initiative;*
  - *Reward & Recognition Initiatives to sustain change;*
  - *Revaluating Change Readiness; and*
  - *Re-training.*

Approach for capacity building framework

Step 1: Training Needs Assessment and Preparation of Training Plan

The most important activity is to create capacities in the department. For this purpose, a draft training plan prepared at the department shall be executed for completeness and also to ensure that it conforms to the requirements of the project. The Training Needs Assessment Approach at the department level would comprise of the following steps

Stages	Key Activities
Stage 1- Understand Key Business Objectives	▪ **Meet with stakeholders and key project staff to understand the strategic business objectives, vision, strategic goals and plan**
Stage 2- Clarify Competencies	▪ **With the support from various selected representatives within the department, the department shall understand the competencies mapped to each job role through discussions** ▪ **Develop a standard template for use during the requirement analysis.** ▪ **Define the current and future training requirements of staff**
Stage 3- Agree Training Needs	▪ **Department shall assess training requirements (within each role required to meet the competencies defined for that role) and discuss the same with stakeholders and get a concurrence on the same**
Stage 4- Identify Current Provision	▪ **Department shall analyze the training and development programs being undertaken at the national level by any Govt. agencies**
Stage 5 Recommendations	▪ **Produce a final report summarizing:** - **Technical skills, capabilities and knowledge required for each job role mapped to the competencies identified by the department** - **Recommended solutions to meet the training requirements identified**

Step 2: Selection of Change Agent

Department shall identify the group of change agents responsible for initiating and implementing the change management interventions. These change agents shall be trained at the department and shall directly train the personnel at the field level and participate in the awareness and communicate on initiatives, workshops and provide feedback to the department.

Step 3: Communication and Awareness Plan

Developing a comprehensive communication programme would be an important element of approach to managing knowledge and effective participation and knowledge transfer.The objectives of the communication plan would be to:

- *Create awareness about the new system and benefits*
- *Build acceptance and ownership of the system*
- *Manage user expectations and information requirements*
- *Provide information on available support and resources*

Before devising any communication strategy it is important for the process owners to answer the following key questions:

- *Who needs to know about the changes?*
- *What do they need to know about the changes?*
- *When do they need to know about the changes?*
- *How shall the information be communicated?*
- *From whom shall the information be communicated?*

Department shall achieve this by creating a Crisp and Clear communication via various communication options available at the department such as Seminars and workshops, Press/media, Bulletins, briefings, announcements, Audio- Visual Communication, Poster Campaign, Website, E Mail and Social media sites

Step 4: Assessment of Trainings

Department shall **conduct assessment test** to assess the quality of training being imparted and to check the retention level in the minds of the trainees.