Sri Lanka Service Classification Framework (SLSCF)

ICTA
ideas actioned

Document Control

Document Title	Service Classification Framework for Government of Sri Lanka
Abstract	This document provides information on information classification, its use, security and other important related aspects.

Table of contents

1. Terms, Definitions and Abbreviations

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 recognized 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 categorizations 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, analyzed, 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 organization's human resources.*
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. 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.

Terms	Definition
	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 recognized 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 Government 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 organized 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 defense system or acts of foreign interference;* – *Defense plans and operations;* – *International relations, that relate to significant political and economic relations with international organizations 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 public's 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.*

Terms	Definition
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.
Sensitive Information	Information that requires classification, which is Secret, Confidential, or Restricted.
Security Controls	Hardware, procedures, policies and physical safeguards that are put into place to assure the integrity and protection of information and the means of processing and accessing it.
Service owner	The recognized officer who is identified as having the authority and accountability under legislation, regulation or policy, for the delivery of a service on behalf of the Government of Sri Lanka.
Service Classification Register	A register of information about all services both internal and external provided by an organization. For each service, the register holds details including service name, description, classification, owner and related information assets.

List of Abbreviations

Abbreviation	Meaning
A&M	Approach and Methodology
CIA	Confidentiality, Integrity and Availability
FAQ	Frequently Asked Questions
GIC	Government Information Center
GoSL	Government of Sri Lanka
GPR	Government Process Re-engineering
IAR	Information Asset Register
ICT	Information and Communication Technology
ICTA	Information and Communication Technology Agency
IFR	Information Field Register
ISMS	Information Security management System
IT	Information Technology
LIFe	Lanka Interoperability Framework
MoU	Memorandum of Understanding
MoA	Memorandum of Agreement
RFP	Request For Proposal
ToR	Terms of Reference
SLGICF	Sri Lanka Government Information Classification Framework
SLSCF	Sri Lankan Service Classification Framework
SCR	Service Classification Register

2. Background

2. Background

2.1. Project brief

Information and Communication Technology Agency (ICTA) of Sri Lanka is the apex body involved in**ICT policy formulation and direction**for the nation. For providing Government information and services in a citizen friendly manner, it is required to use information and services in an integrated manner. Therefore, a common approach for identifying the sources, owners, level of sensitivity, level of security required of such information and services has to be established.

ICTA had already looked at some aspects of information classification by launching the Lanka Interoperability Framework (LIFe), where it is focused on enabling interoperability. In order to provide integrated information and services to citizens, it is required to identify the intended party or occasion and share such information and services with other Government organizations. Therefore, in the process of integrated electronic service provision, factors such as what information can be shared with whom, in which form should also be considered from an information security perspective.

In order to fulfill the above mentioned requirement, it is required to develop a proper approach and methodology and a set of templates which could be used in classification of Information and Services. A classification of information and services should be derived by considering but not limited to semantics, ownership, process and policies.

This project had been envisaged by ICTA to **formulate framework for Information and service classification** which would be used for **creation of national level policy on data accessibility and sharing.**

2.2. The Sri Lanka Service Classification Framework (SLSCF)

The ensuing pages of this document details the National Service Classification Framework, its use and adoption within government organizations.

This classification framework is based and built upon the *Sri Lankan Government Information Classification Framework (SLGICF)* – a separate document, which should be read in conjunction with the Service Classification Framework to gain a holistic understanding of the Service classification process detailed in this document.

Whilst the Information Classification Framework discusses on the aspects of identification of information assets and their classification, the Service Classification Framework details the identification of services within an organization, the information assets required for service delivery, the controls to be applied for such information assets and the respective classification of services within an organization.

This document supports the implementation Service Classification in Government organizations. It is part of a suite of documents that assist organizations to meet information and service classification requirements.

2.3. Purpose of document

The purpose of this document is to provide a reference framework for services classification for organizations of Government of Sri Lanka. The document attempts to identify various services, related information assets and service level controls to be applied based on the sensitivity of services and information.

The need for having a consistent approach to deal with the sensitivity and confidentiality of information assets shared within services has been kept in perspective while developing this document.

By providing a standard approach to information service classification, the framework facilitates for improved interoperability and consistency of transactions (like information exchange) amongst Sri Lankan Government organizations along with citizen and private organizations.

The following objectives have been considered while preparation of this document:

- Service classification is defined and elaborated;
- A framework for Service classification is presented which would help the organization in:
  - *Distinguishing between different information types available with organization;*
  - *Protection of sensitive informationfrom un-authorized usage and disclosure;*
  - *Protection of liquidation damagesand reputation loss; and*
  - *Preservation of Intellectual propertyof Govt. of Sri Lanka.*
- Help in creation of data access and sharing policyat National Level; and
- Facilitate information sharing across various Government organizations for integrated service delivery.

This document is not a mandatory standard, but rather a guideline for Organizations for classification of Information and data.

2.4. Key stakeholders and audience

Once finalized and approved by the competent authority, it is assumed that this document will be made accessible to Organizations within the Government of Sri Lanka as a reference document. Following is an indicative list of key stakeholders and target audience for this document:

Key stakeholders	Indicative responsibility matrix
ICTA	▪ *Review and finalize the Information and data Classification framework* ▪ *National level service and data sharing policy* ▪ *Guidelines for Information security*
Head of Organizations	▪ *Overall in-charge of Organizational information, data and services* ▪ *Adoption and implementation of Information classification for Organization*
Chief Innovative Officer	▪ *Develop understanding on creation and maintenance of information* ▪ *Identify and mitigate risk related to information mismanagement (leakage, privacy issues etc.)*
Public Relationship Officers	▪ *Understanding of information sharing boundaries, relevant sensitivity of the data and associated risk with privacy*
Program managers for all ICT Initiatives	▪ *Define and maintain Information classification within ICT Projects*
Record Keeping staff	▪ Detailed information on classification, sensitivity, security, risks and management of Information within organization
All external organizations working directly with Government of Sri Lanka	▪ *Understand classification and implement relevant measures to avoid data privacy issues*
All organizational staff	▪ *Understand classification, implications and actions to be taken to prevent misuse of information*
Support desk and GIC Team	▪ *Understand classification, implications and actions to be taken to prevent misuse of information*

2.5. Scope

This document is intended for the use of staff within Sri Lanka Government organizations. It will be of particular relevance to:

- *Service owners and users /editors who are responsible for classification and control of Sri Lanka Government services;*
- *Information owners and users/editors who are responsible for classification and control of Sri Lanka Government information assets;*
- *Information asset custodians;*
- *Individuals who are designing organizational services such as business process specialists, service designers and system architects;*
- *Business managers and service stakeholders;*
- *Information security managers and auditors who may assess the security of services;*
- *Records managers and others who have responsibility for managing classified information assets over time; and*
- *Chief Innovative Officers (CIO) and other ICT managers and staff responsible for the supply and operation of information systems.*

2.6. SLSCF requirements

All organization services both internal and external should be assigned an appropriate classification and associated controls in accordance with the SLSCF, to encourage a consistent approach for cross-organization and inter-governmental information sharing.

This framework requires that organizations must:

- *Determine appropriate service classifications for each service offering both internal and external;*
- *Apply controls to services that reflect their classification levels; and*
- *Keep a register of services offered together with the respective information assets.*

2.7. SLSCF implementation

This framework must be used by all Sri Lanka Government organizations to determine the classification of provided services. Ideally the SLSCF should be applied to all services, and integrated into business processes to best protect information assets used to provide services from unauthorized access, use, modification or destruction while maintaining high levels of performance and interoperability.

It is recognized that implementation of the SLSCF will be progressive in nature. It is therefore recommended that SLSCF be applied in the following order:

- *All new services should be evaluated against SLSCF during their acquisition or creation;*
- *All services involved in existing information transfers either outbound, inbound or within the organization; and*
- *Existing services should be evaluated when process changes occur to the collection or storage of the information, such as during the implementation of a new records or document management process or of a new information system. A particular driver for an implementation or review of services classification would be the implementation of a new process or system which enables the transfer of information beyond an organization's boundaries (for example to another organization or business partner).*

Acknowledging that this framework can appear complex, the relavent experts (SLCERT, internal or external consultants appointed by the government) will assist organizations upon request with the assessment of information assets against this framework.

2.8. Document Structure

In order to present the concepts of Information Classification in an objective and logical flow for better understanding of the reader, the report has been structured in a number of sections and addresses the following key aspects:

- *What, why and how of Service Classification;*
- *Defining service classification levels;*
- *Framework for Service Classification;*
- *Implementation of Service Classification; and*
- *Way forward.*

While different sections of the document would be more useful to different stakeholders, it is suggested that the entire document should be read for complete understanding of the project and intended outcomes. Thereupon, the relevant section may be studied more in details and applied for applicable usage. The rest of the document describes each of the above mentioned points in separate sections.

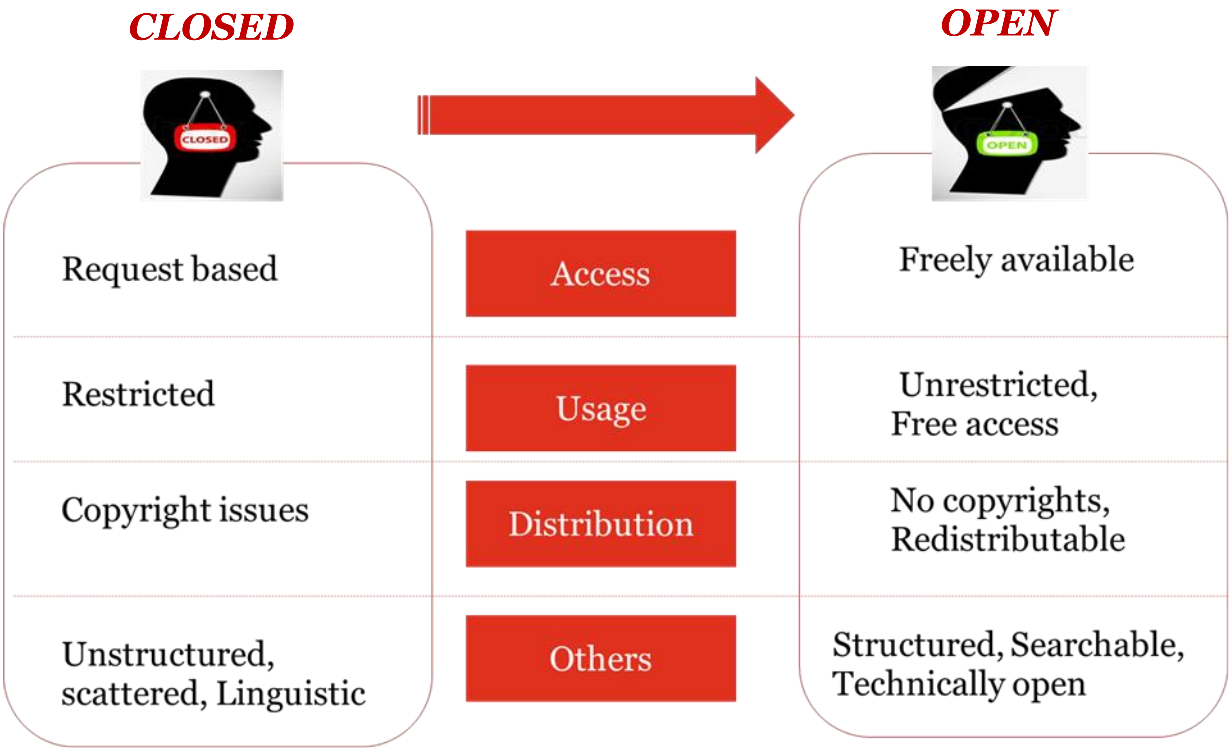
3. Open Government- A new model for governance

3. Open Government – A new model for governance

Open Government”refers to a Governance model where Government transformations are led by effective sharing of information amongst all stakeholders like Organizations and citizens. The current issues with non-sharing of data to public and how they are resolved in Open environment is mentioned below:

Issue	Resolution in Open Government model
Lack of awareness	Effective sharing of information creates awareness and educating organization and citizens
Lack of time bound services	Easy tracking of services by citizens and organizations and empowering them to seek penalties for non-compliance of time bound services
Limited accountability and supervision	Time bound services and transparency leads to higher accountability within the government
Delayed redressal of grievance	Open data would lead to faster closure of service request and public grievances based on time bound services and higher accountability

Open Government is closely linked with Open Data model which promotes sharing of data with everyone with minimum restrictions and is explained with the help of following diagram.



CLOSED		OPEN
Request based	Access	Freely available
Restricted	Usage	Unrestricted, Free access
Copyright issues	Distribution	No copyrights, Redistributable
Unstructured, scattered, Linguistic	Others	Structured, Searchable, Technically open

3.1. Open Data Benefits

A. Benefits to citizens

- *Transparency into Government functioning;*
- *Better decision support system based on informed decisions;*
- *Promote time bound services to citizens; and*
- *Social governance of Government.*

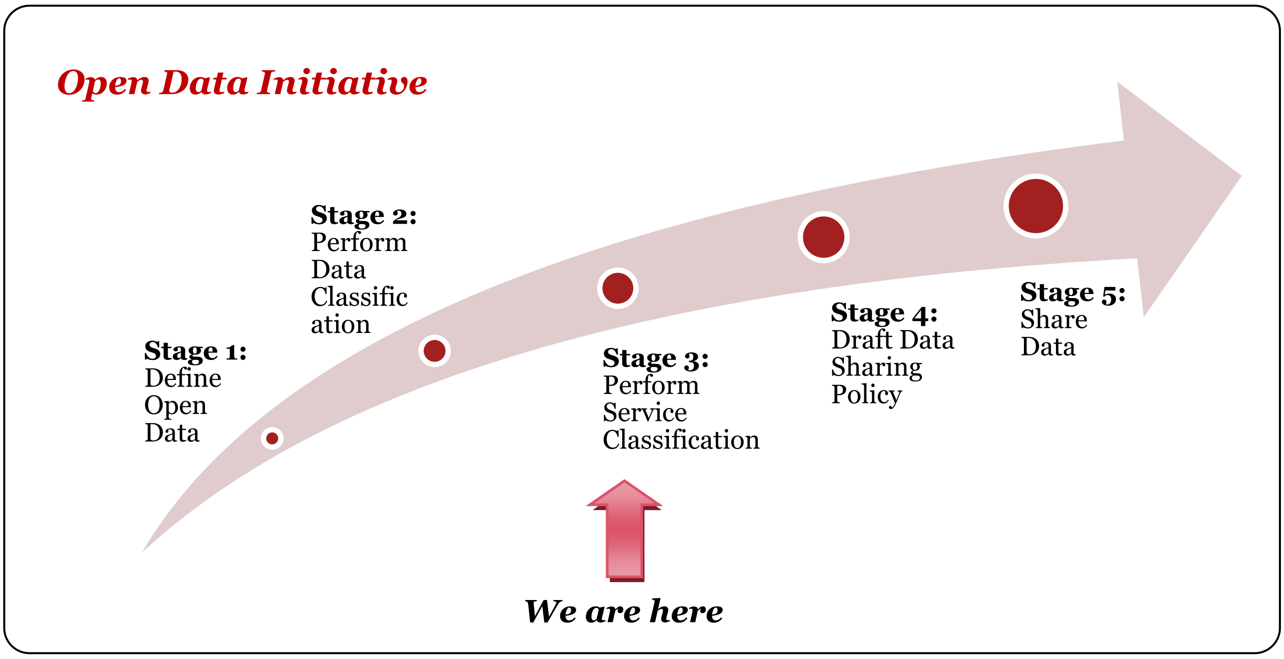
B. Benefits to Government of Sri Lanka

- *Key driver for economic growth;*
- *Impetus for higher accountability;*
- *Participation and collaboration with citizens; and*
- *Reduced trust deficit and enhanced relationship between citizens and Government.*

C. Benefits to Organizations

- *Reduced queries from other organizations/citizens;*
- *Information reuse as organizations will not be required to create data which is already available by other organization and available in public domain;*
- *Reduce malpractices within organization due to information awareness;*
- *Impetus for higher accountability;*
- *Streamlining organization's information gathering and processing procedures; and*
- *A mechanism to identify incorrect and outdated data.*

3.2. Service Classification – Step towards Open Data in Sri Lanka



Open Data Initiative

Stage 1: Define Open Data

Stage 2: Perform Data Classific ation

Stage 3: Perform Service Classification

Stage 4: Draft Data Sharing Policy

Stage 5: Share Data

We are here

Stage 1: Define Open Data – This is the first stage where all the data which needs to be opened is required to be identified.

Stage 2: Perform Data Classification – Once the data has been defined, proper classification based on the impact of the sharing of information has to be assessed. This document presents an indicativeand reference framework for assessing the impact of information sharing. The organizationcan use this framework and perform assessment on the currently available data. Based on the impact and findings, appropriate controls would have to be identified.

Stage 3:Perform Service Classification – Service delivery mostly involves sharing of information in one form or other. Hence it is only logical to state that service classification framework must evolve from information/ data classification framework.The security classification assigned to a service must be same as the highest security classification of the data being shared or transferred during the course of service delivery.

Stage 4: Draft Data Sharing Policy – A data sharing policy would be drafted based on the inputs from both information and service classification frameworks to facilitate data sharing among government organizations. It is expected that the policy would cover controls for – *People, Process and Technology.*

Stage 5: Share Data and feedback loop – The next step of the journey provides provisions for sharing of data and mechanism for feedback for improvement of the system.

Objective:This document would primarily focus on Stage 3while providing basis for Stage 4 and 5

4. Basics of Service Classification Framework

4. Basics of Service Classification Framework

4.1. What is Service Classification

Sri Lanka Government services are business offerings that deliver value to or enable outcomes for its clients. Each organization will have a number of business services that are delivered to consumers. Consumers may be its constituents (citizens), or they may be other organizations that deliver services to constituents.

The Services Classification Framework provides a consistent, logical and comprehensive view of all Sri Lanka Government services, independent of the physical departments and other entities that make up the Sri Lanka Government.

For the purpose of this framework, 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 system encompassing principles, methodology, tools and framework for designating different categories to Services based on their transactional nature andthe impact and value of the information assets that are used in the delivery of a particular service.

The following guiding principles help elaborate the definition of "What is Service Classification":

- *It applies to all services across the organization (both internal and external services);*
- *It provides basis for data sharing and accessibility policies across organization;*
- *The classification should be done according to sensitivity and value of the information (but not limited to);*
- *The framework should be simple to understand and administrator;*
- *The value of information changes with time, regulatory requirements and changing business environment;*
- *The classification should not be dependent or open to interpretation by different people; but rather a set of governing rules;*
- *The service classification should include extended organization - department, business partners, contractors, other organizations and citizens;*
- *Classification is not ownership of single individuals and impacts everyone; and*
- *The classification rules are dynamic and needs constant upgrade.*

4.2. Why Service Classification is required

Identification and classification of services primarily enable the delivery of government programs and services, whilst making sure such services are simple, seamless and connected. The Sri Lanka Service Classification Framework (SLSCF) provides a guide and a consistent approach to assist organizations in making the transition to connected and shared modes of operation.

Apart from promoting Open Government and Open Data models, SLSCFwill also help with the following:

- **Formation of National Level Data Sharing Policy –** Based on the data classification, a national level data sharing policy can be defined through which relevant information assets may be shared within and outside the Government.
- **Integration with LIFe (Lanka Interoperability Framework) –** LIFe is an interoperability framework defined by ICTA which governs the mechanism for data sharing across governmental organizations. The framework aims to provide an integrated platform for sharing of data, for which it is extremely essential to classify data in appropriate category. Therefore it is essential that a policy is laid down for all organizations to establish a common language for Information Classification.
- **Creation of Integrated e-Service delivery –**ICTAaims towards an implementation of 'e-Sri Lanka', through which an enabling environment would be created, where multiple stakeholder partnerships would be developed between public sector, private sector and civil society, to 'take the dividends of ICT to every village, to every citizen, to every business and to transform the way government thinks and works'. One of the key success factors to this enablement is presence of integrated service delivery platform which cannot be achieved without sharing of information based on appropriate classification.
- **Apply Security Policies–**In today's world safety of information- organizational and citizen data is extremely important. The loss of data or sharing can lead to legal issues, reputation damages and lack of trust within the citizens. Therefore, it is important to classify data based on different attributes to ensure its safety.It is expected that different types of information should be only available to authorized people. With information classification, the information can be assessed in terms of sensitivity and managed– Protection, Retention, Transmission and Integrity.
- **Supporting routine disclosure and active dissemination –** Once the data classification is done, the various organization and citizens can easily share the data based on data sharing policy. The key ingredient to data sharing policy is ability of classify the data according to various factors.

4.3. Who can assign Service Classification

Each organization is responsible for ensuring that all services – both internal and external – are classified by the defined service owner within the organization.

In case of information assets that are externally generated, and not otherwise classified, the organizational officer who receives them should ensure that an owner and custodian are assigned, and the relevant classification of the asset is determined*(please refer the SLGICF for detailed steps in carrying out information asset classification).*

Subsequently, the service owner should identify all information assets used in the service delivery including information assets of other organizations. Using this document the service owner is responsible for determining the classification level of the particular service according to the guidelines of the SLSCF. Once a service is classified, all information regarding the service should be documented in the Service Classification Register.

5. The classification system

5. The classification system

This section outlines the system to be used for classification of services within the Sri Lanka Government. When providing services, it is essential that every department is aware of the following key aspects of service delivery:

- *Nature of services that an organization provides, including:*
  - *Government to Government;*
  - *Government to Citizen;*
  - *Government to Business;*
- *Types of Services that an organization provides, including:*
  - *Over the counter;*
  - *Online;*
  - *Informational;*
  - *Verification;*
- *Identification of internal services within the department;*
- *Identifying services provided to customers (other government entities, private organizations or citizens)*
- *Identifying external information required to provide services;*
- *Information that is obtained, processed and given out within a service;*
- *Information assets within a service must be handled with due care and in accordance with authorized procedures;*
- *Information within a particular service must be made available only to people who have a legitimate 'need-to-know' to fulfill their official duties or contractual responsibilities; and*
- *Information within a service must only be released in accordance with the policies, legislative requirements and directives of the Government and the courts.*

Information assets typically fall into three broad categories:

- *Information intended for public use/consumption;*
- *Routine information without special sensitivity or handling requirements; and*
- *Information which, because of the adverse consequences of unauthorized disclosure, or legislative obligations requires additional controls to protect its confidentiality and meet handling requirements.*

5.1. Sri Lanka Service Classification Framework (SLSCF)

The SLSCF provides a basis to classify a particular service based on the transactional nature of the service and the sensitivity of information that the service requires in its delivery. Thus, a service is classified taking to consideration the impact or consequence of unauthorized disclosure of information within the service.

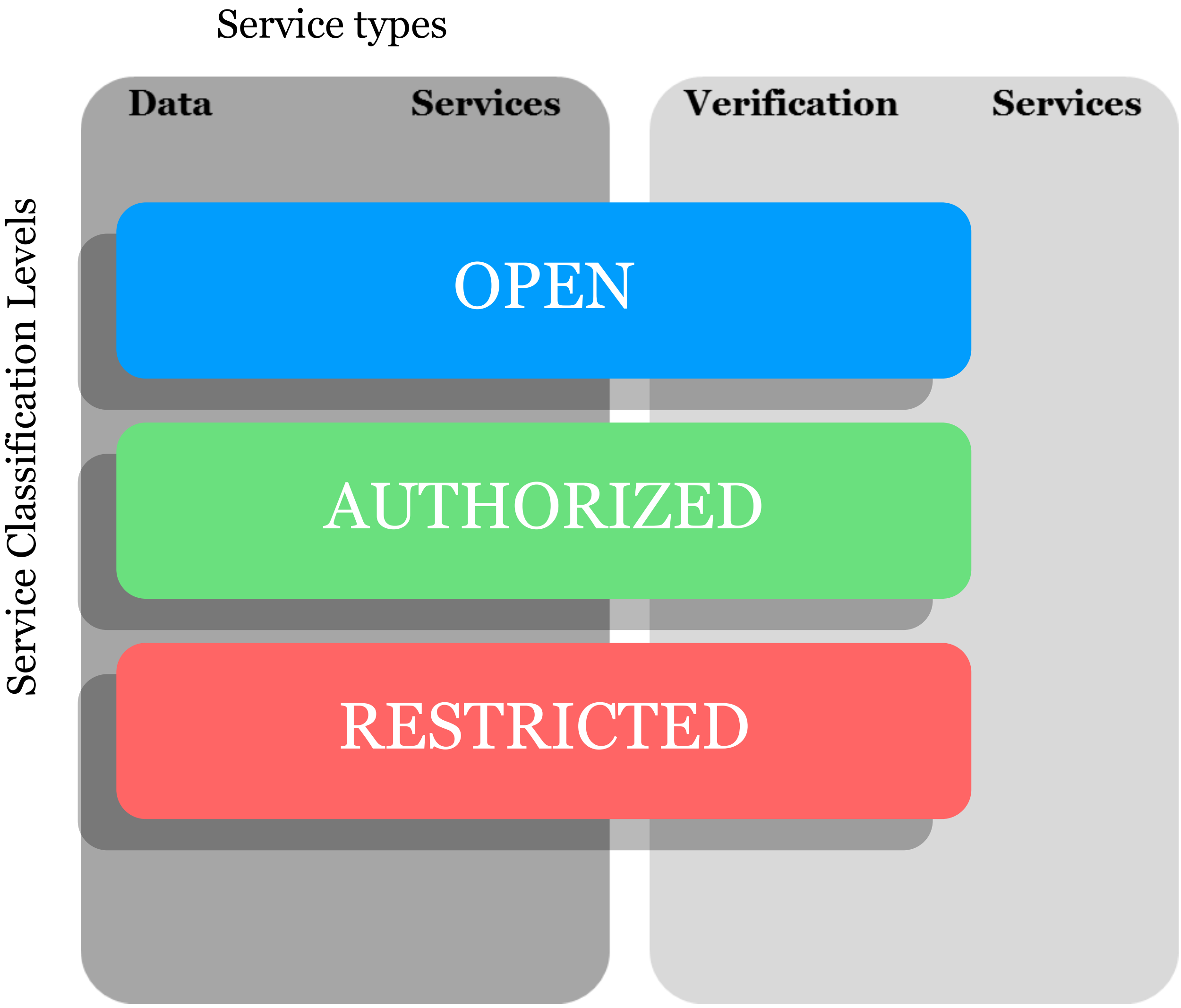
Classification of the data being shared or transferred during serviced delivery has a bearing on the service classification of the service. In other words data classification is a stepping stone inclassifying a service. The classified data can be logically grouped into data sets. These data sets will be assigned the highest security classification of the individual data elements that is part of the data sets.Based on the data sets that are being shared during service delivery, the services can be classified with the highest security classification of the data sets that are being shared.

Classification model adapted for Sri Lanka has the following elements:

1. ***Service Classification Levels***–*Service classification represents sharability and sensitivity rating (or security rating) that must be applied to the service.*

2. ***Service Type*** – *Service type supplement the service classification system for identifying the transactional nature of the service.*

The diagram below represents Sri Lanka Service Classification Framework; details of each of elements are described in sections below:



5.1.1. Levels of Service Classification

Broadly, threelevels service classification have been defined as part of the Service Classification framework including “Open”, “Authorized” and “Restricted”.The “Service Type”should also be at all times accompany a respective service classification level in order to ensure correct handling and an easy appreciation of the ‘need to know’ requirement of information shared within the service.

A. Open

Any service which is easily available to the public, Government employees, organizations, regulators, project managers, support staff and contractors which includes information deemed public by legislation or through a policy of routine disclosure can be classified as **“Open”**.

This type of services contains information that requires minimal or no protection from disclosure.

Examples of Openservices include:

- *Information hosted on a public website including organization contact persons;*
- *Weather Information;*
- *Organization processes and information;*
- *Crime statistics; and*
- *Agriculture information services.*

B. Authorized

Services classified as **“Authorized”**are services which require a formal agreement between organizations (both internal and external) for data sharing when providing the service. Authorized services would entail input, processing or output of either a singular or multiple information fields classified at “Limited Sharing” or higher.

In the case of services classified ‘Authorized’, information within such services are subject to the disclosure of which may be limited or prohibited.

Examples of Authorized services are:

- *Status check of service delivery;*
- *Health benefit programs;*
- *Driving License verification;*
- *Employee Provident Fund services; and*
- *Verification of NIC number.*

C. Restricted

Services which are classified **“Restricted”**requires explicit approval and authorization when providing such services. Sharing of information that are classified as either “Confidential” or “Secret” would form a basis for a service to be classified as Restricted.

Unauthorized disclosure of information within a restricted service could cause serious damage to national security, Government, nationally important economic and commercial interests or threaten life. It could also raise international tension and seriously damage relations with other governments, shut down or substantially disrupt significant national infrastructure and seriously damage the internal stability of Sri Lanka or other countries.

Examples of Restricted services are:

- *Personal case files such as benefits, program files or personnel files;*
- *Tax returns or financial health of organization;*
- *Sharing of personal health information of individual;*
- *Land information;*
- *Trade secrets; and*
- *Salary information.*

5.1.2. Service Types

Service types supplement the Service classification levels by enabling an organization to establish the service output which a service would provide. Service types are applicable for both services provided internally such as HR services and external services to customers including citizens, other government organizations and private entities.

Broadly two types of services are provided by an organization, namely:

A. Data services; and
B. Verification services.

A. Data Services

When all or part (specific)information within a service is shared as a service output, such services are defined as "Data Services". Most key services provided by an organization would be categorized as Data Services as in most cases the service output would provide part or complete information.

For example:

- *Status check of service delivery;*
- *Health benefit programs;*
- *Driving License verification;*
- *Employee Provident Fund services; and*
- *Verification of NIC number.*
- *Personal case files such as benefits, program files or personnel files;*
- *Tax returns or financial health of organization;*
- *Sharing of personal health information of individual;*
- *Land information;*
- *Trade secrets; and*
- *Salary information.*

B. Verification Services

This service type is applied when the service output is of verification nature only. For example the output may be *"Yes or No"* to an inquiry made. **"Verification Service"** is used when none of the actual information used within the service is provided as output.

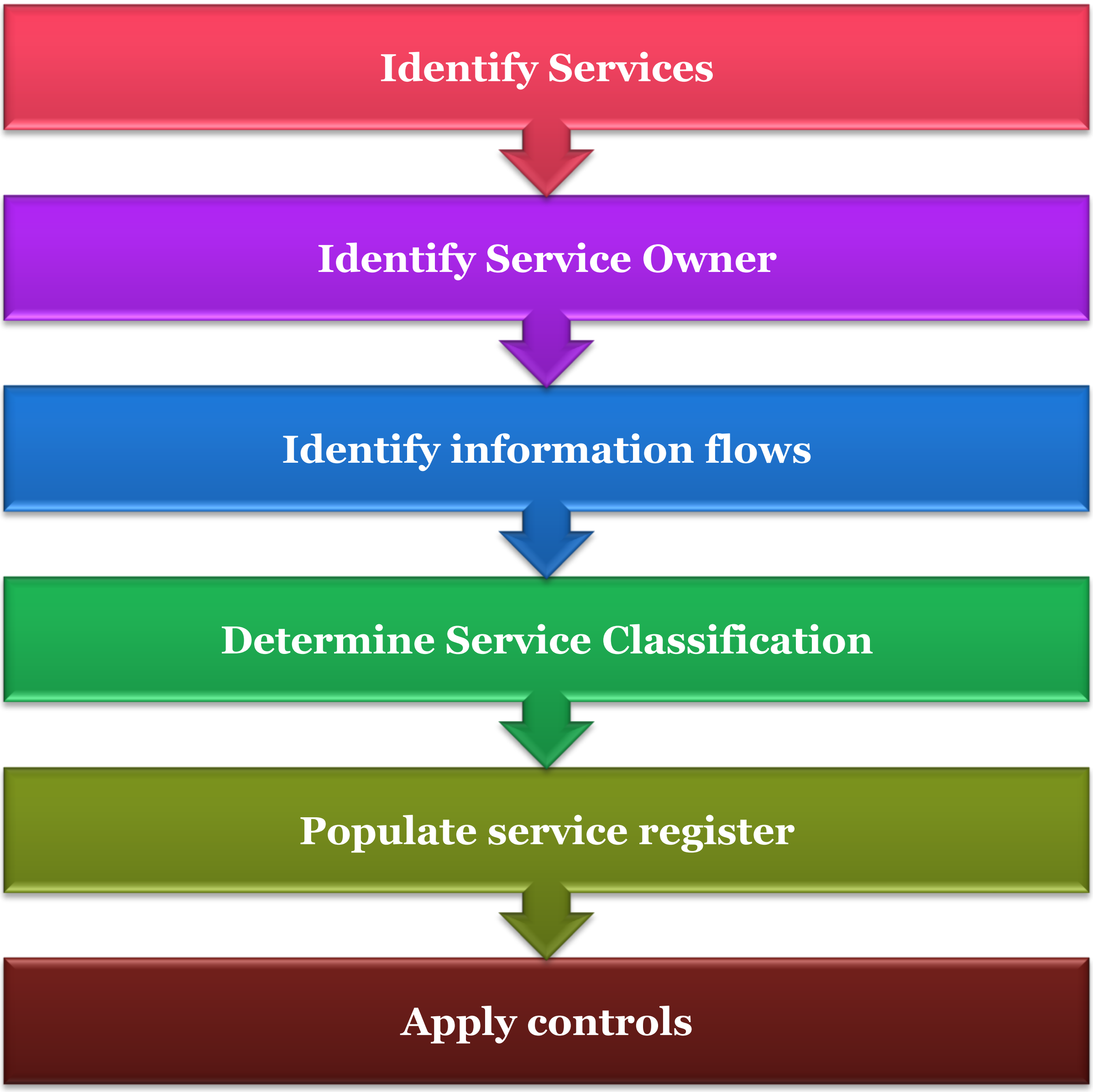
For example:

- *Confirmation of NIC number;*
- *Confirmation of Driving License number;*
- *Background verification; and*
- *Passport verification.*

6. The service classification process

6. The service classification process

This section provides detail on the service classification process, which is described diagrammatically below. Each of the steps identified in the diagram below is expanded in more detail in the following sub-sections.



Identify Services

Identify Service Owner

Identify information flows

Determine Service Classification

Populate service register

Apply controls

6.1. Identify services

Services are defined as an identifiable collection of information assets, which deliver value to consumers by facilitating outcomes consumers want to achieve. Service delivery enables an organization to perform its business functions, thereby satisfying a recognized organization requirement.

Examples of services include, but are not limited to:

- *Internal services*
  - *Human Resources*
  - *Finance*
  - *Administration*

- *External services*
  - *Citizen services*
  - *Other Governmental organizations*
  - *Private organizations*

6.2. Identify the service owner

Each organization is responsible for ensuring that all services have a classification that is authorized by the service owner, and that a custodian who is responsible for implementing and maintaining classified information assets within the service according to the rules set by the owner.

The service owner is responsible in identifying information flows including dependencies from other organizations in providing the service. Also, taking to consideration the information assets and their respective information classification levels used within the service, the service owner should use this framework in classifying the service.

6.3. Identify information flows

In order to establish the correct service classification for a service, all information inputs and outputs must be identified. Information assets that are used both at input stage and output stage of the service must be identified with the respective information classification of the information asset and documented in the ***Service Classification Register (SCR)***.

When information assets from other government or private organizations are required, such information assets should also be identified along with their respective classification levels. The final service outcome or the value that is created for the consumer is the output of a particular service. Therefore, all information assets and their respective information classifications that are used in the final service delivery should also be identified.

In the event a new information asset *(collection of information fields, which have not yet been classified as an asset)* is to be created as the final service output, the following process should be conducted:

- Identify the information fields that constitute the final service output;
- Through the use of the Sri Lanka Government Information Classification Framework (SLGICF), classify the information fields;
- Using SLGICF, group the collection of classified information fields as an Information Asset and derive the classification level for the particular information asset;
- Update both the IFR and IAR as necessary; and
- Update SCR with the new information asset and its classification level.

6.4. Determine the service classification

Subsequent to the identification of all information assets used at both input and output of the service, the highest classified information asset along with any limitations on dissemination should be identified.

The highest identified information classification level and any respective DLMs or Caveats should be applied to the following table to derive the Service classification of the particular service.

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**					

Note: For the following information asset classifications, the service owner is responsible for choosing the most appropriate Service classification level based on the context of the service and related information assets:

- *Limited sharing with Sensitive DLM*
- *Limited sharing with Sensitive: Private DLM*
- *Confidential with Sensitive DLM*
- *Confidential with Sensitive: Private DLM*

For all other information classification levels the table above provides a specific correlation to the selection of the appropriate service classification level.

6.5. Populate the Service Classification Register (SCR)

Organizations should establish and maintain an SCR to record the classification of services and their related information assets used in the service delivery. The SCR will ideally be maintained in a central location and should cover all services of an organization, thus be readily accessed and referred to by the service owners and other users.

At a minimum, the SCR should include:

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

6.6. Apply controls

Appropriate controls must be appliedto commensurate the defined service classification level, 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.

Controls to be applied for each service classification level are outlined in the document ***"Data Sharing Policy"***.

6.7. Ongoing activities

6.7.1. Education and awareness

The ongoing education and awareness of all employees in the importance of security classifying information, is critical to the success of the overall organization security environment and service classification objectives. Organizations should ensure that all employees have a clear understanding of the service classification framework and the information security classification framework, their responsibilities, and the NEED-TO-KNOW principle. Employees who create, process or handle security classified information assets within a service should be trained in how to handle such classified information.

Education and awareness programs will likely vary across an organization and between organizations and depend on the type of work and types of services and related information assets dealt with. For example, where staff is not expected to deal with a RESTRICTED service, training can concentrate on general awareness and the controls and processes surrounding the handling of information assets related to services classified PUBLIC or AUTHORIZED and how to obtain assistance if they do need to handle other classification levels.

6.7.2. Maintain services classification register – continuous review

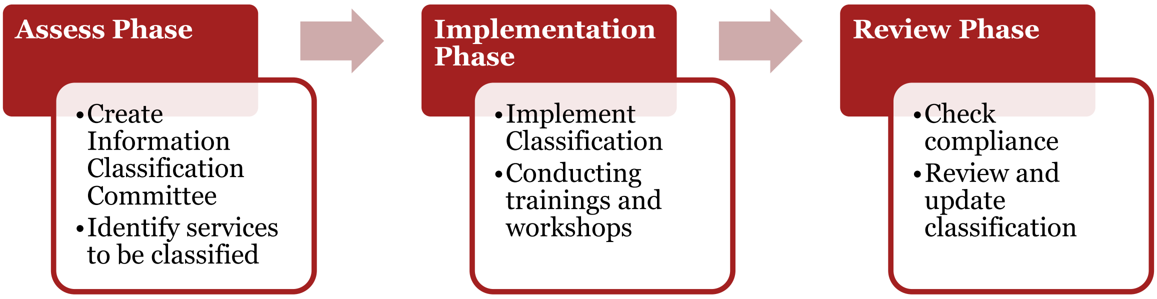
As environments and circumstances change, information asset owners would review security classifications to ensure that the protection being afforded is cost-effective and commensurate with the level of risk.

As detailed in the SLGICF, security classification makes information assets more expensive to handle, store and transfer, so it is important to ensure the information security classification is appropriate. Thus may require de-classifying information assets that are no longer sensitive, or increasing the classification where the consequence of compromise has changed.

Service owners should use the SCR to annually review the classification levels of information assets that are included in the delivery of the service, and update the service classification level accordingly.

7. How to implement Information Classification

7.How to implement Service Classification


Assess Phase
•Create Information Classification Committee
•Identify services to be classified
Implementation Phase
•Implement Classification
•Conducting trainings and workshops
Review Phase
•Check compliance
•Review and update classification

Stage 1: Assess Phase

This is the first stage in the implementation of service classification and starts with mobilization of the Information Classification Committee *(as Classification of a service is based on the classification of information assets as per SLGICF, the committee defined in SLGICF is referred for easy adoption)*.This committee will be responsible for end to end implementation of Service classification and relevant areas. Suggested team members along with their key roles and responsibilities have been identified and detailed in sections below. This phase also establishes and identifies the services to be classified.

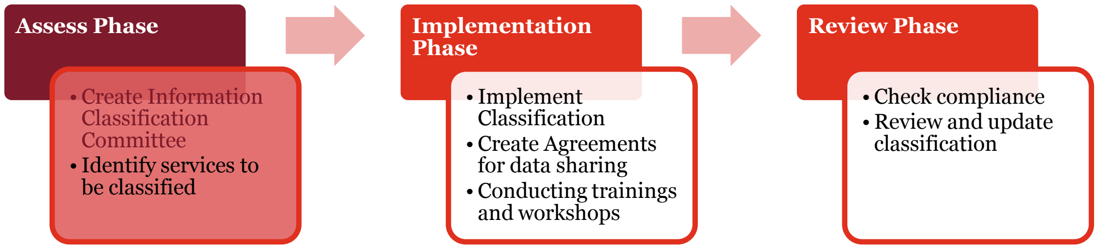
Stage 2: Implementation Phase

Once the services have been identified for classification, the classification process is applied to obtain the right classification. To support the larger cause of the project, this stage also deals with provision of training to all staff members and other key persons for better system acceptance of the information and service classification process.

Stage 3: Review Phase

In this stage, the objectives of the engagement i.e. Service Classification implementation are verified through regular checks. Based on the checks and feedbacks, the information classification policy may be revised. The changes will have to be applied again through the same process through which classification was done earlier.

7.1. Phase 1: Assess Information Classification



Assess Phase

- Create Information Classification Committee
- Identify services to be classified

Implementation Phase

- Implement Classification
- Create Agreements for data sharing
- Conducting trainings and workshops

Review Phase

- Check compliance
- Review and update classification

7.1.1. Mobilize Information Classification Committee

The same committee established for Information Classification within the organization has been adopted to drive the Service classification initiatives within the organization. Given that both information classification and service classification go hand in hand, it is only logical that the same committee made responsible for service classification.

Additional members to the Information Classification Committee are mentioned in **Bold**below:

- *Head of organization and (or) ministry;*
- *Chief Innovative Officer of the organization;*
- *Public Relationship Officers;*
- *Programme managers for all IT Initiatives;*
- *Record Keeping staff;*
- ***Service heads**; and*
- ***Department heads**.*

Recommended Terms of Reference (ToR) for this committee would be as follows (additional points for service classification are mentioned in **Bold**):

- *Define organizational specific Information Classification Policy based on generic policy defined by ICTA;*
- *Define inventory of information assets to be classified;*
- *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 stakeholders 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;*
- ***Define inventory of services to be classified**; and*
- ***Define appropriate controls based on service classification**.*

7.1.2. Identify Services to be classified

The classification process is required to be undertaken for all services below (but not limited to):

Internal Services

- *Departmental budgets;*
- *Legal services;*
- *Human Resources; and*
- *Finance and operational services.*

External Services

- *Government to Government*
  - *Passport verification;*
  - *NIC verification;*
  - *List of offenders; and*
  - *Legal services to other departments.*

- *Government to Citizen*
  - *NIC Issuance;*
  - *Driving License Issuance;*
  - *Weather information; and*
  - *Granting of Deeds.*

- *Government to Private organizations*
  - *Verification services to Banks;*
  - *Tenders;*
  - *Employee verification; and*
  - *Employee Provident Fund services.*

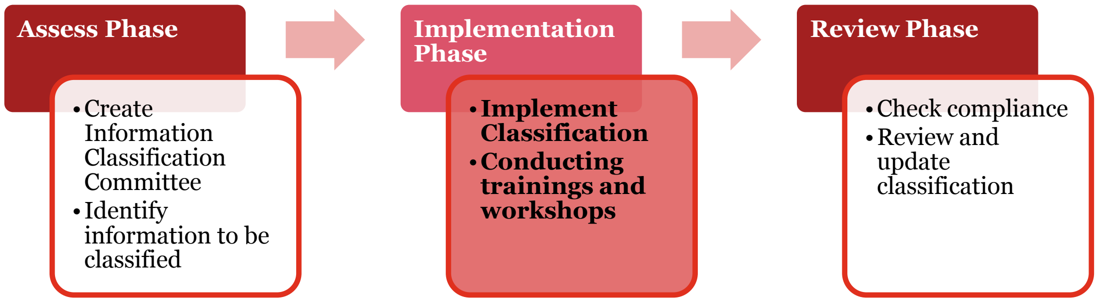
Data Services

- *Status check of service delivery;*
- *Health benefit programs;*
- *Driving License verification;*
- *Employee Provident Fund services; and*
- *Verification of NIC number.*
- *Personal case files such as benefits, program files or personnel files;*
- *Tax returns or financial health of organization;*
- *Sharing of personal health information of individual;*
- *Land information;*
- *Trade secrets; and*
- *Salary information.*

Verification Services

- *Confirmation of NIC number;*
- *Confirmation of Driving License number;*
- *Background verification; and*
- *Passport verification*

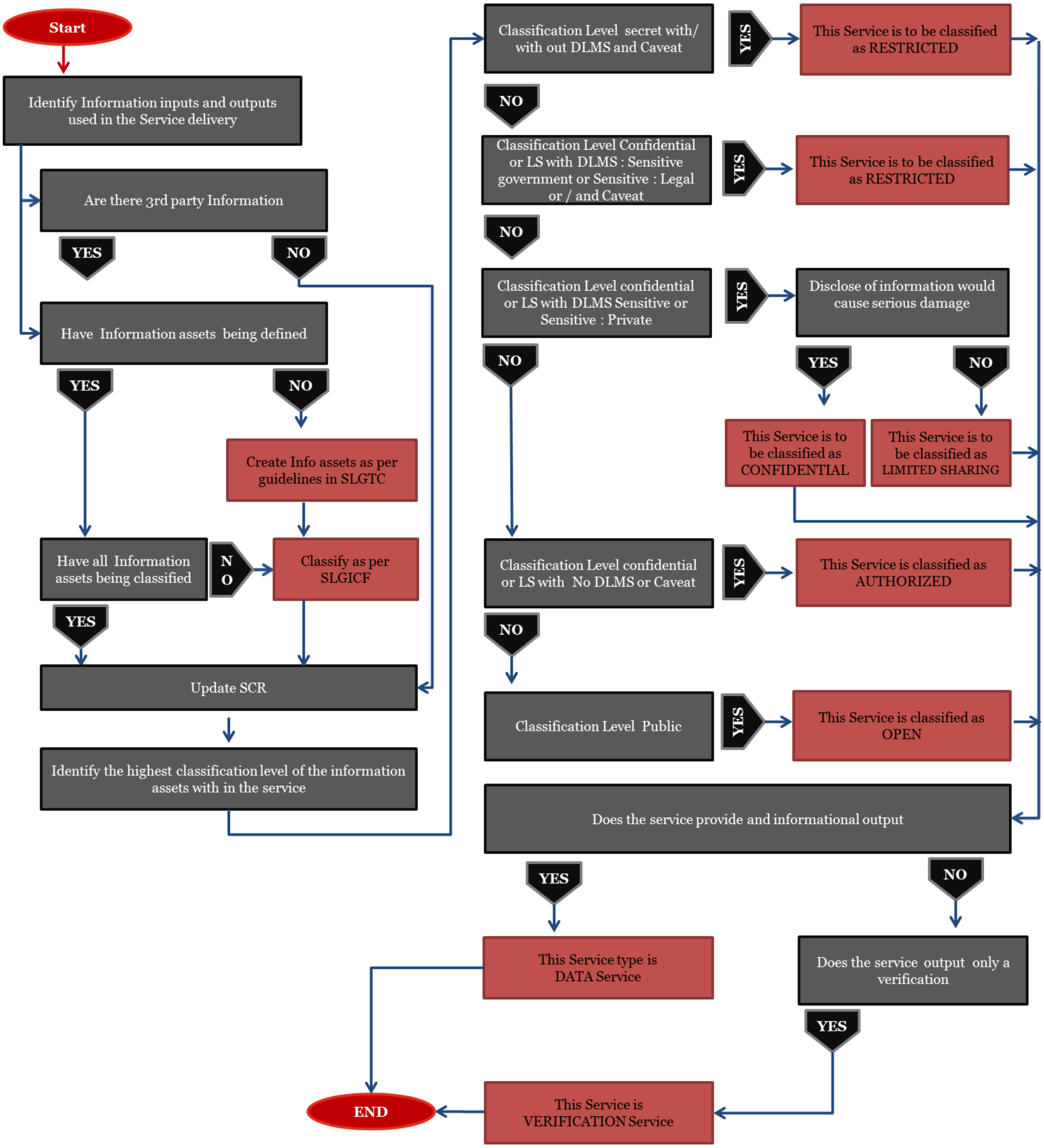
7.2. Phase 2: Implementation Phase


Assess Phase
• Create Information Classification Committee
• Identify information to be classified
Implementation Phase
• Implement Classification
• Conducting trainings and workshops
Review Phase
• Check compliance
• Review and update classification

7.2.1. Implement Classification

Services depending up on its sensitivity and the impact that its unauthorized disclosure could have can be assigned any of theclassifications levels as described in the SLSCF. In order to identify the transactional nature of the service the “Service Type” should also be mentioned along with the service classification. The following diagram can assist in deciding the appropriate service classification and service type for any service.

7.2.1.1. *Apply classification and service type*


Start
Identify Information inputs and outputs used in the Service delivery
Are there 3rd party Information
YES
NO
Have Information assets being defined
YES
NO
Create Info assets as per guidelines in SLGTC
Have all Information assets being classified
N O
Classify as per SLGICF
YES
Update SCR
Identify the highest classification level of the information assets with in the service
Classification Level secret with/ with out DLMS and Caveat
YES
This Service is to be classified as RESTRICTED
NO
Classification Level Confidential or LS with DLMS : Sensitive government or Sensitive : Legal or / and Caveat
YES
This Service is to be classified as RESTRICTED
NO
Classification Level confidential or LS with DLMS Sensitive or Sensitive : Private
YES
Disclose of information would cause serious damage
NO
YES
NO
This Service is to be classified as CONFIDENTIAL
This Service is to be classified as LIMITED SHARING
Classification Level confidential or LS with No DLMS or Caveat
YES
This Service is classified as AUTHORIZED
NO
Classification Level Public
YES
This Service is classified as OPEN
Does the service provide and informational output
YES
NO
This Service type is DATA Service
Does the service output only a verification
YES
END
This Service is VERIFICATION Service

7.2.1.2. *Document classified services in a register (Service Classification Register - SCR)*

Once a service has been classified, the following information must be documented in the SCR.

- *Service name;*
- *Description of service (i.e. what is it about)*
- *Information assets used in the delivery and classification level;*
- *Service classification; and*
- *Service owner.*

*Please refer **Annexure A** for the SCR format*

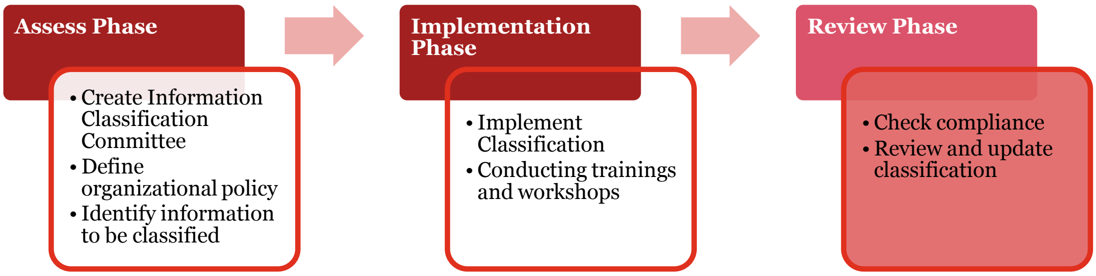
7.2.2. Conduct Trainings and Workshops

IT Project Managers with guidance from Information Classification Committee needs to plan for conducting trainings/workshop for all stakeholders on the need and process of Information and Service Classification. The various stakeholders who need to be trained are:

- *All organizational staff;*
- *Record Keeping staff;*
- *Support desk and GIC;*
- *Programme managers for all IT Initiatives;*
- *Public Relationship Officers;*
- *Head of organizations & ministries; and*
- *Chief Innovative Officer of the organization.*

The training should include protection of Information assets and its classification during entire life cycle of information from capturing to disposal and service classification aspects. The training should also include the incident raising and management policy to deal with any violations that may arise due to non-fulfillments of processes. The training should be done in batches followed by refresher courses so that necessary policies are followed always. It is also important to identify and train the “change agents” which can be helpful in spreading the awareness regarding importance of the Information and Service Classification.

7.3. Phase 3: Review and Update Information Classification


Assess Phase
• Create Information Classification Committee
• Define organizational policy
• Identify information to be classified
Implementation Phase
• Implement Classification
• Conducting trainings and workshops
Review Phase
• Check compliance
• Review and update classification

7.3.1. Check compliance

In order to ensure a through monitoring mechanism needs to be developed for review of Service Classification Implementation across organization. Following activities needs to be carried out (not limited to):

1. *Perform impact assessment of service classification implementation.*
2. *Conduct training need assessment (to verify the training requirements).*
3. *The committee in accordance with information security team should ensure that confidentiality of the information is secured in accordance with organizational requirements, and other regulations and guidelines.*
4. *The access rights for various types of users are appropriate.*
5. *The information and service classification team needs to ensure that data compiled from multiple sources is classified with at least the most secure classification level.*

7.3.2. Review and Update Classification

Based on the outcome of the above reviews, it is essential to establish a change control process to regularly review the effectiveness of the policy and make necessary changes. Furthermore, the changes may be brought by regulatory changes, changes to the business environments and other periodic reviews.It is important to develop a feedback mechanism with ICTA as well so that the changes which are applicable across organizations may be shared with ICTA in an agreed process.

8. Way Forward

1. Formulation of organizational level sharing policy

Data sharing policies are formulated to govern the sharing of data between various organizations as part of service delivery. While considering data classification and subsequent data sharing, it is essential to understand that sharing organizations may not always classify the data in same manner. This may happen due to different legislations and mandate of different organization and sensitivity of data across them.While the primary organization, to which data belongs should preferably sign a MoU/MoA, to document the terms of the arrangement and treatment of the data so that confidentiality, availability and integrity is not compromised during process of sharing. It is suggested that Legal and privacy experts be consulted as part of the MoU/MoA process. The MoU should consider the Information security during entire lifecycle of data. Through these agreements, the necessary importance can be given to avoid data leakages and prevent misuse of information.

2. Creation of National Level Data Sharing Policy

This document would also become the basis for formulation of national level data sharing policy.

9. Annexures

Annexure A – Service Classification Register (SCR)

Service name	Description of service (i.e. what is it about)	Information Assets used within the service		Information Asset Origination (within department, Government organization, Private organization)	Service classification
		Asset	Classification		