सत्यमेव जयते

EoI Reference No.: EIII/64(6) /Revamp/2021

Expression of Interest (EoI) for

Selection of System Integrator for
Design, Development, Implementation and Maintenance of Foreign Trade Statistics System for
DGCIS

Directorate General of Commercial Intelligence and Statistics
565, Anandapur, Ward No. 108 Sector– 1, Plot No. 22, ECADP,
Kolkata, West Bengal 700107
Phone: 033 2443 4055
eMail: dg[dot]dgcis[at]nic[dot]in

November, 2022

Contents

1. Letter of Invitation

1. Letter of Invitation

The Directorate General of Commercial Intelligence and Statistics (DGCIS), M/o Commerce and Industry, invites prospective & eligible participants for their Expression of Interest (EoI) for "Selection of a System Integrator for Design, Development, Implementation and Maintenance of Foreign Trade Statistics System".

DGCIS desires to leverage the state-of-the-art technologies to revamp and modernize its entire IT systems which includes its FTSS software, its website, dashboard, Business Intelligence Module, data dissemination portal, its mobile app as well as the associated hardware infrastructure. In order to execute the same, DGCIS desires to conduct the selection of the System Integrator in two steps. The first step would constitute soliciting proposals on Expression of Interest (EoI), which is an openly advertised competitive shortlisting process giving equal opportunity to all interested bidders to be considered for shortlisting. In this step bidders would be shortlisted on the basis of their responses to the EoI. In the next step, the Request For Proposal (RFP) would be shared with the shortlisted agencies and a bidder will be selected amongst them, as per the QCBS criteria mentioned in the RFP document, as the System Integrator for this project.

Interested Service Providers who meet the pre-qualification criteria may furnish their Expression of Interest with all the necessary documents on or before the date and time mentioned in the Critical Dates sub-section of this section.

(a) in a sealed cover along with the covering letter duly signed by an authorized signatory at the following address:

Shri Manish Kumar
Deputy Director and Head of Office,
Vaanijya Tathya Sadan,
565, Anandapur, Ward No. 108,
Sector– 1, Plot No. 22, ECADP,
Kolkata – 700107

(b) or by email at hoo-dgcis@gov.in, with a copy to s.acharya.dgcis@gov.in. In case the proposal is submitted via email, the attachment shall be zipped and protected by a password. The password is to be shared with DGCIS after EoI submission date-time and before EoI opening date-time.

1.1. Single Point of Contact person

Bidders are required to direct all communications related to this EoI, through the nominated Single Point of Contact (SPOC) person, mentioned below:

Name: Shri Srijan Acharya **Designation:** Deputy Director	**Email ID:** s[dot]acharya[dot]dgcis[at]gov[dot]in **Contact number**: 98737 25055

1.2. Critical Dates

Sl. No.	Critical Dates	Date	Time
1.	Publishing Date	29-11-2022	As per CPP portal
2.	**EoI Submission End Date**	**18-12-2022**	**20:00 Hrs**
3.	EoI Opening Date	19-12-2022	11:00 Hrs

The EoI document download start date is same as the Publishing Date. The document download end date is same as the Submission End Date. Bid Submission Start Date is same as the Publishing Date.

2. Introduction

2. Introduction

The Directorate General of Commercial Intelligence and Statistics (DGCIS), M/o Commerce and Industry, is the premier organisation for compilation and dissemination of all trade related statistics of India. For this task, over time, it has created a Data Centre (DC) and a Data Recovery (DR) centre and has been implementing IT solutions for day-to-day work through the FTSS software package developed and maintained by its own officers. It also has a number of channels for dissemination of information such as the website, Data Dissemination Portal, the Exim Analytics Dashboard, and the mobile app -DGCIS Exim.

2.1. Project Background

In light of the current advancements in terms of Open-Source Technologies and applications of emerging technologies, the Directorate General of Commercial Intelligence and Statistics (DGCIS) desires to revamp its present IT system.

The major focus areas of this initiative concerning digital transformation of DGCIS' IT system are to re-develop its legacy Foreign Trade Statistics System (FTSS) application in Open-Source Technologies, migrate its databases from Oracle to PostgreSQL or any other Open-Source Relational Database system, migrate all its legacy applications to Open-Source Technologies, host all or some of its applications and databases to any MeitY empanelled cloud, and incorporate Artificial Intelligence / Machine Learning principles while modifying / redeveloping its application, The key rationale behind this initiative is to make the IT Systems cloud-ready, futuristic, more efficient, secure, cost effective and up to date.

2.2. Project Objectives

DGCIS intends to select a System Integrator (SI) for the re-development of its legacy Foreign Trade Statistics System (FTSS) application in Open-Source technologies, migrate its existing databases from Oracle to an open-source database system, host all or some of its other applications and databases in any MeitY empanelled cloud, and incorporate Artificial Intelligence / Machine Learning principles while modifying / redeveloping its application, **without compromising on the efficiency and security aspects of the applications and databases**. The contract duration would be for a period of 5 years (15 months for Development and Go-Live + 45 months of Operations & Maintenance) on TCO basis with the following objectives and envisaged outcomes that the Service Integrator has to ensure throughout the contract period. The contract shall be renewable for two (02) more years after expiry of five years on mutually agreed terms.

- ✓ Establish effective and efficient Infrastructure monitoring & management practices to ensure reliability, availability, quality of services and security of the Information systems in on-premises as well as cloud environment
- ✓ Design and Develop the Foreign Trade Statistics System (FTSS) application in Open-Source Technology (Java and Python) stack
- ✓ Procure, Supply, install, commission, maintain, manage and support the IT infrastructure required for the DC site and DR-backup
- ✓ Procuring, setting up, installation, configuration, management of application servers, database servers/storage in the cloud environment.
- ✓ Incorporate/adhere the security and Interoperability guidelines, i.e., MeitY guidelines for safety and security norms, during the contract
- ✓ Ensure compliance to the audits and the observations of regulatory bodies.
- ✓ Observe best practices required to Operate, Maintain, Manage, Support and Service

It is expected that the SI should give its best performance as required by DGCIS for successful completion of this project.

2.3. Overview of DGCIS's ICT Infrastructure

Currently, DGCIS has centralized setup with Data Centre [DC] and Disaster Recovery [DR] Site at its premises in Kolkata. All applications are hosted at Data Centre, Kolkata and are accessed by all end users over LAN. All the sections/units of the DGCIS office are connected through LAN. Following provides a brief overview about DGCIS's present IT infrastructure:

A. **Network:** The network infrastructure of DGCIS primarily consists of the following items

- **Core-Switch:** Core switches are backbone of whole network system of DGCI&S and are responsible for routing and forwarding at the highest level. DC to DR connectivity is established by DC to DR site core switch. The core switch is configured in VSS (Virtual Switching System) mode which provides fault tolerance and high availability.
- **Fortinet Firewall:** Fortinet Firewall is configured in High Availability mode; it provides security and protection to whole DGCI&S network with its rich set of security policies and antivirus feature, cisco ASA is between server farm switch to core switch which provides add-on security to server.
- **DMZ:** All web applications are broadcasted to public network via DMZ network of firewall in order to provide security to web applications.
- **Active Directory:** All clients are joined in domain and each user is authenticated with AD server and different authorization and access level are defined at this server.
- **Oracle Database:** Production and Warehouse oracle database is configured as 2 node RAC (Real Application Cluster), which provides High Availability, Fault Tolerance and Load balancing.
- **Oracle Golden Gate:** Database objects are being replicated with Oracle Golden Gate utility between DC and DR.
- **Oracle WebLogic:** Oracle Forms and Business Intelligence Application runs on the WebLogic (middleware) Server
- **SPARC T7-1 Server:** DGCIS has four SPARC M7 processor based T7-1 servers for Production Environment.
- **Oracle FS1-2 Storage:** DGCIS currently has two FS1-2 Storage for DC-DR environments. The Oracle FS1-2 flash storage system delivers enterprise-grade storage capabilities that are optimized for flash media and engineered with Oracle software.
- **Symantec NetBackup:** It is backup solution from Symantec v7.7.3, which is used to run automated backup and restore functions in Tape devices. Oracle X5-2 server is used as a backup Server & SL150 as a tape drive.

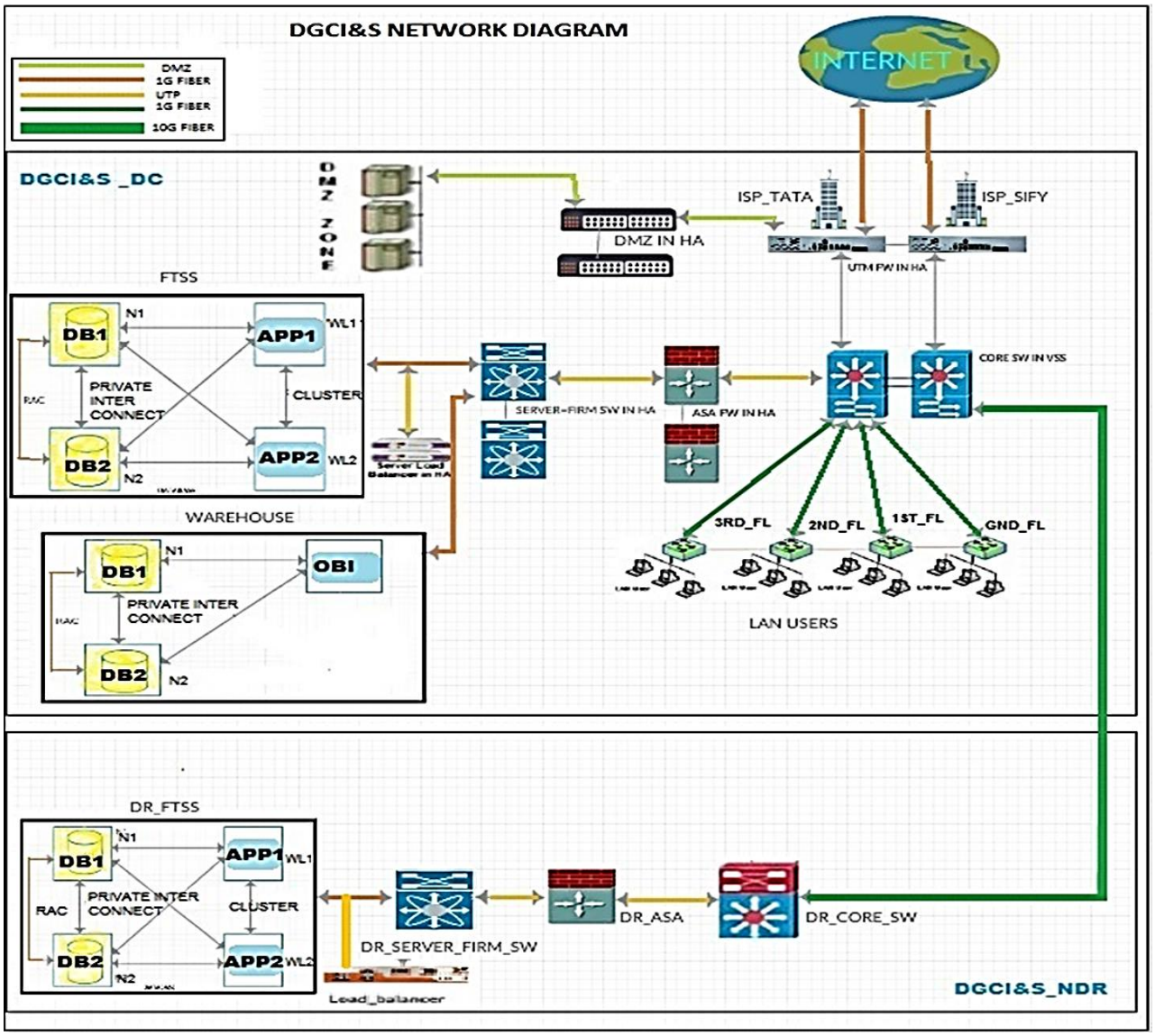
- **LDOM: Solaris:** LDOM is a server virtualization and partitioning technology that is used to host multiple instances of Solaris virtual machines (VMs) on an Oracle server. Solaris 11.3 is used as OS in production environment.
- **Brocade SAN S/W:** SAN switch is used to connect servers, storage and tape library in SAN environment.
- **LDAP:** LDAP Server is used to authenticate Internet Users.
- **Wide Area Network**

  Presently DGCIS has two connectivity modes, through primary (Tata) and secondary (Sify) Internet Service Providers (ISPs).
- **Local Area Network**

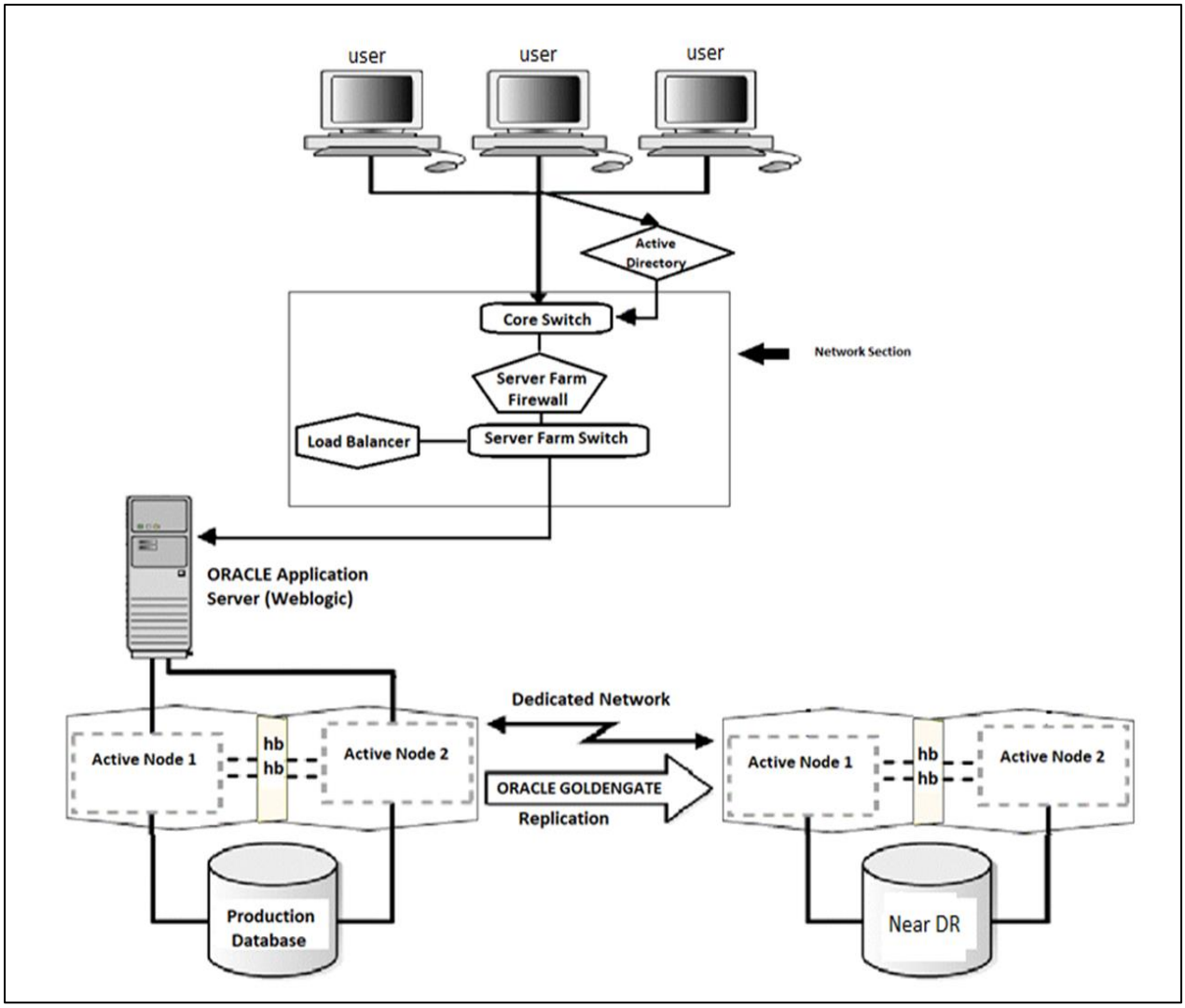
  In DGCIS' office the LAN is based on Layer 3 and Layer 2 switches. The switches used at the different floors of the office buildings are managed. All switches are property of DGCIS and are under AMC with respective vendors.

The following diagrams provide a broad overview of the ICT Infrastructure currently at work in DGCIS:

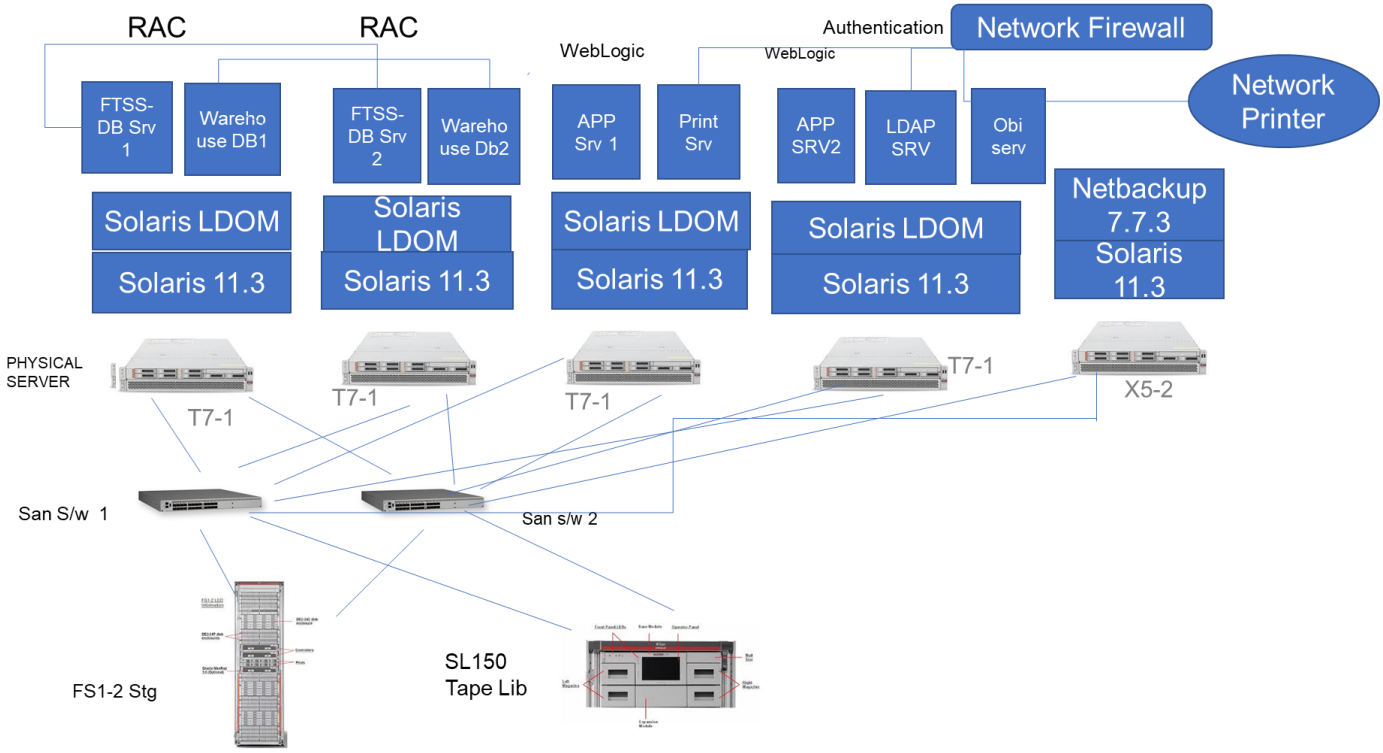
IT Infrastructure Diagram (DC/DR)



Production & Warehouse Database and WebLogic Application Server Architecture



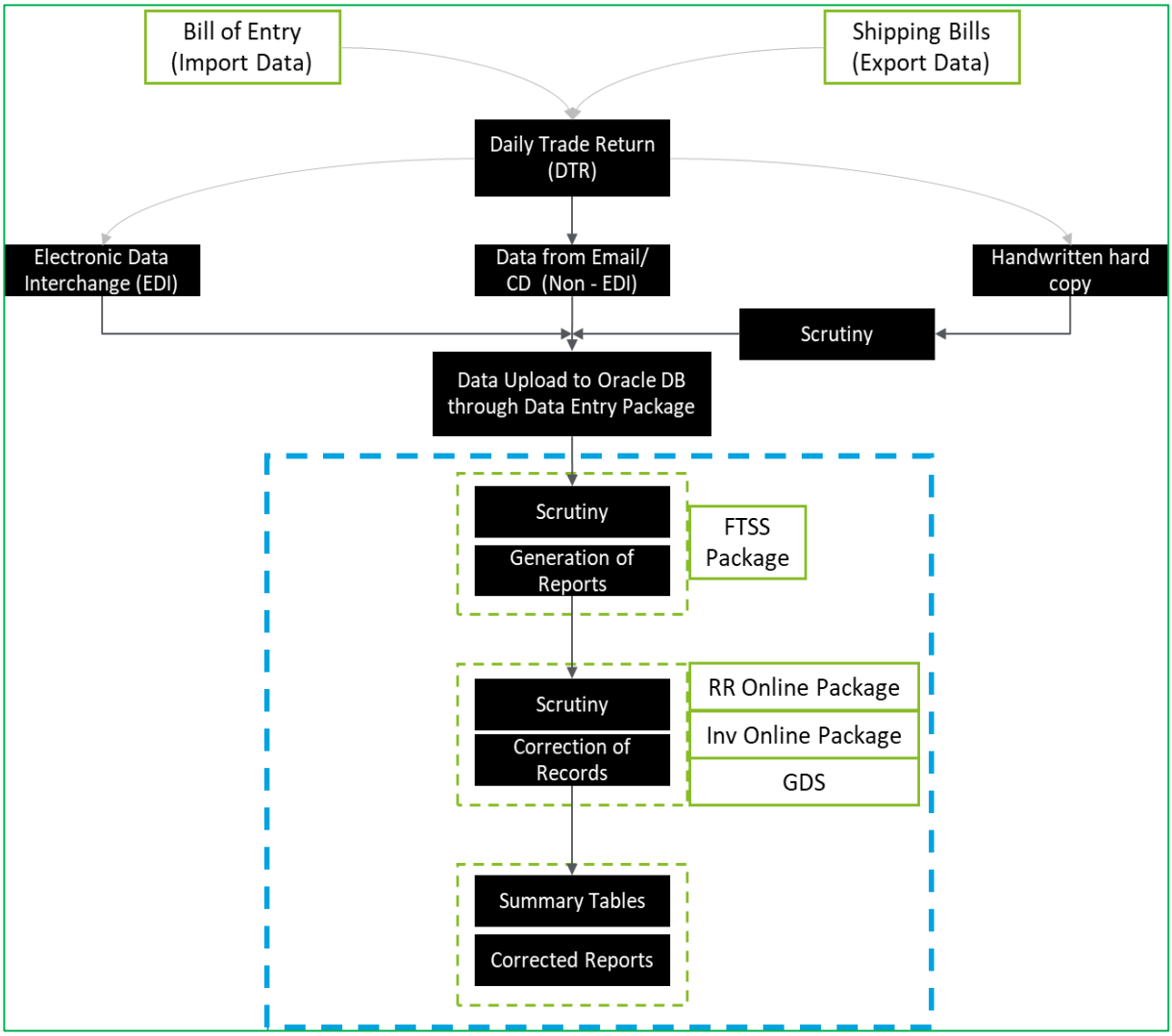
Server & Storage Architecture- DC



B. A brief on the data processing work

On a daily basis, Foreign Trade Data are received by DGCIS from Customs and SEZs in the form of Daily Trade Returns (DTRs) which are part of Shipping Bills (for Export) and Bills of Entry (for Import). After validation, foreign trade data are disseminated in various ways – in the form of Quick Estimates and Press Note released by the Department of Commerce on the 15th of every month for the preceding month, Principal Commodity Group by country level information for the Brochure publication, 8-digit commodity level publication for Monthly Statistics of Foreign Trade of India (MSFTI) and quarterly 8-digit level publication SFTIC (Statistics of the Foreign Trade of India by Countries).

Following is a workflow-based representation of the data processing mechanism being followed: The current IT application landscape of DGCIS consists of the following elements,


Bill of Entry
(Import Data)
Shipping Bills
(Export Data)
Daily Trade Return
(DTR)
Electronic Data
Interchange (EDI)
Data from Email/
CD (Non - EDI)
Handwritten hard
copy
Scrutiny
Data Upload to Oracle DB
through Data Entry Package
Scrutiny
Generation of
Reports
FTSS
Package
Scrutiny
Correction of
Records
RR Online Package
Inv Online Package
GDS
Summary Tables
Corrected Reports

C. Software packages

Internal Data Processing Software packages include:

Sl. No.	Package Name	Functionality
1.	FTSS RAC	The FTSS RAC package is used to prepare the exception reports, summary tables and reports as well as upload the approved data into the system.
2.	RR_Online	The package is used for tallying record to record entries in trade data corresponding to Standard units, Quantity and Rate errors.
3.	Inv_Online	Used to identify and correct Invalid Country and Commodity Code errors in trade (Export and Import) data.
4.	Group Dump System	Used to correct errors in trade data corresponding to Standard units, Quantity and Rate errors which may have been missed at RR stage.
5.	Data Entry Package	Used for uploading manual data into the Export and Import DTR Table.

D. Database Licenses

Sl. No	Product Description	License Type	Version	RAC Cluster
1	Oracle Database Enterprise Edition ATS for Oracle 10g software, oracle database EE Processor perpetual license	Perpetual license	12.1.0.2.0	Yes
2	Oracle Database Enterprise Edition (Perpetual License)	Perpetual license	12.1.0.2.0	Yes
3	Oracle Database Enterprise Edition (Oracle Business Intelligence Suite Foundation Edition - Processor Perpetual License)	Perpetual license	12.1.0.2.0	Yes
4	Oracle Database Standard Edition (Oracle ATS of Oracle Database SE Oracle 1 - Click Ordering Programmed U0073er plus Perpetual License with Back Support	Perpetual license	11.2.0.1.0	No
5	Oracle Database Standard Edition		11.2.0.1.0	No

	Oracle ATS for providing on-site maintenance support of SUN Fire X4170 server			
6	Oracle Database Enterprise Edition (Web logic) (Perpetual License) Golden Gate (Perpetual License)		11.2.0.1.0	No

E. Data Dissemination Channels

Currently, DGCIS has the following channels for dissemination of finalized data for the public:

1. Data Dissemination Portal
2. Exim Analytics Dashboard
3. Business Intelligence Module
4. DGCI&S Website
5. Exim Mobile App

1. Data Dissemination Portal: The Data Dissemination Portal is the main channel for dissemination of finalized data to the public. The application is connected to an Oracle database containing the finalized MSFT data (ITCHS wise, country wise and port wise export and import figures) for each month till the latest month. Any user can login to the portal as a guest, run a query on the database and see the number of records fetched by the query. Thereafter, the user is given an option to pay, through BillDesk for the data on a per-record basis, and once the payment is made the data can be downloaded from the portal. Frequent users can have credentials created by DGCIS and make advance payments for data downloading. The charges for downloading for frequent users is automatically debited from their account.

Portal link - http://ftddp.dgciskol.gov.in/

2. Exim Analytics Dashboard: This, as the name suggests, presents a dashboard with basic charts and diagrams related to Exim trade. The user can analyse various scenarios by deep diving into the data through this dashboard.

Portal link - http://www.eximanalytics.dgciskol.gov.in/dgcis/EXIM-Analytics#/home?_g=()

3. Business Intelligence Module: This module runs on Oracle BI platform and provides an opportunity to users to do trade analytics on the platform itself, with the help of indicators / indices. It uses the trade data of India from DGCIS as well as world trade data from the Comtrade platform to arrive at indicators.

Link: http://da.dgciskol.gov.in/bi-security-login/login.jsp

4. DGCI&S Website: The website is main channel of dissemination of information regarding DGCIS. Apart from information, few publications, which are not disseminated through other channels, are also disseminated through the website. There is an admin dashboard which is used internally for uploading of files and other information to the website, as well as for periodic maintenance of the website.

Link: http://www.dgciskol.gov.in/

5. Exim Mobile App: This is the app version of the Exim Analytics Dashboard. The name of the app is DGCIS EXIM. Through the app a user can mine through current and historical data pertaining to commercial intelligence and statistics on the go. It provides information in the form of numbers and figures, graphs and plots and one can simply browse through years of data, and compare information from various periods and sources. If one wants such data offline, this app has a facility to email the reports.

Available at -
https://play.google.com/store/apps/details?id=com.dgcis.exim&hl=en_IN&gl=US

3. Instruction to Consultants

3. Instruction to Consultants / Bidders

3.1. General

a) The Bidder is expected to examine all instructions, forms, terms and specifications in the bidding documents. Failure to furnish all information required by the bidding documents may result in the rejection of its bid and will be at the bidder's own risk.

b) All costs and expenses incurred by the Bidders in any way associated with the development, preparation, and submission of responses, including but not limited to; the attendance at meetings, discussions, demonstrations, etc. and providing any additional information required by DGCIS, will be borne entirely and exclusively by the Bidder.

c) No binding legal relationship will exist between any of the Bidders and DGCIS until execution of a contractual agreement.

d) Each Bidder acknowledges and accepts that DGCIS may in its absolute discretion apply selection criteria specified in the document for evaluation of proposals for short listing / selecting the eligible System Integrator. The EoI document will not form part of any contract or arrangement, which may result from the issue of this document or any investigation or review, carried out by a Bidder.

e) Every Bidder will, by submitting his Bid in response to this EoI, be deemed to have accepted the terms of this EoI and the Disclaimer. However, if there are any critical suggestions the same may be discussed with DGCIS.

f) Bidders are advised to study all instructions, forms, terms, requirements and other information in the EoI documents carefully. Submission of the bid shall be deemed to have been done after careful study and examination of the EoI document with full understanding of its implications.

g) Failure to comply with the requirements of this paragraph may render the Proposal noncompliant and the Proposal may be rejected. Bidders must:
   - include all documentation specified in this EoI;
   - follow the format of this EoI and respond to each element in the order as set out in this document; and
   - comply with all requirements as set out within this document.

h) Bidders are required to direct all communications related to this EoI, through the nominated Single Point of Contact (SPOC) person, mentioned below:

Name: Shri Srijan Acharya **Designation:** Deputy Director	**Email ID:** s[dot]acharya[dot]dgcis[at]gov[dot]in **Contact number**: 98737 25055

i) DGCIS may, in its absolute discretion, seek additional information or material from any Bidder/s even after the EoI closes and all such information and material provided must be taken to form part of that Bidder's response.

j) Bidders should provide details of their contact person, telephone, fax, email and full address(s) to ensure that replies to EoI could be conveyed promptly.

k) If DGCIS, in its absolute discretion, deems that the originator of any query will gain an advantage by any response to such query, then DGCIS reserves the right to communicate such response to all Bidders.

l) Queries / Clarifications, if any, may be taken up with the contact persons detailed above before the deadline for submission of bids between 09.30 am to 6.00 pm on any working days (Monday to Friday, except holidays).

m) Bidder should not have been blacklisted / debarred from participation in the Bid process by any of the Govt. Departments (Central or State)/ PSUs/ DGCIS/ Financial Institutes in India.

n) DGCIS will notify all short-listed Bidders in writing or by mail or by publishing in its website as soon as practicable about the outcome of their EoI. DGCIS is not obliged to provide any reasons for any such acceptance or rejection.

3.2. Publication of EoI Document

The EoI document will be made available on Central Public Procurement Portal (CPPP): https://eprocure.gov.in , Government e Marketplace (GeM): https://gem.gov.in/ and also on DGCIS' website, http://www.dgciskol.gov.in/.

3.3. Pre-bid Meeting & Clarification

a) For the purpose of clarification of doubts of the bidders on issues related to this EoI, DGCIS intends to hold an online Pre-Bid meeting. The date, time and online link of the meeting will be communicated through email to the consultants who have sent their queries to DGCIS SPOC. The queries of the Bidders, in writing, should reach by e-mail to the e-mail id of SPOC, **within five working days** after publication of the EoI.

b) It may be noted that no queries of any bidder shall be entertained received after the Pre-Bid meeting. Clarifications on queries will be given in the Pre-Bid meeting. Only the authorized representatives of the bidders, will be allowed to attend the Pre-Bid meeting. For each bidder, maximum of two representatives are allowed. The representatives should be employees of the Bidding Company

c) The responses will be transmitted to the prospective bidders through appropriate means. However, it will be bidder's responsibility that they collect all responses. Non-attendance at the Pre-Bid meeting will not be a cause for disqualification of a Bidder. The queries should necessarily be submitted in the following format in editable MS Excel workbooks.

#	Section	Page Number(s)	Content of EoI requiring Clarification(s)	Points of clarification	Suggested Clause (if any)
1.					
2.					
3.					
4.					

d) DGCIS shall not be responsible for ensuring that the bidders' queries have been received and / or addressed by them. Any requests for clarifications after the indicated date and time may not be entertained by DGCIS.

e) At any time, prior to the date of submission of Bids, DGCIS may, for any reason, whether at his own initiative or in response to a clarification requested by a prospective bidder, modify this document by means of amendments or corrigenda.

f) Any such corrigendum shall be deemed to be incorporated into this EoI Document.

g) The amendments shall be notified on DGCIS website and these amendments will be binding. The bidder is not supposed to change any clause in tender document downloaded from website.

h) In order to afford prospective bidders reasonable time to take the amendment into account in preparing their bids, DGCIS may, at his discretion, extend the deadline for the submission of bids suitably.

3.4. Consortium & Sub-Contracting Conditions

Bidders are allowed to participate as a Consortium or Joint-Venture, clearly indicating Lead Bidder in the partnership agreement. The lead partner should have the maximal contribution in the project with respect to intellectual input (or input from human resources / skilled manpower). In such a case, the maximum number of partners, including the lead partner, should not exceed three (03). The qualification criteria, as mentioned in section 4 of this document, "Qualification Criteria", shall be applied **only to the lead partner.** *Among all the partners of the consortium, only the lead partner would be the party responsible and accountable for the success of the project.*

3.5. Statement of Confidentiality

This document contains information that is proprietary and confidential to Directorate General of Commercial Intelligence and Statistics (DGCIS), which shall not be disclosed outside the bidder's company, transmitted, or duplicated, used in whole or in part for any purpose other than its intended purpose. Any use or disclosure in whole or in part of this information without explicit written permission of DGCIS is prohibited. This document is provided to the Bidder on the basis of the undertaking of confidentiality given by the Bidder to DGCIS. DGCIS may update or revise this document or any part of it. The Bidder acknowledges that any such revised or amended document is received subject to the same terms and conditions as this original and subject to the same confidentiality undertaking. The Bidder will not disclose or discuss the contents of this document with any officer, employee, consultant, director, agent, or other person associated or affiliated in any way with DGCIS or any of its customers, suppliers, or agents without the prior written consent of DGCIS. Any use or disclosure in whole or in part of this information without explicit written permission of DGCIS is prohibited.

In this context it may be noted that the bidder who is finally selected after the RFP phase shall be required to sign a Confidentiality-cum-nondisclosure agreement with DGCIS.

3.6. Amendment to the EoI document

a) At any time prior to the deadline for submission of Bids, DGCIS, for any reason, may modify the EoI document, by amendment or corrigendum.

b) The amendment will be posted on DGCIS' website, http://www.dgciskol.gov.in/.

c) All Bidders must ensure that all amendments/enhancements (if any) in the EoI have been considered by them before submitting the Bid. DGCIS will not have any responsibility in case of any omission by Bidder/s.

d) DGCIS at its discretion may or may not extend the deadline for the submission of Bids.

e) DGCIS shall not be liable for any communication gap. Further DGCIS reserves the right to scrap the tender or drop the tendering process at any stage without assigning any reason.

3.7. Language of Proposal

All proposals are to be submitted in English. In case any original document is not in English, then it should be accompanied by an English translation of the same, and in case of ambiguities, the intent of the English version, as interpreted by DGCIS, shall be taken as final.

3.8. Period of Validity of Proposal

The offer for EoI as per this document shall be valid for a period of six (06) months, which may be extended further, if required, by DGCIS
In exceptional circumstances DGCIS may solicit the Bidders' consent for extension of the period of validity. Any such request and response thereto shall be made in writing.

3.9. Deadline for submission of Bids

a) The Bids must be received online by DGCIS at the website specified, not later than the last date of Bid submission as indicated in the section 1, "Letter of Invitation".

b) DGCIS may, at its discretion, extend the deadline for submission of Bids by amending the Bid documents with intimation on the mentioned website, in which case, all rights and obligations of DGCIS and Bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

c) DGCIS shall not be responsible for non-receipt / non- delivery of the Bid documents due to any reason whatsoever.

3.10. Clarification of Proposals

During evaluation of Proposals, DGCIS, at its discretion, may ask the Bidder for clarification of its proposal. The request for clarification and the response shall be in writing (e-Mail), and no change in the substance of the proposal shall be sought, offered or permitted.

The decision of DGCIS is final towards evaluation of the proposals.

3.11. Proposal Ownership

The proposal and all supporting documentation submitted by the Bidder shall become the property of DGCIS unless DGCIS agrees to the Bidder's specific request/s, in writing that the proposal and documentation be returned or destroyed.

3.12. Proposal Preparation Costs

The Bidder shall be responsible for all costs incurred in connection with participation in the EoI process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings/discussions/presentations, preparation of proposal, in providing any additional information required by DGCIS to facilitate the evaluation process, and in negotiating a definitive contract or all such activities related to the bid process.

DGCIS will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

3.13. Acknowledge of Understanding of Terms

By submitting a proposal, each bidder shall be deemed to acknowledge that it has carefully read all sections of this EoI, including all forms, schedules and annexure hereto, and has fully informed itself as to all existing conditions and limitations.

3.14. Banned or Delisted Bidder

Bidders have to give a declaration that they have not been banned or delisted by any Government, PSUs and its subsidiaries. If this declaration is not given, the Bid will be rejected as non-responsive. This declaration will be submitted in the EoI Covering Letter Annexure – B.

3.15. False / Incomplete statement

Any statement/declaration made by the Bidder, if proved wrong or false or incomplete or such as to withhold any information relevant to shortlisting of bidders, at any stage of the

shortlisting process or in the event of his proposal having been accepted shall render his/their proposals liable to be cancelled/rescinded.

3.16. Right to Terminate the Process

DGCIS may terminate the bid process at any time and without assigning any reason. DGCIS makes no commitments, express or implied, that this process will result in a business transaction with anyone.

This EoI does not constitute an offer by DGCIS. The Bidder's participation in this process may result in DGCIS selecting the Bidder to engage in further discussions and negotiations towards the execution of contract. The commencement of such negotiations does not, however, signify commitment by DGCIS to execute a contract or to continue negotiations. DGCIS may terminate negotiations at any time without assigning any reason.

4. Qualification Criteria

4.1. Bid Evaluation Methodology

The objective of evaluation methodology is to shortlist service providers on the basis of the responses submitted by them.

To meet DGCIS's requirements, the shortlisted agency must have the requisite experience in providing services in the field of ICT, the technical know-how, and the financial wherewithal that would be required to successfully set-up the required infrastructure and provide the services sought by DGCIS, for the entire period of the contract.

DGCIS reserves the right to modify the evaluation process at any time during the EoI process (before submission of responses by prospective bidders), without assigning any reason, whatsoever, and without any requirement of intimating the Bidders of any such change. Any time during the process of evaluation DGCIS may seek specific clarifications from any or all Bidders. Further, DGCIS reserves the right to reject any proposal in case same is found incomplete or not submitted in the specified format given in this EoI document.

4.2. Qualification Criteria and their weightages

Minimum Qualification Criteria

a) The bidder must be a Company registered under Companies Act, 1956/2013 or a partnership firm registered under LLP Act, 2008.

b) The bidder should have been operating in the area of software development, implementation, IT consulting, procuring and providing IT infrastructure for last ten (10) years before date of submission of bid.

c) The Bidder should have average annual turnover of INR 200 Crores from IT/ ITeS and other IT related services (excluding sale of hardware) in the last three financial years viz. 2020-21, 2019-20 and 2018-19 and should not have incurred loss in last three (03) financial years

Qualification Criteria for shortlisting

Sl. No.	Technical Qualification Criteria	Break up of Parameters	Weightage/ Score	Max. Score
A.	**Criteria about the organization – 75%**			
1.	Relevant experience of executing integrated software project(s) (Project Design and implementation) involving complex business processes, rule engine & workflows or have worked for application development projects of similar nature in the last 5 years (min. 2 projects)	2 to 5 projects	5	15
		6 to 10 projects	10	
		> 10 projects	15	
2.	ISO certifications (ISO 27001 or ISO 20000 and CMMi Level 5 & above)	ISO 27001	2	10
		ISO 20000	2	
		CMMi level 5	6	
3.	Number of qualified professionals on payroll of bidder holding BE/ B.Tech/ MCA/ M.Sc. (IT) degree and experience of working in the domain of Application development, web portal design/ development, AI and ML based applications including implementation of cloud solution, System Integration, Data Centre setup, project management and planning, system architecture design (min. 500 employees)	500 to 1000	5	10
		>1000 <=2000	7	
		> 2000	10	

4.	Experience of handling large integrated IT projects (>40 crores) for Government Clients (at State and National Level) in the last 5 financial years (central/state government / PSU.)	2 to 5 projects	5	10
		6 to 7 projects	7	
		8 projects or more	10	
5	Project Experience of implementing at least 2 projects invoving development of a large software.	2 projects	4	10
		3 to 4 projects	7	
		>=5 projects	10	
6.	Project Experience in emerging area of AI-ML (min. 2 projects).	2 projects	1	5
		3 - 5 Projects	3	
		>= 6 projects	5	
7	Relevant experience of application hosting and maintenance on cloud platform and providing support on Cloud Data Centre management (min. 2 projects)	2 projects	1	5
		3 - 5 Projects	3	
		>= 6 projects	5	
8	Relevant experience of commissioning Data Centre	2 Project	1	5
		3 - 5 Projects	2	
		>= 6 projects	4	
		Additional 1 mark to be provided in case of execution of 2 Government projects		
9	Has Delivery Centre in Kolkata with at least 500 technical employees			5

C.	Criteria about overall financial strength - 25%				
Sl. No.	**Description**	**2018-19**	**2019-20**	**2020-21**	**Average (Mean)**
1.	Turnover figures (in Rs. Crores)				
2.	Net profit figures (in Rs. Crores)				

The bidders are also required to submit a small write-up (within 200 words) on two **most relevant** projects each for points 4, 5 and 6 of Table A above:

Client Name	Cost of Project	Brief Description of Project (within 200 words for each project)

Minimum qualifying marks is 75%.

The bidders must disclose any conflict of interest that they know may impact objective performance and impartial advice for their services.

No legal documents such as certificates of incorporation of the firm, powers of attorney, financial statements, or translations of standard brochures is being requested at this stage of EoI; responses are to be made solely on the basis of self-declaration. However, in the next stage, during submission of tender documents in response to the RFP all supporting documents of the declarations made herein would be requested for and verified by DGCIS.

5. Scope of Work

5. Scope of Work

5.1. An Overview

The scope of this project on Revamping of IT systems of DGCIS consists of two parts – software application development part and infrastructure part. The software application part again consists of two parts. The first part consists of revamping and rebuilding the core FTSS package -used for in-house data processing - afresh, as well as migration of the existing databases to open-source database. The FTSS application is to be hosted from newly procured in-premise infrastructure. In the other part of software application development, the different dissemination channels such as website, Data Dissemination Portal, the Exim Analytics Dashboard as well as the mobile app – DGCIS Exim – are to be revamped and hosted in cloud infrastructure. The databases of the existing applications are also to be migrated as per requirement. In the infrastructure part of the scope, the vendor is to procure appropriate infrastructure – hardware and cloud – to develop, host and test the applications. Thereafter, the

thus revamped IT applications as well as the infrastructure are to be maintained for a period of three (03) years and nine (09) months[1].

While the new FTSS application is to be hosted from in-premise infrastructure, the aim is to develop it in such a way that it is cloud native, and can be easily migrated to the cloud infrastructure as and when the need arises (**cloud native applications**).

Further, in future there might be a need to migrate from one cloud platform to another and, hence, the technology used to develop these **applications should be cloud agnostic** so that the applications are readily portable to any MeitY empanelled cloud.

5.2. Revamping of IT Infrastructure

At present both the DC and DR are located in DGCIS premises. All the applications, except the website, are hosted from the Data Centre. A hybrid-model is envisaged in the revamped scenario, where the core application for data-processing, the FTSS package, will be hosted on on-premises infrastructure, while the other applications which are used for dissemination of data to public – shall be hosted from cloud infrastructure. The procurement of the on-premise hardware and cloud infrastructure is to be made by the SI, ensuring the ownership of DGCIS on the in-premise infrastructure.

5.3. Migration of databases

At present all the data of DGCIS is stored in Oracle databases, in the on-premises servers of DGCIS. The details of the databases are provided in the 'As-Is Report', included as an addendum to this EoI Document.

All the databases are to be migrated to PostgreSQL or any similar open-source relational database. *The database which is to be procured must have support from enterprises and should not be community supported products.* There might be a need to make minor alternations and modifications in the present table structures before or after migration, whichever is convenient. Thereafter, the databases containing sensitive transactional data are to be located in on-premise infrastructure, while the databases containing finalized aggregated data for the public, which are the bases for the dissemination channels, are to be migrated to the cloud infrastructure. Appropriate data masking and security measures are to be taken to migrate the data in the cloud. Further, the databases that are on-premises should be created in a cloud-ready manner.

5.4. Revamping of the FTSS package

The FTSS package is the core application through which day-to-day data processing is done by officials of DGCIS. This application was developed by in-house officers of DGCIS and is maintained by their successors. Now there is a need to modernize the application. However, the business processes remain almost same and hence, the functioning of the application would

[1] The project is conceived to be of a total of five (05) years – 15 months for development of applications and 45 months for maintenance. Thereafter, the contract will be extendable by 2 years on mutually agreed terms.

be similar. Details of the present application is given in 5.37. DGCIS's current Application: Module-wise description. The SI has to prepare a new version of the application - FTSSv2 - after system requirement study and prepare SRS & SDS, System Due diligence and submission of detailed report and obtaining of due approvals.

5.5. Revamping of the dissemination channels

The (1) Data Dissemination Portal, (2) Exim Analytics Dashboard, (3) Business Intelligence Module, (4) DGCIS Website and (5) Exim Mobile App consist the data dissemination channels of DGCIS. All data for public is disseminated through these applications / channels. The online links to these channels are given in Section 1 of this EoI document, through which the reader can have a first-hand idea of the portals and dashboards.

The idea is to revamp and integrate all the data dissemination channels into one platform using open-source technology. The DGCIS website will be the main platform to be visited by the user. From there the user may visit the new dashboard, through a link created in the website, for the purpose of segmenting, visualizing and analyzing the data, etc. Thus, the new dashboard would be integrated to the new DGCIS website. The mobile app should be a mobile/tablet version of the dashboard with all or most of the functionalities of the dashboard.

5.6. Schedule of Services

This schedule of services sets out precise list of services that the SI will be providing as part of this project for meeting the project goals. The schedule of services also contains various deliverables, schedule, reports and product details that are to be provided by the SI as part of this project.

SI will be required to provide quality and timely services to DGCIS for the successful design, development, and implementation of FTSSv2 (i.e., the revamped FTSS application). All the activities performed by the SI during different phases of the project shall be closely monitored by DGCIS. The SI is strongly advised to carefully read the Schedule of Services and prepare their proposal accordingly.

It is expected that SI will carry out an assessment of number of resources required to undertake the scope of services under this engagement. However, at any time, a minimum of three (03) resources will have to be deployed by the SI to deliver the services as proposed in this scope. For any services defined beyond the scope of services, DGCIS may ask for additional resources from SI as per rates to be submitted with commercial proposal of RFP.

The broad schedule of services for the SI during the contract period would include, but not limited to:

a) Performing a system requirement study and prepare SRS & SDS, System Due diligence and submission of detailed report.

b) Design and development of the dissemination channels of DGCIS as outlined in section 5.4 of this chapter, 5.4. Revamping of the dissemination channels.

c) Design and Development of FTSSv2 (application software):

Design and Develop the Foreign Trade Statistics System (FTSS) application in Open-Source Technology (Java and Python) stack.

- Development of the Project Implementation plan.
- Design, Installation, Configuration, Customization of Software Related solution for DGCIS as per requirements outlined in scope of work.
- Quality Review, reporting and approval.
- Project and Product Documentation.
- Detailed Post Implementation documents for each and every module and sub-modules to be prepared and submitted to the client. Approval of the same from the client to be taken.
- Developing and designing of Operational Handbook for each and every module and sub modules, in simple and clear language.
- Patch and update management.

d) Migration of databases of existing applications – FTSS, applications of dissemination channels, etc. to PostgreSQL or any other open-source relational database.

e) Supply, installation, configuration and commissioning of IT hardware and Network Components for Data Centre Site and DR-backup & installation of required system software for FTSSv2 application hosting.

f) All procurements, including all non-IT components, should be made in the name of DGCIS. Original invoices of procurement of all hardwares and softwares, including all non-IT components, should be submitted to DGCIS.

g) Migration of data from existing (old) FTSS to the proposed (new) FTSSv2

h) Application Testing i.e., unit testing, integration testing, system testing, load testing

i) User Acceptance Testing (UAT)

j) Commissioning of FTSSv2

k) Go-Live of FTSSv2

l) Training & Capacity Building

m) Operation & Maintenance of FTSSv2

i. Application and Infrastructure support including modifications and integration with future systems.
ii. Bug Fixes and Management.
iii. Software Change and Version Control.
iv. User Support and Annual Maintenance of the application to SLA.
v. Application monitoring and Compliance to SLA.
vi. Database Administration.

vii. User Administration.

n) Conducting a Review Meeting every fortnight with DGCIS to apprise the progress of the project and resolve any issues that requires decision making from the DGCIS side.

5.7. Business Process Analysis

SI shall assess the existing business processes of DGCIS to supplement the understanding gathered from the high-level business processes included in the Functional Requirement Specifications (FRS) of this document. The selected bidder's objective shall be to develop comprehensive solution to support all the business needs of DGCIS in detailed manner along with other functional requirements as stated in the RFP document.

5.8. System Requirement Study and Preparation of SRS & SDS

a) Although an indicative FRS, TRS and Schedule of Service have been provided in the EoI and RFP document, the SI shall carryout an independent and detailed assessment study of functional, technical, and operational requirements of DGCIS.

b) The SI is responsible to carry out an independent system study at DGCIS Office to thoroughly understand the function and operational process of department by

   i. interacting with concerned section officials and understanding the entire setup, process flows, and business logics involved,

   ii. reviewing the existing systems, process, and existing application software,

   iii. detailing various use cases scenarios where AI/ML or any other technology driven innovation can be applied,

   iv. understanding/ assessment of data migration requirement and strategy,

   v. understanding/ assessment of data inputs and outputs requirements by collecting all input forms, registers and report formats of DGCIS,

   vi. understanding/ assessment of existing applications from perspective of integration with proposed application,

c) Based on the above study, preparing the System Requirement Specifications (SRS) as per the latest version of the IEEE Standard for drafting the SRS, and obtaining Sign-off of SRS from DGCIS.

d) The SI should try to create an 'agile' SRS, whereby the SRS document remains a flexible document and making small changes are easy.

e) Based on the approved SRS, preparing the Software Design Specification (SDS), based on the principles of Enterprise Architecture (EA).

f) Preparation and submission of Project Implementation Plan in compliance to the project schedule (to be provided later in the RFP document).

5.9. Design and Development of FTSSv2 (Application Software)

The scope would include the following.

a) Development of the departmental FTSSv2 application based on the approved SRS and SDS, including the AI/ML module for data processing.

b) **Agile standard development methodology** should be adopted for Software Development, covering the entire SDLC (Software Development Life Cycle).

c) The applications should be cloud native, i.e., it should exploit the advantages of cloud computing delivery model.

d) The development should be based upon automated workflow system & open standards.

e) SI may use any workflow management software for building all the required workflow features in the application software. ***All the applicable licenses (if any and as applicable time-to-time) shall be provided by SI and procured in the name of DGCIS.***

f) The SI should identify and integrate the new application with all internal and external systems and services as per the requirement of the proposed system.

g) The FTSSv2 must have integrated security/ monitoring features with the following:

   i. Definition of Roles/ user group/ user type and Users

   ii. Define Role-wise add/ edit/ view/ delete rights for each Entry Form/ Report in all modules

   iii. Digital Time and User Stamping of each transaction

   iv. Online monitoring of the User activities using user activity logs

   v. Encryption of data wherever required

h) The information and forms collected from various sources and the development of the application software will have to be converted into appropriate electronic open standard format(s) as mentioned in 'Interoperability Framework for E-Governance in India'- v1.0 issued by Ministry of Electronics & Information Technology (MeitY), Government of India.

i) The audit trail should provide a facility to trace the path of changes in application software.

j) The SI would also ensure that the hosting services should be portable to another vendor without any changes to hosting environment.

k) The SI should configure specific system modules and third-party applications, if and when required.

l) The SI should carryout testing of the FTSSv2 including unit testing, integration testing, system testing, etc. along with User/ Final Acceptance Testing and share test reports.

m) The SI should conduct various testing including Load Testing, Performance Testing etc. and making necessary changes to the proposed IT system based on such test results. SI shall share such test reports.

n) All tools required for load testing and performance testing should be standard. In case any third-Party tools are required, the same are to be arranged by the SI for this project on its own cost.

o) The SI should undertake any other work required to complete the proposed revamped IT system as per requirement of DGCIS.

p) **The SI is required to provide detailed profile of the team proposed for application development phase in their response to the RFP (after it is published) which shall not be alterable under general circumstances.**

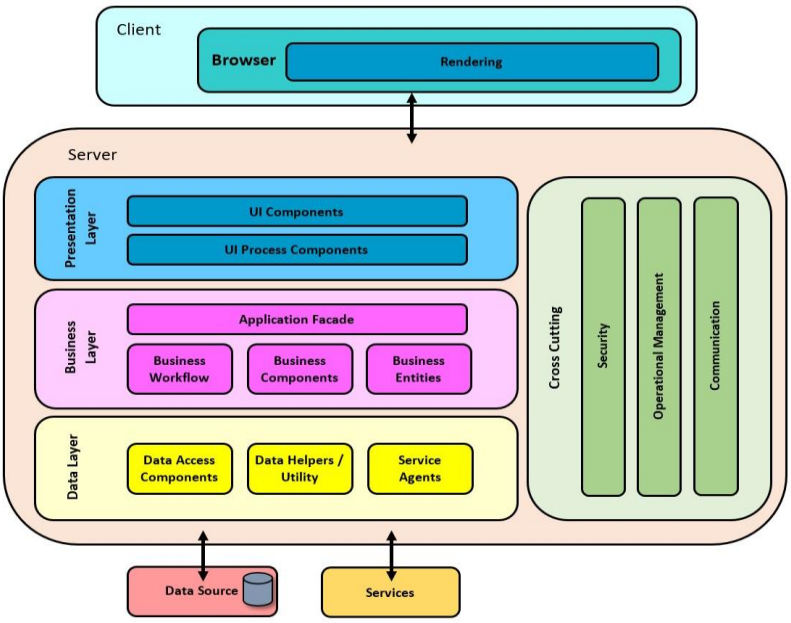


Figure 1: Web Application Architecture

5.10. Integration of FTSSv2

a) The SI will be responsible for integration of FTSSv2 with CBIC ICEGATE SFTP Server, SEZ SFTP Server (NSDL), through development of appropriate programs and APIs.

b) Identify the data/ services which is to be exchanged between the FTSSv2 and the other internal/ external systems and DGCIS website and develop relevant programs.

c) Identify integration touch points for ensuring seamless integration with these internal/ external systems and DGCIS website.

5.11. Design and Development of Applications for Dissemination channels

Integrated Dashboard: The new dashboard will be the main platform for a user to visualize, analyze and, thereby, gather insights from the data as well as download the data as per their requirements. With the help of GUI tools, the user should be able to create graphs and charts as per his / her necessity. In order to analyze the data, the user should also be able to do a **drill down** of the data – i.e., instantly shift from an overview of the data to more detailed and granular view within the same dataset by clicking on a metric in the dashboard. The user should also be able to **add-on** several columns for analyzing the data. For descriptive analysis, data-segmentation tools such as pivot-tables, graphs and charts, should be present. For predictive analysis, basic tools such as fitting of trend-lines and regression lines should be available with the help of GUI. The dashboard has to be made efficient in regard to speed of performance and incorporation of user-friendly features.

Additionally, there should be an option to display similar economic indicators through the process of web-scraping. For example, if the user is interested in the trade of tea, then after analyzing the data of tea he/ she would like to know few economic indicators such as annual production, domestic annual consumption, etc. about tea. This information on economic indicators should then be made available through web-scraping or any other technique.

The dashboard should be a combination of the present Exim Analytics Dashboard, Data Dissemination Portal and the Business Intelligence Module and more. That is, the functionalities of the new dashboard should include all the functionalities of these three portals /modules. Additionally, it may include one or two extra modules, the idea of which may crop up during discussion of the design with the SI and/or as suggested above.

Integration of Payment Platform with the Dashboard: At present, the users of the Data Dissemination Portal can use a query to select the data they want and then purchase the data by paying through a BillDesk Payment gateway - which is integrated with the portal. Therefore, the new Dashboard should have an option for the users to select the data they require and have multiple payment channels, including UPI, integrated with the Dashboard through which they can purchase the data. This functionality should be made and added to the dashboard in a modular nature, so that as and when there is a decision to make data downloading free for users, this functionality can be turned off easily. Further, there should be some functionality to collect statistics on visitor count, number of downloaders, amount of data downloaded, total amount received by DGCIS from users, etc..

Chat-bot or AI Assistant: There should be a chat-bot in the dashboard to assist the user to cull out the data they desire. There should be a counter to count the number of issues resolved by the solely by the chat-bot.

Key Requirements of Dashboard

a) Intuitive and easy to Navigate -The design should be visually appealing, user-friendly, have a unified look and feel and provide easy navigation throughout.

b) Design - Dashboard should be developed utilizing modern design and standards, compatible with all the modern browsers (Mozilla, Firefox, Safari, Chrome, Internet Explorer, Opera etc.) while providing graceful degradation for older browsers.

c) Search mechanism - Dashboard should have an AI-powered search function with various attributes to choose from. Sub-searches should also be available based upon various filters.

d) Presentation of Data - Dashboard should present data in various forms such as pie-chart, graphs etc. Data should be print friendly and user should be able to share the desired data via email, social media channels etc. User should also be able to download the desired data in various formats such Word, Excel, pdf etc.

e) Multi-platform support - The dashboard should be developed as Responsive, supported on major hardware platforms such as desktops, mobiles and hand-held devices, etc. The solution should automatically render a mobile-friendly view when opened on a browser of a mobile device.

f) Integration with website - The dashboard needs to be integrated with the DGCIS website.

g) User Management – Admin: The admin should be able to manage the overall content of the Website and Dashboard through a customized dashboard (as is the case at present) and also should have the option to edit/ delete contents. Through the Admin panel, the administrator should be able to make small amount of changes in the dashboard. The administrator should be able to create users as per the requirement and assign necessary permissions to update/delete/modify the content, similar to the current application.

Website: The architecture and functionalities of the website will primarily be the same as the present website. The look and feel of the website, along with the display of banner images as well as the design of the home page and all other pages are to be revamped.

Mobile App: The mobile app should contain the functionalities of the new dashboard, as many as possible, suited to ease of access through mobile devices.

The website and the mobile app should be cloud native applications and should not use any proprietary services of the Cloud service provider. They should be cloud agnostic so that they are readily portable from one cloud to another.

Key requirements of Mobile App

a) The Mobile Apps should provide an intuitive and user-friendly GUI that enables users to navigate and apply actions with ease. The GUI should be responsive with very little or no delays or time lag at launch or whilst navigating through screens.

b) The Mobile Apps should enable ease of configuration and changes to existing GUIs, and support the introduction of new screens.

c) The Mobile Apps should provide on screen tips and online help to aid users while interacting with it.

d) Should make use of data available in the existing Database and reduce duplicate data entry

e) Provide way for users to provide feedback on the mobile apps, a quick way to report bugs, and provide suggestions.

f) For a feedback mechanism, incorporate analytics to track and identify users experience and actions.

g) Apps should be easily customizable

h) Network level security, traffic should be encrypted using secured connectivity

i) Should provide mobile Apps download based on phone OS and services

j) Apps should structure overall content with proper tagging to make them screen reader friendly.

k) Apps should ensure Compatibility with all platforms like windows, Android, Blackberry & Mac iOS etc.

l) Apps solution should develop Resolution independent design structure i.e. Mobile Apps should adjust itself automatically as per the screen resolution of the Mobile i.e. 1024*768, 1200*800 etc.

m) Mobile Apps should work flawlessly across different platforms

n) There should be minimum use flash contents so that home page should be loaded quickly.

o) It should not occupy excess RAM of the client device.

p) There should be a mechanism to collect statistics on the usage of the app by various users.

Important Parameters for design of Dissemination channels

a) Performance of the dashboard, i.e., speed with which the results will be displayed, is of paramount importance in designing of the dashboard.

b) Security of data and the dissemination platforms - It should conform to standard industry security guidelines such as Guidelines for Indian Government Websites (GIGW),

c) Accessibility – It should conform to industry accessibility guidelines such as World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0.

5.12. Data Migration

The System Integrator shall perform the data migration from existing online portal/existing database to an open-source relational database platform such as PostgreSQL, etc.. *The database which is to be procured must have support from enterprises and should not be community supported products.* The Data Migration to be performed by the System Integrator shall be preceded by an appropriate Data Migration strategy & methodology prepared by System Integrator and approved by DGCIS. Even though DGCIS is required to provide formal approval for the Data migration strategy, it is the ultimate responsibility

of System Integrator to ensure that all the data sets which are required for operationalization of the agreed user requirements are migrated and validated. Any corrections identified by DGCIS, during Data Quality Assessment and Review, in the data migrated by System Integrator, shall be addressed by System Integrator at no additional cost to DGCIS.

Broadly, data migration will consist of the following activities:

i. Conduct Data migration study and submission of data migration report
ii. Define all the specifications that are needed to populate the data into the new system
iii. Prepare uniform codification of all data sets
iv. Develop the data migration templates/ Forms/ Format and facilitate the migration of legacy and new data elements into the new system.
v. Profiling the data present in the legacy systems to identify what data is available and/or needs transformation
vi. Extracting the required data from the legacy system
vii. Transforming the extracted data to the form/format as required
viii. Cleansing the transformed data of any inconsistencies and errors
ix. Loading the cleansed data into the proposed system
x. Arranging for a hands-on training of the officials of DGCIS on how to use the new relational database platform such as PostgreSQL.

5.13. Testing of FTSSv2 and all other applications

a) Preparation and submission of detailed testing plan and strategy.
b) Prepare and share various use cases and scenarios regarding testing, etc.
c) Performing unit testing, integration testing, system testing, load testing and security testing. Security testing (safe to host audit) shall be carried out by CERT-In empanelled agencies.
d) Conducting testing of various components/ modules of the FTSSV2, as per the latest version of the IEEE 730 standards. The bidder shall be required to share the testing documents and standards with the designated software testing team, wherever applicable/ required.
e) Taking corrective steps based on the testing reports i.e., rectifying the software issues/ bugs reported during the testing.

5.14. User Acceptance Testing (UAT)

a) The SI will conduct User Acceptance Tests (UATs) to ascertain whether the proposed IT system or any sub-system(s) is capable of meeting the functional and technical requirement as per the RFP and Performance requirements.

b) Preparation and submission of detailed UAT plans.

c) Submit Test Cases along with results with DGCIS for review and verification at the time of UAT.

d) Prepare and submit various use cases, scenarios along with results with DGCIS for carrying out UAT.

e) The SI shall conduct orientation workshop(s) for the users before handing over the application to DGCIS for UAT.

f) The orientation workshop shall be conducted at the location(s) prescribed by DGCIS.

g) UAT shall be done jointly by DGCIS, SI and PMU (appointed by DGCIS). SI shall assist DGCIS and PMU in carrying out UAT of FTSSv2.

h) Rectifying the application software (FTSSv2) issues/ bugs reported during the testing to be compliant with the test case outcomes.

i) DGCIS may reject any module/ system or any part thereof that fails to pass any test or do not conform to the specifications/ DGCIS requirements. The SI shall rectify such rejected item/ module or parts thereof or make alterations necessary to meet the specifications and shall again perform the testing, all these activities shall be performed at no additional cost to DGCIS.

j) DGCIS will provide full co-operation to the SI in conducting the UAT which shall be carried out on the development server.

k) Final approval/ user acceptance of the application software shall be given by DGCIS after successful implementation and testing. This is the responsibility of the SI to obtain the UAT approval from the DGCIS.

l) All the costs towards testing and commissioning to be borne by the SI.

5.15. Final Acceptance Testing

Pre- requisite of Final Acceptance shall include submission of the following:

i. Software supplied under the RFP including customization & deployment of Software Related solution for DGCIS application, integration, etc.

ii. All documentation related to the developed solution and relevant acceptance test document (including IT Components, Non-IT components).

iii. Installation and commissioning shall include:

   a) Installation and Commissioning of IT, non – IT components.

   b) For both IT & Non-IT equipment's software manuals / brochures / Data Sheets / CD / DVD / media are supplied to DGCIS.

iv. Availability of all the defined services shall be verified and mutually agreed between DGCIS and the selected bidder.

v. Testing must demonstrate that the new systems satisfy the operational and implementation performance criteria mentioned in the RFP document (which is to be published later).

vi. The SI shall be required to demonstrate all the features / facilities / functionalities as mentioned in the RFP(which is to be published later).

5.16. Code Level Audit Review

DGCIS will apply for code level audit (within 1 month from Go-Live) from Cert-In empanelled vendor after Go-Live of the solution. System Integrator shall support DGCIS during such activities. Audit cost will be borne by the selected bidder. **The code level review shall be carried out thoroughly for all modules/sections of the entire application from security and performance perspective and if any kind of vulnerability is pointed out by the auditor, the same shall be rectified/ fixed by the bidder.**

5.17. Performance Review

Performance is another key requirement for the Project and DGCIS shall validate and review the performance of the deployed solution. Performance Review will be a regular activity conducted quarterly for the first year after Go-Live during the stabilization period and subsequently half-yearly for the remaining support periods. Ongoing Performance Review is to be done after Go-Live at the above-mentioned periodic interval of time during the contract period or as decided by DGCIS. This review will be done against certain key parameters defined in SLA, to validate the compliance to all service conditions agreed. DGCIS or its representatives may carry out all the tests detailed in the acceptance test schedule to confirm that the performance of the different modules, subsystems, and entire installation satisfies the specified requirement of specifications including service performance for DGCIS to validate the performance; the SI needs to demonstrate the tests and their results to DGCIS during the testing phase. Such parameters include request-response time, workflow processing time, concurrent sessions supported by the system etc.

The SI shall make available the software programs and test cases required for carrying out the acceptance tests as per the schedule. Any additional test equipment deemed required during validation shall be arranged by the SI at no cost to DGCIS, so as to complete the validation as per the specified time schedule in this document. The SI shall indicate whether the software package includes programs for testing under full load conditions and overload conditions by creation of artificial data in consultation with DGCIS. Such test program shall be provided by the SI for the limited purpose of testing. Any deficiency found during validation in performance of the system as per the requirement shall be rectified by the SI immediately. Any component or module failing during the acceptance tests or requiring alterations necessary to meet specification requirements shall be replaced at no extra cost to DGCIS at site by the SI. These shall be done within two weeks of the initial reports.

5.18. Post Implementation Services

Following are the post implementation services to be provided by the on-boarded system integrator (given in details in next section of this document);

User Support and Maintenance of the application

The scope of application support and modifications and integration with future systems covers the following activities

i. enhancement / modifications with respect to new / enhanced / enriched functionality,
ii. ensuring the desired functioning of the interface / integration,
iii. preparation of test scripts and interim application testing,
iv. installation of application and testing whenever required,
v. modification or preparation of new reports as per requirement,
vi. providing technical support on system parameters and requirement for newly implemented system,
vii. management and administration of databases in accordance with agreed standards,
viii. present relevant information and training if applicable and necessary regarding the use and functions of new products and services to a defined number of relevant users designated by DGCIS, and
ix. providing handholding support to end users in carrying out the business process transactions.

5.19. Bug Fixes and Management

Bug Fixes and Management is an important activity and based on the severity level, it becomes highly critical. There should be committed involvement in resolution of bugs based on following.

- Problem definition
- Request Analysis
- Priority Categorization
- Logging Bugs and tracking to resolution

It should address all the errors/bugs/gaps in the functionality offered by the offered solution (vis-à-vis the FRS) during the operations & maintenance period. It should identify and resolve application problems like system malfunctions, performance problems, data corruption etc. due to which the software related solution for DGCIS may not be able to achieve the desired performance There should be a defined responsibility matrix for the following:

a) updating all available patch/ updates,
b) providing handholding support to end users,
c) ensuring proactive and timely support in identification and provision of solutions including support for resolution,
d) timely logging of Bugs/Problems, and
e) submitting Daily / Weekly / Monthly Status Reports to DGCIS.

5.20. Software Change and Version Control

The Software Capacity Building & Version control process must be defined and approved.

a) The version control and configuration information for the operational system and other application software (if any) must be maintained.

b) All configuration changes or minor customizations to the application which requires development effort should be documented in detail.

c) Changes in the application, which are mandatorily required for complying with any of the predefined requirements, FRS or To-be Functional solution should be treated as extremely important, and hence are to be completed and documented in detail.

d) All changes during the stabilization or support & maintenance phase shall be subjected to the comprehensive & integrated testing to ensure that the changes implemented in the system meets the desired and specified requirements of DGCIS and doesn't impact any other function of the system.

e) A Quarterly Report on the changes performed on the application and resolution of malfunctions carried out should be submitted.

f) Troubleshooting of all possible problems, monitoring of erratic behaviour through the Application Logs should be carried out at the earliest after detection.

g) All planned changes to application systems shall be coordinated within established Change Control processes to ensure that:

   a) Appropriate communication on change required has taken place or proper approvals have been received.

   b) Schedules have been adjusted to minimize impact on the production environment.

h) For any changes to the software, a document indicating proposed changes impact to the system in terms of functional outcomes/additional features added to the system etc. should be submitted and verified by the technical team. The team have to changes/update in portal/application as per instruction given by DGCIS; no extra cost will be paid for change request before Go-live.

i) Approval from DGCIS should be made mandatory for all the proposed changes before implementation of the same into production environment and such documentation is subject to review at the end of each month/quarter.

j) All such documentation should be preserved up to date to reflect the latest enhancements/modifications made to the application. All documentation should be prepared as per latest industry standards and should incorporate necessary version control mechanism.

5.21. Hand-over all required documentation to operate and maintain the system

System Integrator will supply DGCIS the following:

a) System Software / Application including error free source code shall be handed over to DGCIS before Go-Live of the applications and finally before expiry of the Contract.

b) Information relating to the current services rendered and data relating to the performance of the services; entire documentation relating to various components of the Project, any other data and confidential information related to the Project;

c) All other information (including but not limited to documents, records and agreements) relating to the products & services related to the project to enable DGCIS to carry out due diligence in order to transition the provision of the Project Services to DGCIS or its nominated agencies, or its replacing Selected bidder (as the case may be). Such information would also include licences, licence keys, etc. procured in the name of DGCIS.

5.22. Commissioning of FTSSv2 and all other applications

a) Only after the successful completion of UAT and Security Testing from the CERT-In empanelled agencies, the application software shall be deployed on the production environment. The responsibility, both administrative and financial, to get the applications audited shall solely rest with the SI.

b) The SI shall be responsible for installation, integration, testing and commissioning of the hosting environment on the on-premises infrastructure and the additional systems on the cloud platform, along with all the allied equipment, software, updates, patches etc. at the production environment as and when needed.

c) Only after successful deployment of FTSSv2 on production environment, FTSSv2 would be deemed to have been commissioned.

Hosting Requirements

i. SI will be responsible for installation of all the software required for the successful hosting of the FTSSv2.

ii. In case there is any requirement of application specific server at any point of time, the SI shall be required to provide the same also without any additional cost to DGCIS.

iii. Infrastructure should provide sufficient capacity in terms of data processing, data storage and network bandwidth to handle the overall load and traffic coming to the FTSSv2 without compromising the overall performance of the system. The infrastructure should provide dedicated IP, dedicated SSL/ TLS certificate.

iv. It will be the responsibility of SI to prepare the specification for infrastructure i.e., servers, CPUs, RAM, storage, required software, other equipment, and the network requirements for running the FTSSv2 efficiently. Whatever infrastructure is needed shall be clearly accounted in the bid document.

v. Appropriate redundancies shall be built in IT infrastructure as per standard industry practices. The SI shall inform DGCIS about the cost of hosting of FTSSv2 on on-premises infrastructure and share the appropriate documentary proof.

vi. The SI shall formulate an effective Back-up Strategy and Disaster Recovery Plan and shall be responsible for implementing the same at the time of commissioning of FTSSv2.

vii. It is mandated that the SI shall host the DGCIS applications other than FTSSv2 on the MeitY empanelled CSPs. In no case, SI shall host the application on cloud platform of any company which has a history of data loss and security breaches.

viii. SI shall be configuring the DGCIS provided domain name on its servers.

5.23. Go-live of FTSSv2 and all other applications

a) After successful commissioning of FTSSv2, FTSSv2 would be declared as Go-Live and enter into AMC phase, and the SI would be issued a Go-live certificate by DGCIS.

b) SI shall share all the passwords/ access rights/ addresses along with all relevant details of the application/ server/ database/ hardware (if any) with DGCIS from the day of Go-live.

c) SI shall also handover complete, fully tested/ audited, bug free, final version of FTSSv2 source code (in softcopy format) along with the signed hash of the final source code printed on the SI letter head and complete details of technology and software (with versions) used for the development of FTSSv2.

5.24. Documentation

DGCIS shall review the project documents developed by SI including requirements, design, installation, training and administration manuals, version control etc. Any issues/gaps identified in any of the above areas, shall be addressed to the complete satisfaction of DGCIS.

a) Preparation of the documents, like but not limited to, Software Requirement Specification (SRS), screen layouts, Software Design Specifications (SDS), Change Management Plan, Training Plan, Test Cases, Scenarios & Results, Software Code (softcopy), User Manuals, Training manuals, Operations & Maintenance Manual, Administrator Manual, Security Policy, etc. as per acceptable standards.

b) Updating all above mentioned documents time to time, specially whenever there is any change, update in the FTSSv2. Submit all the updated documents to DGCIS

c) Obtaining sign-off for all the documents from DGCIS.

d) Provide OEM documentation with every unit of the equipment supplied. The language of the documentation should be in English. The technical documentation should include illustrated catalogues/ reference manuals/ technical manuals and operation manuals.

e) The Selected bidder will provide all software related documentation, Indicative list of documents include:

- High Level Design Document.
- Low Level Design Document.
- SRS Documents.
- User Manual.
- Training Manuals.
- Unit Test Cases.
- UAT Report.
- Performance Test Report.
- Various Reports during the O&M phase like utilization, issue report, performance, etc.
- Knowledge Transfer.

5.25. Training and Capacity Building

Training of key stakeholders is essential for ensuring that the software developed is actually put to use. Hence, the SI shall ensure a proper training to the designated end-users on the system so as to make them well conversant with the functionalities, features and processes built in the proposed system.

a) Training Plan: The selected bidder shall provide comprehensive and detailed training plan describing the proposed approach & methodology, calendar/ timelines, course contents, course duration, training materials, training tools, training logistics, etc.

b) The content of the training plan and schedule shall be prepared by the SI in consultation with DGCIS at an appropriate time period. The SI shall submit the final document for approval of DGCIS before initiating the training activity.

c) Training Overview: The training overview shall be provided to DGCIS's Steering Committee and PMU members (if proposed) before beginning of each training phase. SI shall incorporate the changes suggested/ inputs provided by the DGCIS during the training overview. The overview sessions will not be counted in total number of training sessions.

d) The selected bidder shall arrange separate training sessions for different categories of participants in batches (Approx. Batch size: 20+ participants).

e) Training could have multiple sessions as per the need and requirement of the project/ application. Hence, the SI shall conduct Training Needs Analysis of all the concerned staff and chalk out a systematic training plan. There should be sufficient number of trainers in every training session for conducting the training program.

f) Re-training of the above staffs whenever significant changes are made in the FTSSv2 and/ or personnel.

g) Assessment of Training Effectiveness: Evaluate effectiveness of training programs and workshops by obtaining formal feedback from each participant after completion of each training program/ workshop. The SI will be responsible for re-conducting the training of the whole batch in case the average score is less than 70% and the additional cost of such re-training sessions shall be borne by the SI.

h) The requisite training infrastructure like space, seats, projector with screen etc. shall be provided by DGCIS in consultation of SI.

i) The training shall be organized by the SI wherein specialised logistics and supportive facilities (if any), apart from the above-mentioned facilities, should be arranged by the SI only, and all associated cost shall be borne by the SI.

j) SI shall conduct training at the location(s) prescribed by DGCIS

k) The SI shall provide training material like handouts, user manual (role base), the language of training manual shall be in English.

l) The training content and mode of delivery must be approved by DGCIS. Training material should be provided in hard and soft copies both. The SI shall ensure that all the training documentation in Hardcopy and Softcopy is in place (user training, operation procedures, visual help-kit etc.) before beginning each training session.

m) The cost incurred on carrying out the training at prescribed location(s) shall be borne by the SI which includes trainer's and other support team member's fees/ salary along with all incidental expenses like travelling, lodging-boarding, local conveyance etc.

n) DGCIS will bear its own expenses related to travel and lodging of its personnel.

o) SI should also provide online help corner for the users and upload user manuals, self-running demos, save and maintain FAQs online so that users can obtain system specific technical/ functional help online as and when required. The system should also maintain module-wise online user Feedback database.

5.26. Supply of Software/ Application/ RDBMS/ Other related Software/ Licenses

a) SI shall supply all the software with adequate number of licenses procured in the name of DGCIS, required for the proposed system. The ownership of the softwares should rest with DGCIS. Original invoice of procurement of all hardwares and softwares should be submitted to DGCIS.

b) The software provided should have the OEM/ vendor support for a period of not less than 5 years from the date of go live.

c) Software tools for implementation, Data Migration, testing etc. shall be part of the offered solution and shall be arranged by the SI without any additional cost to DGCIS.

d) All support services including updates, upgrades and patches for all software modules shall be provided by the SI till the end of the AMC period.

5.27. Authorization, Security and Access

a) The SI shall assist DGCIS in formulating appropriate security/ authorization, control policy to prevent unauthorized access to the DGCIS network, IT on-premise infrastructure as well as to the FTSSv2 components e.g., programs, data, screens and outputs.

b) The SI shall build adequate access rights and control mechanisms into the proposed IT system to prevent any unauthorized access to the FTSSv2 or any of its part/ data/ information.

5.28. Business Continuity Planning

The selected bidder shall prepare and implement the Business Continuity Plan for DGCIS. The strategy should include details of infrastructure, location, operations, management and policies based on Business Impact Analysis carried out in consultation with the DGCIS officials.

5.29. Disaster Recovery Drill

It has been decided that a separate Data Recovery (DR) Centre is not to be maintained for the time being as it would entail unnecessary financial burden. Regular back-ups of all the applications are to be taken and uploaded to a NIC location in a different seismic zone. A periodic drill is to be conducted every quarter whereby the SI is to restore the systems using the backups. This is to ensure that in the event of a disaster the applications can be re-started with the latest backed up data with minimum time lag.

The Disaster Recovery drill will be taken before Go-Live of the applications and successful drill will be an acceptance criterion. Subsequently, a drill is to be taken once every three months. The drill shall ensure that in case of a disaster a smooth and proper transition happens.

5.30. Disaster Recovery and Back-up Policy

a) The SI shall formulate an effective Back up strategy and Disaster Recovery Plan and will be responsible for implementing the same during the contract period.

b) The SI shall revise/ update the backup policy keeping pace with the technological advancement.

c) The SI shall test the effectiveness of the Back-up Strategy.

d) The SI shall submit the DR drill report to DGCIS.

5.31. General Scope

a) The SI must provide comprehensive on-site warranty/ on-site maintenance duly backed up by authentic OEM support for the entire IT infrastructure supplied and installed under the project and thereafter maintenance phase for the entire period of contract as per the agreed SLA.

b) Preventive maintenance services to be carried out at least once in a quarter (3 months).

c) Corrective maintenance services to be carried out as and when required.

d) Asset management services i.e., creation of a database of all the IT hardware (if any) and software assets, record installation and removal of any asset and inform DGCIS even if it is temporary, register all the licensed software with the respective OEMs and maintain the registration details.

e) Configuration management services i.e., maintaining the record of all the hardware and software configurations, to ensure that no unwarranted changes are carried out, version management of the configurations, accessibility of the configurations should be only with the admin and designated officials.

f) Vendor management services i.e., coordination with external vendors/ OEMs/ CSP/ ISP etc., maintaining the database of all the vendors with their contact details.

g) Server management services i.e., administration, performance tuning, patch management, usage statistics, access details, logs, security etc.

h) Backup and recovery of all the system software, application software, database, etc. as per the Standard/ CSP policy.

i) SI should ensure that all the software, hardware, peripherals, accessories, subcomponents required for the functionality and completeness of the solution should also be provisioned according to the requirements of the solution. Also, any additional components, sub-components, assemblies, sub-assemblies that would be required to meet the desired performance requirements (as per SLA) will have to be provisioned by the SI at no additional cost to DGCIS.

j) To ensure that the application design and implementation takes care of necessary security aspects such as data safety, access controls, integrity, backup measures.

k) Bidder should ensure that none of the quoted components and sub-components is declared end-of-sale, end-of-life, and end-of-support by the respective OEM at the time of bid submission. If, the OEM declares any of the products/ solutions end-of-sale subsequently, bidder should ensure that the same is supported by the respective OEM from its date of deployment till the end of the contract period.

l) SI will be responsible for the generation and submission of necessary documentation required during the entire project by DGCIS.

m) The SI will be responsible for maintaining the required performance levels as per the agreed SLA failing which the penalty, as applicable and as defined in the subsequent sections of the RFP document (to be shared later), shall be imposed on the SI.

5.32. Scope of Work for Cloud Service Management

The System Integrator will be responsible for the following:

i. Bidder shall be responsible for procuring, setting up, installation, configuration, management, upgradation, and migration of application servers, database servers/storage to the cloud environment. The cloud must be a 'MeitY- empanelled cloud'.

ii. The indicative list of DGCIS's applications / portals to be migrated and hosted in the procured cloud environment are given as follows;
    (a) Integrated Dashboard (to be developed)
    (b) DGCIS Website (to be re-developed)
    (c) Exim Mobile App (to be re-developed)

iii. Maintain and manage the required network components for the cloud services procured by the SI for DGCIS. Setup and configure the VMs, storage, Network, Database etc. at DC site meeting requirements of DGCIS.

iv. Service provider shall be responsible for implementation, management and monitoring of Distributed Denial-of-Service (DDoS), Intrusion Prevention System (IPS), Intrusion Detection System (IDS) Services, etc.

v. Service provider will implement anti-malware and conduct regular vulnerability scanning and penetration testing of systems and infrastructure.

vi. Service provider shall have public Services in De-Militarized Zone (DMZ) and High security services in Militarized Zone (MZ).

vii. Service Provider shall configure external connections to the hosting infrastructure required to upload database/files etc.

viii. Service provider is expected to understand the complete architecture of existing applications and processes necessary for smooth migration of applications and databases including interdependencies between applications and data.

ix. Service provider shall be responsible for deployment of Security patches on Hardware and Software.

x. Bidder will be responsible for migrating to cloud and managing the cloud services.

xi. The bidder shall be responsible to monitor the cloud services and ensure 99.9 % uptime of all services as per agreement.

xii. Deployment of specified Applications on cloud, security administration, planning and implementation of cloud management and monitoring portals for complete infrastructure and services procured.

xiii. Provide access to DGCIS for installation/commissioning and management of Virtual Machines. Provisioning of scalable storage capacity as per requirements of DGCIS and availability of such services as per agreement.

xiv. SI shall provide necessary technical documentations, design documentations, standard Operating Procedures (SOPs) required for operations and management of services.

xv. SI shall have provision to provide and support additional VM requirements and related services.

xvi. SI shall provide necessary details including sizing, current loads, utilization, expected growth/demand and other details for scale up/scale down at the end of first year in close coordination with DGCIS.

xvii. Monitoring of performance, resource utilization and other events such as failure of services, degradation of services, availability of network, storage, Database systems, OS etc.

xviii. The applications should be cloud native and should not use any proprietary services of the Cloud service provider, i.e., services which are specific to a particular Cloud Service Provider and are not available with other similar providers. They should be cloud agnostic so that they are readily portable from one cloud to another.

5.33. Project Management

a) Co-ordinate all activities with the Program Management Unit (PMU)/ Steering committee set-up by DGCIS.

b) Ensure timely delivery of all the deliverables related to proposed IT system.

c) Supervise and ensuring delivery, installation and commissioning of IT infrastructure as per BOM supplied with the technical bid.

d) Co-ordinate among various stakeholders and other vendors.

e) Ensure that day to day issues related to the proposed IT system are handled and solved immediately.

f) Monitor risk management related aspects and project delays;

5.34. Project Monitoring and Reporting

a) The Bidder shall describe the proposed project monitoring and reporting methodology in the bid which is to be published later.

b) SI to submit a written weekly progress report to DGCIS for review. The frequency of report submission can be modified mutually during critical phases of the Project.

c) Report exceptions and issues that require immediate attention of DGCIS on a regular basis.

d) The SI's Project Management team will be responsible for updating the Program Management Unit (PMU)/ Steering committee of DGCIS in progress review meetings to be held at periodic intervals.

5.35. Scope of Work for DC installation and Commissioning

The System Integrator will be required to procure and install the in-scope hardware IT infrastructure for DC and thereafter maintain the same as per the scope of work mentioned in

this section. The scope shall include procurement, supply, transportation, storage, unpacking, installation, testing, successful commissioning and satisfactory completion for the DGCIS Data Centre.

DGCIS shall provide the necessary minimum constructed space for DC. The System Integrator shall do the site preparation for DC – which includes all non-IT components such as civil and electrical works.. Data Centre shall be located in DGCIS premises in Kolkata. The SI shall take necessary clearances from DGCIS for civil, electrical, and mechanical works including false ceiling, partitioning, installation of electrical component, cable laying etc at DC. **The SI shall also be responsible for assistance in procurement of necessary cloud infrastructure from NIC for taking regular backups for Disaster Recovery Drill** as mentioned in Section 5.31. Disaster Recovery Drill.

The SI shall also be required to arrange for an **auditing of the electrical systems** of the DC. Only after a successfully audit the SI may commission the DG.

The list of work of the SI would include

i. Procuring, setting up, installation, configuration, management, upgradation and support the IT infrastructure required for the DC

ii. Data Centre IT Management facility (e.g., server, storage, network, security, and allied items) for management and monitoring of the entire DC

iii. Consider the following to setup and build the DC:

   a. Scalability
   b. Availability
   c. Security and
   d. Manageability

iv. Procure, Supply, install, and commission the required cables, PDUs, sockets, distribution boards etc. as per requirement of the existing electrical system. If required SI shall accomplish the assessment of existing electrical system without any extra cost.

   a. Check the earthing of each rack connection.
   b. Check the connectivity of the rack from the UPS
   c. Test the power failover of racks.
   d. Perform testing on installed electrical system.
   e. Perform cable dressing and labelling

v. Supply, Installation and Commissioning of Network, Network, Server and Storage Equipment:

   a. The delivery of all equipment / software / services would be accepted only after inspection, testing and approval of the equipment / software / services by the authority specified by the DGCIS, if required so. Inspection charges would be borne by the bidder only and the DGCIS would make no extra payment in this regard. If the equipment's are found to be refurbished, same shall be rejected by DGCIS.

b. The bidder shall be responsible for understanding the existing compute architecture and based on that revamp the configuration and architecture after consultation with DGCIS

c. The bidder shall be responsible for submitting Post Implementation document to DGCIS which consist of architecture, configuration etc.

vi. SI should procure, configure and commission all IT hardware, network components and non-IT requirements for setting up the DC and DR-backup.

vii. The methodology used by SI should ensure that the Data Centre Site Hardware can be rapidly deployed.

viii. SI must also procure and successfully install all the system software such as operating systems and any other software for using the DGCIS system

ix. The proposed components must be forward-looking with at least a seven-year horizon to start with; should also accommodate any scaling up requirements necessitated in future.

x. The SI would provide Installation and Commissioning Report to DGCIS.

Further, the following are to be maintained:

i. Infrastructure should provide sufficient capacity in terms of data processing, data storage and network bandwidth to handle the overall load and traffic coming to the FTSSv2 without compromising the overall performance of the system. The infrastructure should provide dedicated IP, dedicated SSL/ TLS certificate.

ii. It will be the responsibility of SI to prepare the specification for infrastructure i.e., servers, CPUs, RAM, storage, required software, other equipment, and the network requirements for running the FTSSv2 efficiently. Whatever infrastructure is needed shall be clearly accounted in the bid document.

iii. Appropriate redundancies shall be built in IT infrastructure as per standard industry practices. The SI shall inform DGCIS about the cost of hosting of FTSSv2 on on-premises infrastructure and share the appropriate documentary proof.

5.36. Change Request

i. DGCIS may at any time, by a written order given to the SI, make changes in scope of the work or schedule of services as specified in the RFP document, which is to be published later.

ii. While approving any change request, if required, DGCIS may ask the SI to deploy the required resources on-site.

iii. The change request/ management procedure will follow the following steps:

a) Identification and documentation of the need for the change: The information related to initiator, initiation date and details of change required, and priority of the change will be documented by DGCIS.

b) Analysis and evaluation of the Change Request: Impact of the change in terms of the estimated effort, changed schedule, cost and the items impacted will be analysed and documented by the SI.

c) Approval or disapproval of the change request: DGCIS will approve or disapprove the change requested including the additional payments (as per the quoted man-month rate), after discussion with SI on the impact of the change on schedule. Any change request where the total man-month effort requirement is upto the 15 man-days shall not be considered as change request, and shall have no financial implications on DGCIS.

d) All changes outside the scope of work or Schedule of Services having financial implications in terms of the overall cost/ time of the project, shall be undertaken by the SI, only after securing the express consent of the DGCIS.

e) Implementation of the change: The change will be implemented in accordance with the agreed cost, effort, and schedule by the SI as mutually agreed upon by the SI and DGCIS.

f) Verification of the change: The change will be verified and tested by the DGCIS on completion of implementation of change request prior to deployment on the production server.

iv. Any change request shall be dealt with in accordance with the Change Control Schedule of the RFP (to be published).

5.37. DGCIS's current Application: Module-wise description

The details of various components of DGCIS's application are presented below:

Data Ingestion Component

This Component handles the input data to the online application. The Foreign Trade data gets generated in customs locations and SEZs in the forms of Daily Trade Return (DTRs) from Bills of Entry (BE) for Imports and Shipping Bills (SB) for Exports submitted by the Importers and Exporters, respectively, in various customs offices and SEZs located all over India.

The DTRs from Customs are received in DGCIS in three different modes, namely,

(i) Electronic Data Interchange (EDI) mode through CBIC ICEGATE SFTP Server and SEZ SFTP Server – The DTRs from SEZs are received online through NSDL Server by DGCIS. This data is hosted on the SFTP host server and accessed through IP and dedicated password. The data is in the form of text flat file with specified data format. This data is formatted in the Database field format and uploaded into the system using a telnet client. Periodicity of this activity is daily, i.e., every day the export and import data of the previous day from each of the SEZs and Ports are updated in the database.

(ii) E-mail (non-EDI) data in the form of Excel files – This data is formatted in the Database field format and uploaded into the system using a telnet client. This activity is done as and when non-EDI data is received from the ports via email.

(iii) Hard copy in handwritten formats – This data received is entered into the Database using a Manual Data Entry module. Except for manual data, all other data are uploaded into the main server by EDP (Electronic Data Processing) Division and separate datasets are maintained for export and import. The manual data are uploaded into the main server by officers of Export and Import after data entry through the Manual Data Entry module. This activity is done as and when non-EDI data is received from the ports via post.

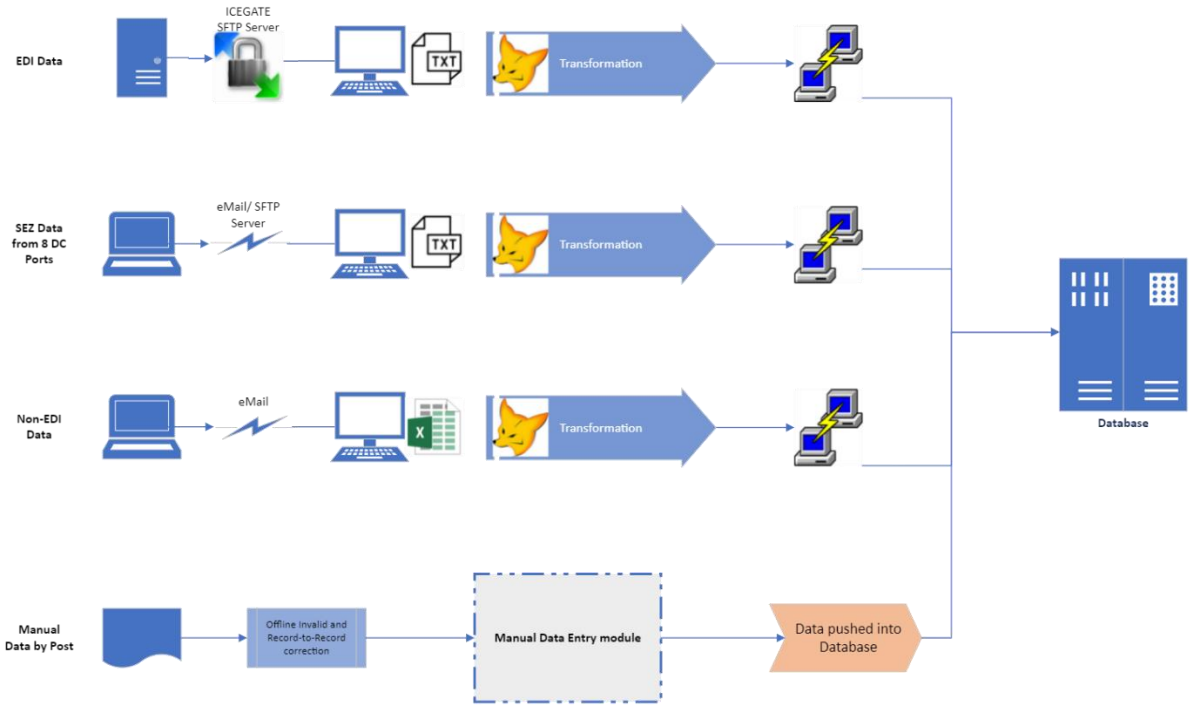


Figure 2: Data Ingestion at DGCIS

Data Record ID (Sequence Number) Generation

After entry into the Database for all DTRs (export and import), a unique Sequence Number is assigned to each entry in the Database. The Sequence number is reset to zero (0) at the beginning of each financial year and each entry in the database is given an incremental sequence number from the last number as present in the Database. Each data entry also contains the date and month of the transaction (Shipping Bill date for export & Bill of Entry date for import).

Invalid Error Generation & Correction Component

After assignment of the Sequence number to each new entry, each of the entries are checked for Invalid Country and Commodity codes (fields in the DTR entry) individually for Export and Import.

User selects the month and year of the database for which the Invalid check is to be run. If the individual Country and Commodity codes in the data entries are not present in the Master Table of Countries and Commodities, a temporary Error table is populated with the Invalid entry for correction.

Error can be of two types:

1. Code does not exist in the Master Table of Commodity/ Country Codes
2. Commodity/ Country Code field is blank

In both the cases, the entries are populated in the temporary table for correction

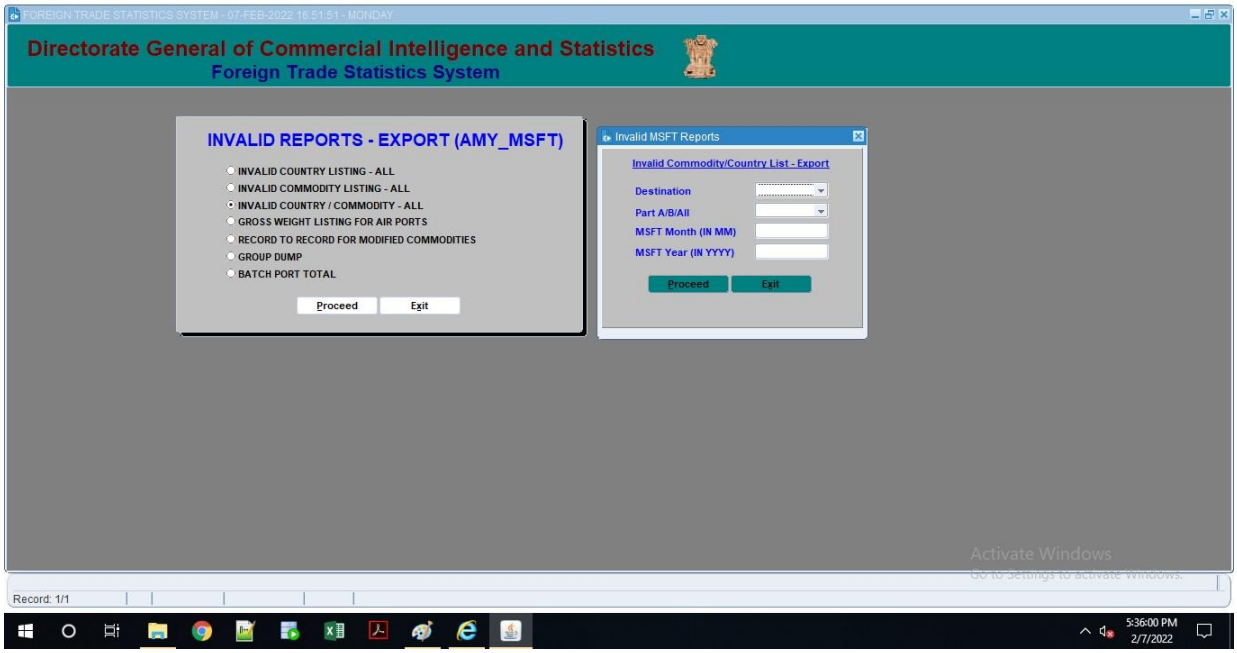


Figure 3: Invalid Error

The temporary table generated for Invalid Country and Commodity codes are distributed for correction amongst the users and the screen for correction is as follows:

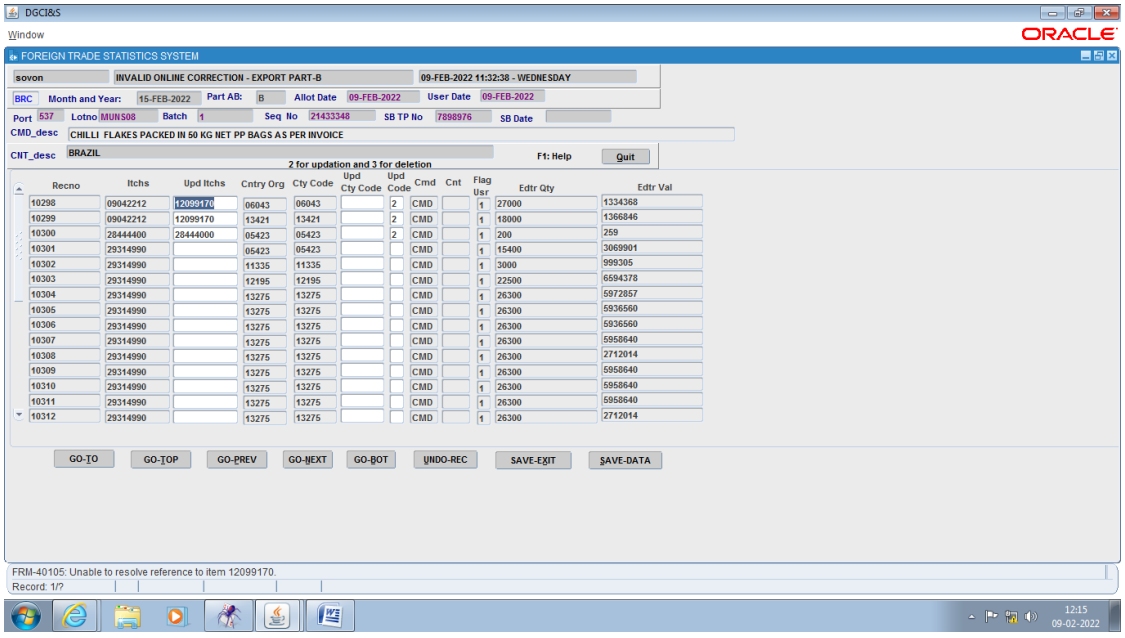


Figure 4: Temporary Table for Error correction

For Invalid Error correction, only Commodity Code (ITCHS) and Country Code are editable for correction, while other fields are non-editable. The user updates the Country and Commodity codes and submits for verification to senior officers and post verification the updated values are pushed into the database corresponding to the original entries.

Error correction for the two error types are as follows:

1. Commodity Code does not exist in the Master Table of Commodity Code – In case of an invalid code entry, the user determines the correct ITCHS Code from the Master Table based on the description of the product or commodity
2. Commodity Code field is blank – In case of a blank code entry, the user determines the correct ITCHS Code from the Master Table based on the description of the product or commodity and updates the Commodity Code for the transaction.
3. Country Code is blank or does not exist in the Master Table of Commodity Code – In case such an error, the user determines the correct Country code based on the description of the item or port of export/ import and updates the Country Code for the transaction.

Auto – Correction/Conversion Component

For each commodity code, a standard measurement unit is defined however, the input data may contain reported unit of quantity different than that of the Standard unit of measurement. In such cases, Stored Procedures are run such that an auto conversion of the unit using the mathematical formula from the reported unit of quantity to the standard unit of quantity.

Group Code Updation Component

All 8-digit Commodity Codes have been classified into 169 Brochure Groups. The commodity codes assigned to each Brochure Group is updated in the beginning of each Financial Year.

After the Commodity Code errors have been corrected, for each individual database entry, Group Code is assigned to the transaction based on the Commodity code, corresponding to the month and year selected.

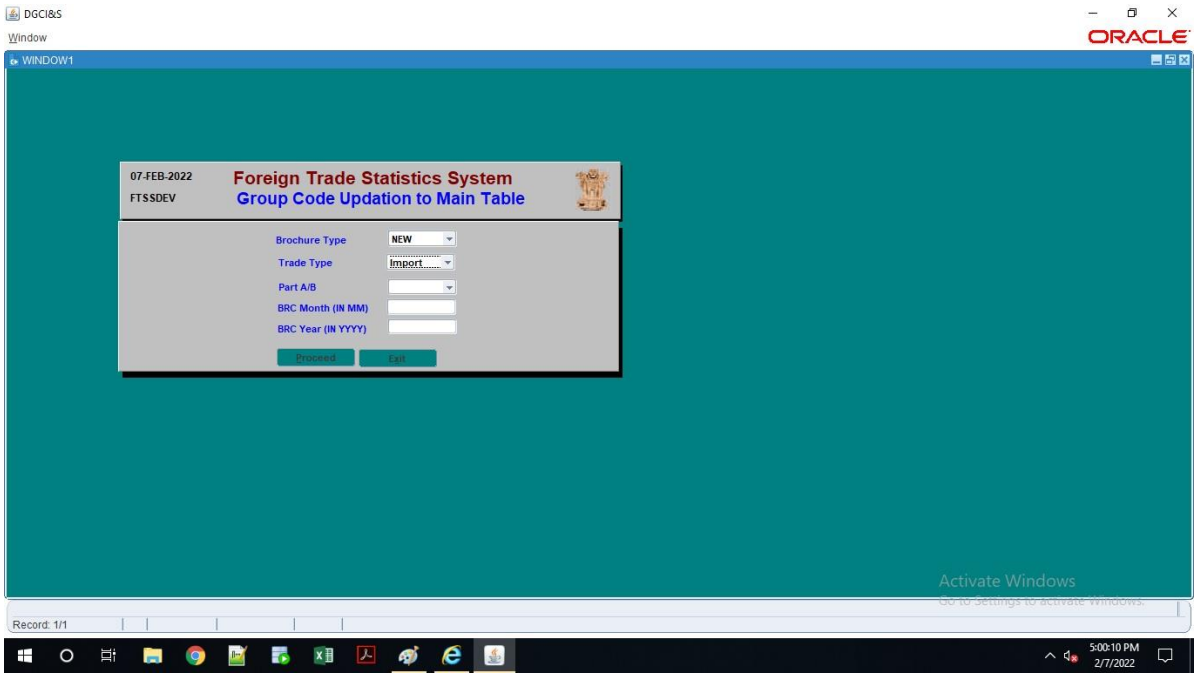


Figure 5: Group Code Updation

Record-to-Record (RR) Error Generation & Correction Component

For all transactions stored in the database, unit value is calculated which is derived by dividing Export/Import Value by the quantity. For all Country Commodity combination, a Historical Mean value is available which are computed on the basis of unit values of historical transactions. The tolerances for each Country Commodity combination are also defined. Upon running of the Record-to-Record check, the transactions where the unit values lie beyond the tolerance range then they are selected for checking.

In this step, those cases are also taken up where the transactions have been reported in units of commercial parlance. These transactions are individually checked, and the reported quantities are corrected to appropriate quantities as per the Standard Unit.

The staff update the quantities of the transactions based on historical reference or if there is a mismatch in the standard units and Commercial units reported based on the description of the commodity provided by the importer or exporter.

Computation of Historical Mean Rates

The benchmark for comparing the current unit values are the historical unit rates. These historical unit rate, which is the mean of the unit values of transactions made in the past months, is computed using the following logic:

1. First the transactions of the past three months are taken for each country x commodity combination. The mean and variance of unit values in these transactions are computed after suitably removing outlier transactions.

2. Then the only those means are taken where the number of transactions is 10 or more. In case 10 transactions are not found in the past three months, then for those country x commodity combinations data for past six months is considered. In case, still there are

less than 10 transactions available, then the means are computed on the basis of past 12 months. If still there are less than 10 transactions, then those country x commodity combinations are dropped.

3. Now, the historical rates are computed only country-wise using the same methodology as elucidated above. These rates are used for those transactions for which the country x commodity combinations have less than 10 transactions and have been dropped earlier.

Group Dump System (Provisional Alpha) Error Correction Component

In this step the unit values are checked country-wise for each commodity against the historical rates. In case the current rates are found to be outside tolerance level then each transaction of that country for the specific time period is checked.

Aggregation of Brochure-MSFT

After successful correction of the errors in the dataset, a month-wise aggregation is run based on the parameters as defined below to the Export and Import data. The transactions corresponding to each of the following parameters are aggregated and collated into a summary table for dissemination.

1. Brochure Code-wise Aggregation
2. MSFT-wise Aggregation
3. State-wise Export data Aggregation
4. Scheme-wise data Aggregation

Master Table creation and Maintenance

The following are the list of Master Tables which are maintained at DGCIS and are updated on a regular basis.

1. Country Code Master Table
2. Commodity Code Master Table
3. Port Code Master Table
4. Brochure Code Master Table
5. State/ Region Master Table
6. Scheme Master Table
7. Lot Master Table
8. Chapter Master Table
9. Unit History Master Table
10. Sensitive Commodity Master Table
11. Section Master Table
12. Dollar Master Table

Application module for Artificial Intelligence and Machine Learning

DGCIS Systems continuously receive, store and process data related to Exim trade from ports concerning all the importers/ exporters across the country. Over a period of time, this data is gathered to provide a lot of statistics comprehension for useful analysis both for compliance as well as to prepare out the interesting patters and exceptions. It is desirable to make use of an appropriate Business Intelligence tool amalgamated with applications of Artificial Intelligence and Machine Learning to analyse and correlate the data and generate reports in various forms which would provide required inputs and enable the policy makers of the DGCIS to develop productive information which will definitely help in better functioning of DGCIS procedures.

The application to be developed by the System Integrator should also have AI-ML components, following are the different AI-ML use-cases basis our initial analysis and discussion with stakeholders:

Case – 1: Blank / Incorrect Country Code

The Data sources for DGCIS' FTSS application are as following:

1. Electronic Data Interchange (EDI) through ICEGATE SFTP Server
2. SEZ Data through e-mail/SFTP server
3. Non-EDI Data through e-mail
4. Manual Data by post

Among the above-mentioned Data sources, the EDI and SEZ data (pts. 1 and 2 above) have pre-decided structures, templates in place and hence the fields are well defined. Thus, the error concerning Incorrect / Blank Country Code does not occur for these data sources. However, for non-EDI and manual data sources, such error may be encountered.

Following are different scenarios under the mentioned case:

a. In the following import data row, the highlighted cell for country code is blank:

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	UoM	Qty	Value	Currency	Rate	Description
1	08133000		Kgs	100	15000	AUD	150	Apple from Australia

Possible application of AI-ML: In the above example, through parsing and analysing the Description field's string or text into logical syntactic components, the AI-ML engine can suggest the COO to be **Australia** and corresponding Country Code can be recommended by the engine by mapping it to be Country Master Table, having the following Structure:

Country Master Table

Code	Country
001	**Afghanistan**
002	**Albania**
003	**Algeria**
004	**Andorra**
005	**Angola**
006	**Antigua and Barbuda**
007	**Argentina**
008	**Armenia**
009	**Australia**
010	**Austria**

Possible Recommendation: The following possible recommendation can be given as an output of the AI-ML engine.

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Recommendation from AI-ML engine	Unit of Measurement	Qty	Value	Currency	Rate	Description
1	08133000		009 (Australia)	Kgs	100	15000	AUD	150	Apple from Australia

If the User accepts the above recommendation, the COO field would be updated, and the AI-ML engine would be trained accordingly.

b. In the following import data row, the highlighted cell for country code is blank and the description contains misspelled Country description

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate	Description

1	11023447		Kgs	100	7000	EUR	70	Pineapple from **Armnia**

Possible application of AI-ML: In the above example, through parsing and analysing the Description field's string or text into logical syntactic components, the AI-ML engine would identify misspelled country name of **Armenia** and thus suggest the correct COO and corresponding Country Code can be recommended by the engine by mapping it to be Country Master Table.

Country Master Table

Code	Country
001	**Afghanistan**
002	**Albania**
003	**Algeria**
004	**Andorra**
005	**Angola**
006	**Antigua and Barbuda**
007	**Argentina**
008	**Armenia**
009	**Australia**
010	**Austria**

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Recommendation from AI-ML engine	Unit of Measurement	Qty	Value	Currency	Rate	Description
1	11023456		008 (Austria)	Kgs	100	7000	EUR	70	Pineapple from **Armnia**

If the User accepts the above recommendation, the COO field would be updated, and the AI-ML engine would be trained accordingly .

c. In the following import data row, the highlighted cell for country code is erroneous, that is, such country code does not exist the Country master table

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate	Description
1	08133000	**1509**	Kgs	100	15000	AUD	150	Apple from Australia

Possible application of AI-ML: In the above example, the AI-ML engine would look-up the COO Code in the country master table and once found unavailable, the engine through parsing and analysing the Description field's string or text into logical syntactic components, would suggest the correct COO - **Australia** and corresponding Country Code can be recommended by the engine by mapping it to be Country Master Table.

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Recommendation from AI-ML engine	Unit of Measurement	Qty	Value	Currency	Rate	Description
1	08133000	**1509**	009 (Australia)	Kgs	100	15000	AUD	150	Apple from Australia

If the User accepts the above recommendation, the COO field would be updated, and the AI-ML engine would be trained accordingly.

Case – 2: Blank / Incorrect Commodity Code

Following are different scenarios under the mentioned case:

a. In the following import data row, the highlighted cell for commodity code is blank:

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate	Description
1		009	Kgs	100	15000	AUD	150	Apple from Australia

Possible application of AI-ML: In the above example, through parsing and analysing the Description field's string or text into logical syntactic components, the AI-ML engine could suggest the Commodity to be **Apple** and corresponding ITCHS code can be recommended by the engine by mapping it to be Commodity Master Table.

Possible Recommendation: The following possible recommendation can be given as an output of the AI-ML engine.

S. No.	Commodity Code (ITCHS)	Recommendation from AI-ML engine	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate	Description
1		08133000 (Apple)	009	Kgs	100	15000	AUD	150	Apple from Australia

If the User accepts the above recommendation, the ITCHS field would be updated, and the AI-ML engine would be trained accordingly .

b. In the following import data row, the highlighted cell for commodity code is blank and the description contains misspelled Commodity description

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate	Description
1		009	Kgs	100	15000	AUD	150	**Aple** from Australia

Possible application of AI-ML: In the above example, through parsing and analysing the Description field's string or text into logical syntactic components, the AI-ML engine could suggest the Commodity to be **Apple** and corresponding ITCHS code can be recommended by the engine by mapping it to be Commodity Master Table.

Possible Recommendation: The following possible recommendation can be given as an output of the AI-ML engine.

S. No.	Commodity Code (ITCHS)	Recommendation from AI-ML engine	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate	Description

1		08133000 (Apple)	009	Kgs	100	15000	AUD	150	**Aple** from Australia

If the User accepts the above recommendation, the ITCHS field would be updated, and the AI-ML engine would be trained accordingly.

c. In the following import data row, the highlighted cell for Commodity code is erroneous, that is, such ITCHS code does not exist the Commodity (ITCHS) master table

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate	Description
1	**081335673**	009	Kgs	100	15000	AUD	150	Apple from Australia

Possible application of AI-ML: In the above example, the AI-ML engine would look-up the ITCHS Code in the Commodity master table and once found unavailable, the engine through parsing and analysing the Description field's string or text into logical syntactic components, would suggest the correct Commodity –**08133000 (Apple)** and corresponding ITCHS Code can be recommended by the engine by mapping it to be Commodity Master Table.

S. No.	Commodity Code (ITCHS)	Recommendation from AI-ML engine	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate	Description
1	**081335673**	08133000 (Apple)	009	Kgs	100	15000	AUD	150	Apple from Australia

If the User accepts the above recommendation, the ITCHS field would be updated, and the AI-ML engine would be trained accordingly.

Case – 3: Deviation of Commodity Unit Rate beyond acceptable limits

At present, for a particular Country-Commodity combination, DGCIS records historic Commodity Unit Rate and stores such rates as Historic Mean Rates derived from at least ten such transactions for the particular Country-Commodity combination.

For a given trade record, if the unit rate falls beyond the acceptable limits (defined by 10% to 1000% of the Historic Mean Rate), then the quantity of the commodity is manually adjusted by DGCIS officials to bring the unit rate within the acceptable limit range.

In the following import data row, Rate (highlighted) is less than 10% of Historic Mean Rate for Import of Country-Commodity Combination and hence does not fall within the acceptable limits:

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate (Value /Qty)	Historic Mean Rate for Import of Country-Commodity Combination
1	08133000	009	Kgs	100	15000	AUD	150	1600 AUD/Kgs

Possible application of AI-ML: In the above example, the AI-ML engine would adjust the quantity of the commodity in such a manner that the unit rate falls within the acceptable range (10% to 1000% of the Historic Mean Rate)

Possible Recommendation: The following possible recommendation can be given as an output of the AI-ML engine.

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate (Value /Qty)	Historic Mean Rate for Import of Country-Commodity Combination
1	08133000	009	Kgs	**75**	15000	AUD	**200**	1600 AUD/Kgs

If the User accepts the above recommendation, the Quantity field would be updated, and the AI-ML engine would be trained accordingly.

From the next such transaction onwards, the AI-ML engine would be trained towards modifying the quantity for that particular Country-Commodity Combination in similar manner.

The above-mentioned probable applications of AI-ML is summarized as following:

Blank/Incorrect Country Code

- **Blank Country Code**: AI/ML engine to learn from the product description to suggest the correct country code
- **Blank Country Code & Misspelled Country Description**: Identification of misspelled country name to suggest country code by breaking the description string into logical syntactic components
- **Erroneous Country Code**: Suggest the correct country code based on the text description of goods

Blank/Incorrect Commodity Code

- **Blank Commodity Code**: AI/ML engine to analyze the product description to suggest the correct commodity code
- **Blank Country Code & Misspelled Commodity Description**: Identification of misspelled commodity name to suggest commodity code through parsing & analyzing the description string
- **Erroneous Commodity Code**: Suggest the correct commodity code based on the text description of goods

Deviation of Commodity Unit Rate beyond acceptable limits

- Based on historic Commodity Unit Rates and depending on the Country-Commodity combination, AI-ML engine would recommend adjusting the quantity of the commodity, such that the unit rate falls within the acceptable range

6. Scope of Work during Operations and Maintenance Phase

6.1. An Overview

DGCIS is looking forward for the delivery of the following broad areas of services under this project:

1. IT Infrastructure Management services
2. Application Management services
3. Server Administration & Management
4. Storage Administration & Management
5. Network & Security Management services
6. Backup/Restore Management for Servers, Database, Applications etc.
7. Configuration, administration, customization, upgrade/ patch/ new release deployment
8. BCP Planning and Disaster Management
9. Reporting & Documentation
10. Help Desk Management

11. Training, knowledge sharing for DGCIS employees.
12. Project Management

6.2. IT Infrastructure Management services

The Successful Bidder shall offer Infrastructure Management Services at the Data Centre for DGCIS as part of the scope of work. These are described below:

- System administration and server management.
- Perform all software installations and updates for software considered under the RFP.
- Develop, maintain, and update processing policies, procedures and documentation related to DC and DR-backup IT Infrastructure.
- Coordinate with the DGCIS on process and procedures changes.
- Prepare, maintain, and ensure adherence to batch job or scheduled processing activities.
- SAN and storage management.
- For remote monitoring and management bidder to provide the link and required network components. This cost should be included as a part of services
- Three personnel – Database Administrator, Network Administrator and Server & Storage Administrator shall be deployed full time in DGCIS premises during the maintenance phase of the project.

6.3. Annual Maintenance Contract (AMC) of FTSSv2 and other applications

- During maintenance phase, the selected SI is required to carry out modification (related to scope of work) / additions / deletions of module / functionality to the Integrated Application without any additional costs.
- The support shall address all user level queries, fixing bugs, enhancements, changes to configurations, customizations, patch updates, upgrades, database administration, security, management of day-to-day task related to Domain / System / Database / Application / VC /Network Administration etc.
- The services covered under post implementation support include:
    - Comprehensive Annual Technical Support Services (ATS) on all the licensed software (DGCIS application, associated software components, database, Anti-Virus, operating systems, etc.) has to be provided by the SI for the O&M period from the date of Final Go live.
    - Applications Functional Support (AFS) for the O&M period for the DGCIS application shall cover all the solution components.

Maintenance of the software for all the applications & related solutions provided to DGCIS should be maintained as per the industry standards. The services covered under post implementation support include: -

i. Operations & Maintenance Services from the date of Final Go-Live.

ii. Helpdesk and Client-Side Support services from the date of Final Go-Live.

iii. Software maintenance and support services from the date of Final Go Live.

iv. Application functional (operational) support services for implemented solution from the date of Final Go-Live.

a) The SI shall provide post implementation support for entire AMC period of 45 months post Go-Live which includes maintenance support, technical support, and implementation and deployment of Change Request raised by DGCIS.

b) If any OEM is involved in the process, the SI shall arrange the support from OEM also for the same period.

c) During the AMC phase the SI shall deploy sufficient manpower to ensure seamless operation of the FTSSv2 system whenever required.

d) SI shall transfer the ownership of the FTSSv2 along with the latest version of source code i.e., all software developed/ customized/ configured/ procured etc. and all the procured licenses and support related documents in the name of DGCIS.

e) Post completion of the 3 years and 9 months of maintenance period, DGCIS in its own discretion, may extend the maintenance contract for two (02) years on mutually agreed basis.

f) During AMC phase, DGCIS may request SI, to make necessary changes in the layout, colour schema, content, MIS reports format, input forms layout etc. However, these changes shall be suggested keeping in view that it should not impact the database schema. The selected bidder shall be responsible to make these changes at no extra cost to DGCIS.

g) The SI shall be responsible to maintain version control and archives of source code, content and database.

h) During entire AMC phase, the SI shall submit the detailed monthly compliance report including system generated report from EMS and HMS in hard and softcopy format to DGCIS within first calendar week of the next month, and on need basis as and when required by the DGCIS. The final format of the report shall be finalized by the SI in due consultation with DGCIS.

Maintenance and Technical Support

i. The SI is required to provide detailed profile of the team proposed for AMC in the technical bid of the RFP (to be published later).

ii. The SI shall make available and implement all upgrades of proposed FTSSv2 and related tools during the AMC period.

iii. The SI shall be responsible for deploying additional manpower for smooth functioning of the project and at no extra cost to DGCIS.

iv. During the entire AMC period the SI shall be responsible for (including following, but not limited to):

A. SI shall be responsible for handling all the issues/ problems faced by the users.

B. Installation of new versions/ software/ releases (including next generation release) upgrades, bug fixes, functionality enhancements, patches to cater to changes (including tax, legal, statutory and policy requirements), any modification or enhancement to existing business processes, changes to configurations, customizations, database administration, data back-up and archiving, security and other technical assistance.

C. Overall administration, operations, monitoring, and maintenance, definitions/ patches/ updates/ service packs, backup, recovery, etc. of the deployed IT Hardware and Software infrastructure at the cloud platform and to ensure the desired uptime.

D. Overall monitoring of the deployed network bandwidth/ links so as to ensure the desired uptime. In case of downtime/ link failure, reporting immediately the same to the Internet Service Provider (ISP) and tracking until the link is restored and services are operational as required.

E. In the event of onsite deployed resource(s) leaving the project/ employment, the same shall be immediately replaced with another resource of equivalent minimum qualifications and experience. All such events should be notified to the DGCIS well in advance.

F. At no time, the provided manpower should be on leave or absent from the duty without prior permission from the designated nodal officer of DGCIS. In case of long-term absence due to sickness, leave etc. the SI shall ensure replacements and manning of all manpower posts by without any additional liabilities to DGCIS. Substitute will have to be provided by the SI against the staff proceeding on leave/ or remaining absent and should be of equal or higher qualifications/ experience.

G. Update, modify, re-build, replace any module, feature of the application, at SI's sole cost, to keep the system free from any defect or deficiency in any aspect that prevent the FTSSv2 and/or any of its sub-systems(s) from fulfilling the functional or technical requirements.

H. DGCIS may request SI, to make necessary changes in the layout, colour schema, MIS reports format, input forms layout etc. However, these changes shall be suggested keeping in view that it should not transform in database schema. The

selected bidder shall be responsible to make these changes at no extra cost to DGCIS.

6.4.Server Administration & Management:

The service provider is expected to provide the Server Administration & Management services as follows-

- Service provider shall provide the “Server Administration service" to keep servers stable, reliable and their operation efficient.
- Administrative support for user registration, User ID creation, maintaining user profiles, granting user access, authorization, user password support, and administrative support for print, file, and directory services.
- Setting up and configuring servers and applications as per configuration documents/ guidelines provided by DGCIS.
- Installation/ re-installation of the server operating systems and operating system utilities.
- OS Administration including troubleshooting, hardening, patch/ upgrades deployment, BIOS & firmware upgrade as and when required/ necessary for Linux or any other O.S proposed as part of this solution whether mentioned in the RFP or any new deployment in future.
- Ensure proper configuration of server parameters, operating systems administration, hardening and tuning.
- Regular backup of servers as per the backup & restoration policies stated by DGCIS from time to time.
- Regularly monitor and maintain a log of the status of critical services, performance of servers including but not limited to monitoring of CPU, disk space, memory utilization, I/O utilization, etc.
- Regular analysis of events and logs and maintain the reports for future audit purposes.
- Managing uptime of servers as per SLAs.
- Take appropriate steps to comply with the audit observations made by various internal/ external auditors.
- Depending on the nature of applications deployed, Service provider shall suggest/ implement appropriate security measures on various servers, especially the Web, Application and Database servers.
- Co-ordinate with SSL Certificate service provider for issuing and deployment of SSL certificates.
- Maintenance of Microsoft’s Active Directory (AD) & Additional Domain Controller (ADC).
- Preparation/ updating of the new and existing Standard Operating Procedure (SOP) documents on servers & applications deployment and hardening.

6.5.Storage Administration and Management: -

- Installation and configuration of the storage system.
- Management of storage environment to maintain performance at desired optimum levels.
- Development of storage management policy, configuration and management of disk array, SAN fabric / switches, etc.
- Configuration of SAN storage whenever a new application is hosted in the Data Centre Site. This shall include activities such as management of storage space, volume, RAID configuration, LUN, zone, security, business continuity volumes, performance, etc.
- Preparation of Standard Operating Procedure (SOP) document for the Storage Administration.
- Regularly monitor and log the state of complete cloud solution including but not limited to Servers, Operating System, Storage, Networking, Backup operations, Disaster recovery drills.
- Service provider shall provide L1, L2, L3 & subject matter expert level of support for any issues related to proposed infrastructure to DGCIS at primary Data Centre site.
- Service provider will coordinate with DGCIS to resolve any problems/issues as per SLA.
- Suggest/Help DGCIS on implementing Data Centre best practices as per industry standards.
- Co-ordinate with DGCIS in implementing any changes that might be required towards the deployment/placement within the Data Centre.
- Compliance to IT Security policies of DGCIS/ Statutory bodies.
- Adherence and maintenance of the user access controls as advised by DGCIS.

6.6.Network & Security Management Services:

Service provider will have to provide complete managed services for all networking components proposed as part of the solution like, switches, routers, firewall, load balancers and links. Configure, manage & modify configuration of the network devices / firewall policies as and when required.

Monitoring & Fault Management of:

- Monitoring & management of Internet, P2P, and IPsec VPN Tunnels proposed as part of this solution.
- Bandwidth utilization, latency, packet loss etc.
- Call logging and co-ordination with VPN, Internet Service Providers, Point-to-point line service providers for restoration of links, if need arises.

Configuration Management:

- Configuration of L2 switches for administration and L3 Switches (If any) for VLAN creation / hardening / routing /load sharing etc.

- Maintaining / Updating of Network diagram.
- Maintaining complete details of network hardware along with interfaces, IP address etc.
- Redesigning of network architecture as and when required by DGCIS.

Security Management Services:

- Addressing the ongoing needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion protection, content filtering and blocking, virus protection, and vulnerability protection through implementation of proper patches and rules.
- Maintaining an updated knowledge base of all the published security vulnerabilities and virus threats.
- Ensuring that patches / workarounds for identified vulnerabilities are patched / blocked immediately.
- Ensure a well-designed access management process, ensuring security of physical and digital assets, data and network security, backup, and recovery etc.
- Quarterly (or as required by DGCIS) review of domain level rights and privileges; Modifying access permissions of existing security policies on existing firewall.
- Adding/ Changing network address translation rules of existing security policies on the firewall.
- Diagnosis and resolving problems related to firewall, IDS /IPS.
- Managing configuration and security of Demilitarized Zone (DMZ) Alert / advise DGCIS about any possible attack / hacking of services, unauthorized access / attempt by internal or external persons etc.
- Implementation of IT security policies as advised by DGCIS/ Statutory bodies.
- Resolution and restoration of services in case of any possible attack and necessary disaster management.
- Shutdown of critical services to prevent attack (internal or external) in coordination with DGCIS.
- Event and correlation.
- IPv6 configuration, if required.

Internet & Web Security & Administration

- Coordination with ISPs for installation / configuration of links.
- Monitoring of Internet links and co-ordination with ISPs for restoration of failed link(s).
- Monitoring bandwidth utilization.
- Carrying out configuration changes on router as per the DGCIS requirements.
- Backup, up gradation and restoration of OS, configuration files etc.

- To ensure working of all the DGCIS's URLs and Internet applications from outside DGCIS's Intranet.
- Backup /restoration/synchronization of configuration files of devices.
- Maintaining static NAT table of ISPs.
- Installation/configuration/management/up gradation of the devices / appliances.
- Successful bidder should provide the DDoS mitigation solution which can handle the attack of 1 Gbps.

6.7.Backup/Restore Management for Servers, Database, Applications etc.:

- To perform backup and restore management in coordination with DGCIS's policy & procedures for backup and restore, including performance of daily, weekly, monthly, quarterly, and annual backup functions (full volume and incremental) for data and software maintained on the servers and storage systems using Enterprise Backup Solution.
- To recover from a crash / other local failure at the DR site, without affecting the primary system or replication process in any way. The full backup shall be taken at the end of the week, whereas incremental backups shall be taken every day and log backup of every 4 hours.
- Ensure proper storage and handling of media to prevent data loss.
- Backup and restoration of Operating System, application, databases, and file system etc. in accordance DGCIS with defined process / procedure / policy.
- Monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies.
- Ensuring prompt execution of on-demand backups & restoration of volumes, files and database applications whenever required.
- Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes.
- Installation, re-installation, upgrade, and patch deployment of the Operating System in the event of hardware/ Software failure, OS issues, release of new version or patches by the OEM etc.
- Generating and sharing backup reports periodically.
- Coordinating to retrieve off-site media in the event of any disaster recovery.
- Periodic Restoration Testing of the Backup.
- Maintenance log of backup/ restoration.
- Update/ Maintain Standard Operating Procedure (SOP) documents.

6.8.BCP Planning and Disaster Management:

In view of providing continuous availability of the applications along with complete managed services and disaster recovery services in case of disaster at primary site, DGCIS desires to take regular backups and upload them onto a NIC location in a different seismic zone as detailed in Section 5.30, Disaster Recovery Drill, of Chapter 5 [[check the section]].

6.9.Service Maintenance:

The bidder requires to operate and maintain the cloud infrastructure at NIC location (DR site) as per the scope mentioned in scope of work

1. Monitoring of backup status.
2. Lag in backup due to any unforeseen errors.
3. Network monitoring
4. Security monitoring and analysis
5. Reporting if any issue is arising in replication.
6. Daily backup at DR end

6.10. DR Drills:

- During the DR drill, the SI needs to arrange the full DR team with sufficient resources and expertise and complete the activity under the supervision of senior resource for co-ordination.
- DR drills should be planned and executed periodically, minimum once in a quarter.
- Drills should be carried out over a minimum period of 24 hours each time. Drills can be conducted for all applications together which could simulate the failure of all systems.
- Each application's DR system shall be accepted by DGCIS only after a successful DR drill has been conducted.
- The exact process of the DR drill should be formulated in consultation with the DGCIS team in a way that all elements of the system are rigorously tested, while the risk of any failure during the drill is minimized. The process should be documented by the successful bidder as part of the disaster recovery plan.
- The date, time, duration, and scope of each drill shall be decided mutually between DGCIS and the successful bidder. Extreme care must be taken while planning and executing DR drills to ensure that there is no avoidable service interruption, data loss, or system damage at DC.
- Provide Event Analysis Reports for the disaster recovery solution as a part of the services.

6.11. Reporting and Documentation

SI should submit reports on a regular basis in a mutually decided format that is daily / weekly and monthly uptime/downtime report. Softcopy of these reports shall be delivered automatically via email at specific frequency and to the pre-decided list of recipients.

Submit information as part of periodic review as and when required by DGCIS. Following is the indicative list of reports:

Reporting

- Service provider shall transfer data back to DGCIS either on demand or in case of termination of contract for any reason.
- Summary of component wise Data Centre uptime.
- Summary of changes in the Data Centre.
- Log of preventive / scheduled maintenance undertaken.
- Configuration Management summary report.
- Change Management summary report.
- Service Level Management – priority/severity wise response and resolution.
- Service Failure Analysis, listing out escalations and downtime/outages, if any.

Incident Reporting

- Detection of security vulnerability with the available solutions / workarounds for fixing.
- Hacker attacks, Virus attacks, unauthorized access, security threats, etc. – with root cause analysis and the plan to fix the problems.
- Standard Operating Procedure (SOP) for DR-backup, System Documentation/ User manuals have to be prepared and maintained up to date with version control.

Documentation

Preparation/ Updating of System Documentation of support requirements, upgrade, patching, cloning & migration in detail with version control. This will also include preparation of System document for complete infrastructure/facilities available in datacentre including Server, storage, network, network security configuration and deployments initially complete document and thereafter regular updating of the same with version controls. This documentation should be submitted as the project undergoes various stages of implementation. Indicative list of documents includes:

- Detailed Project Plan
- Project Management Plan
- Details of complete solution deployed for DGCIS in DR-backup site.

6.12. Training, knowledge sharing and skills development for DGCIS employees: -

- Identification of training needs, evaluation of knowledge transfer requirements on the software tools, technologies proposed under this contract.
- Training on system, implemented customizations & personalization. Periodical training need assessment and training to the existing users on the implemented solution as and when required.
- Training Material should be provided which shall include the presentations used for trainings and also the required relevant documents for the topics being covered.

6.13. Help Desk Support:

Bidder is required to create and maintain Help Desk / hotline that will resolve problems and answer queries related to any issues, problems, concerns occurring in systems.

The help desk support to users shall be provided on 24x7x365 basis. The details regarding telephonic support will be carefully considered, as this will have effect on the support response to DGCIS system end-users. The Bidders response and resolution time will be the basis for end- user support time in DGCIS‟s service level agreements with the Bidder.

During the entire period of the contract commencing from the date of Letter of Award, any charges incurred on transport / shipping of hardware / equipment from and to the Bidder's DC Site will be borne by the bidder. No claims will be entertained in this regard. The entire responsibility of covering for damage in transit, making good the damaged parts lies solely with the bidder.

The selected bidder shall document all the installation and commissioning procedures and provide the same to DGCIS within one week of the commissioning of the DR site and within one week of successful execution of DR drill for DR Site. The selected bidder shall be responsible for documenting configuration of all devices / equipment and keeping back up of all configuration files, so as to enable quick recovery in case of failure of devices

6.14. Other Services

- Provides network link, RPO, RTO and performance monitoring tool dashboard access to DGCIS for real time basis monitoring.
- The service provider shall provide necessary training to DGCIS personnel to monitor the various SLAs, monitor the dashboard in event of switchover/switchback at the time of disaster (planned/testing or otherwise).
- Service provider must make the DC site up with the latest data and applications at DR-backup after a disaster (planned / unplanned / drill) has happened.

6.15. Project Management

Successful bidder's responsibilities include, but are not limited to the following:

- Successful bidder shall nominate a Project manager for entire period of the contract for
- interacting with DGCIS nominated person for all the activities under scope of this project.
- Successful bidder shall submit a detailed project implementation plan and clearly spell out important milestones of project immediately after the award of work.

- Successful bidder will submit the BCP plan and details of BCP committee member from bidder side.
- Be responsible for delivery of services and act as a primary interface to DGCIS for all matters.
- Maintain project communications and provide documentation and adhere procedural standards approved by DGCIS for the execution of the project.
- Prepare a service management plan for meeting the desired performance.
- Management of documentation/deliverables as described under the SOW. Measure, evaluate and report on progress against the project plan.

Annexures

Annexure 'A' - (Bidder Information)

Please provide following information about the Company (Attach separate sheet if required):
-

S. No.	Information	Particulars / Response
1.	Company Name	
2.	Date of Incorporation	
3.	Type of Company [Govt. / PSU/ Pub. Ltd / Pvt. Ltd / partnership/proprietary]	
4.	Registration No. and date of registration. Registration Certificate to be enclosed	
5.	Address of Registered Office with contact numbers [phone /fax]	
6.	GSTIN	
7.	PAN No	
8.	Contact Details of Bidder authorized to make commitments to DGCIS	
9.	Name	
10.	Designation	
11.	FAX No.	
12.	Mail ID	
13.	Company Head Office and Addresses Contact Person(s) Phone Fax E-mail Website	
15.	Whether the Bidder is blacklisted/ debarred at the time of submission of this Tender, by Government of India or Central PSU/PSE/PSB/FI/Regulatory Bodies. If yes, please give details	Yes/No/Comments (if option is 'Yes') (If option is 'Yes' Bidder may Not be considered)

Authorized Signatories
(Name & Designation,
seal of the company)
Date:

Annexure 'B' - (EoI Covering Letter)

[To be submitted on letter head of the company]

To

The Head of Office,
Directorate General of Commercial
Intelligence and Statistics (DGCIS),
565, Anandapur, Ward No. 108
Sector– 1 , Plot No. 22, ECADP,
Kolkata, West Bengal 700107 Date :

Subject: Expression of Interest notice for "Selection of a System Integrator for Design, Development, Implementation and Maintenance of Foreign Trade Statistics System".

Dear Madam / Sir,

Having examined the Expression of Interest (EoI), the receipt of which is hereby duly acknowledged, I/we, the undersigned, intend to submit a proposal in response to your Expression of Interest (EoI) as mentioned in subject above. I/we attach hereto the response as required by the EoI, which constitutes our proposal.

2. I/we certify that the information contained in this response or any part thereof is true, accurate, verifiable and complete to the best of my / our knowledge. This response includes all information necessary to ensure that the statements therein do not, in whole or in part, mislead the department in its short-listing process.

3. I/we fully understand and agree to comply that on verification, if any of the information provided here is found to be misleading during the short-listing process, we are liable to be dismissed from the selection process or termination of the contract during the project, if selected to do so.

4. Subject to deviations, I/we agree for unconditional acceptance of all the terms and conditions set out in the EoI document.

5. It is hereby confirmed that I/we are entitled to act on behalf of our company/ corporation/ firm/ organization and empowered to sign this document as well as such other documents, which may be required in this connection.

6. I/we hereby certify to the best of our knowledge and based on documents available that Our Agency/Society/Company/Trust, including our partners in Joint-Venture / Consortium, if any, has not been blacklisted or delisted by any Government, PSUs and its subsidiaries, which may have an adverse impact on the performance of services.

7. I/we understand you are not bound to accept any proposal you receive.

Yours faithfully,

For *<Name of Company>*

<Signature of Authorized Signatory>

Name:

Designation:

Annexure ‘C’ - (Technical Response Template)

Sl. No.	Technical Qualification Criteria	Break up of Parameters	Please mention the following in the space provided in the next column	Score of Bidder
1.	Relevant experience of executing integrated software project(s) (Project Design and implementation) involving complex business processes, rule engine & workflows or have worked for application development projects of similar nature in the last 5 years (min. 2 projects)		No. of projects	
2.	ISO certifications (ISO 27001 or ISO 20000 and CMMi Level 5 & above)	ISO 27001	Y / N	
		ISO 20000	Y / N	
		CMMi level 5	Y / N	
3.	Number of qualified professionals on payroll of bidder holding BE/ B.Tech/ MCA/ M.Sc. (IT) degree and experience of working in the domain of Application development, web portal design/ development, AI and ML based applications including implementation of cloud solution, System Integration, Data Centre setup, project management and planning, system architecture design (min. 500 employees)		No. of such personnel	
4.	Experience of handling large integrated IT projects (>40 crores) for Government Clients (at State and National Level) in the last 5 financial years (central/state government / PSU.)		No. of projects	
5	Project Experience of implementing at least 2 projects invoving development of a large software.		No. of projects	
6.	Project Experience in emerging area of AI-ML (min. 2 projects).		No. of projects	

7	Relevant experience of application hosting and maintenance on cloud platform and providing support on Cloud Data Centre management (min. 2 projects)		No. of projects	
8	Relevant experience of commissioning Data Centre		No. of projects	
			Whether completed 2 Govt. projects ? Y/ N	
9	Has Delivery Centre in Kolkata with at least 500 technical employees		Y / N	

========== End of Document ==========

Purpose of this Report

The Detailed Project Report (DPR) involves an analysis of the existing ICT infrastructure and the FTSS application being used by the DGCIS. The output of this report will be the building block for the future state of the envisaged DGCIS FTSS System.

The main objective of this DPR is to capture the DGCIS requirements pertaining to the FTSS system and areas of intervention required in existing IT system that would steer the technical and functional specification and technology solution for DGCIS. Additionally, Assessing of various feasible options of deployment infrastructure and network connectivity. A detailed cost breakup and financial analysis for revamping the entire solution are some of the other objectives of this report.

The report will be used by DGCIS officials to take guided decision to choose the suitable database, application and infrastructure migration option and also to carry out detailed planning for change management and capacity building as well as prepare the RFP documents for selection of the System Integrator.

1. Background and Context

The Directorate General of Commercial Intelligence & Statistics (DGCIS) is the premier organization of Government of India for collection, compilation and dissemination of India's trade statistics and commercial information. This Directorate, with its office located at Kolkata, is headed by the Director General, an Additional Secretary level officer of Indian Statistical Services (ISS). DGCIS is ISO 9001:2015 certified and is the first to be awarded for any Government Organization.

The main activities of DGCIS are collection, compilation, validation and dissemination of merchandise Foreign Trade data, trade statistics and various types of commercial information required by the policy makers, researchers, importers, exporters, traders as well as overseas buyers. It is the nodal agency for Export & Import data in the country for Compilation and Dissemination of India's foreign trade statistics. The IT solutions utilized by the officers are hosted at a Data Centre (DC) and a Data Recovery (DR) Centre at their premises.

Different users of Foreign Trade Data

- Government Ministries / Departments – central as well as state
- Reserve Bank of India
- Indian Embassies/High Commissions
- Public Sector Undertakings
- Foreign Embassies
- International Organizations like UNSD, FAO, etc.
- Various Export Promotion Councils, Commodity Boards, Industrial bodies
- Private user

The Foreign Trade data gets generated in customs locations and SEZs in the forms of Daily Trade Return (DTRs) from Bills of Entry (BE) for Imports and Shipping Bills (SB) for Exports submitted by the Importers and Exporters, respectively, in various customs offices and SEZs located all over India.

The DTRs from Customs are received in DGCIS in three different modes, namely,

- Electronic Data Interchange (EDI) mode through Indian Customs EDI Gateway (ICEGATE) Server, Data from SEZs through 8 DC ports
- e-mail (non-EDI) data, and
- hard copy in handwritten formats.

The data volume processed at DGCIS and the distribution of records is shown in the following Tables:[1]

Year	Export	Import	Total
2018-19	133,60,422	121,88,592	255,49,014
2019-20	137,43,809	120,87,439	258,31,248
2020-21 (as on 31- Oct-2020)	63,52,012	50,03,294	113,55,306

The percentage distribution of records based on type of records is given below:

Year	Export			Import		
	EDI	**Non-EDI**	**Manual**	**EDI**	**Non-EDI**	**Manual**
2018-19	93.30	6.70	0.00**	95.21	4.78	0.01
2019-20	92.93	7.07	0.00**	94.93	5.07	0.00**
2020-21 (as on 31-Oct-2020)	92.99	7.01	0.00**	94.68	5.31	0.00**

* Non-EDI includes SEZ also
** Data received from manual ports are negligible

[1] https://commerce.gov.in/about-us/subordinate-offices/directorate-general-of-commercial-intelligence-and-statistics/

The DTRs from SEZs are received online through NSDL Server by DGCIS. Except for manual data, all other data are uploaded into the main server by EDP (Electronic Data Processing). The manual data are uploaded into the main server by officers of Export and Import Divisions after data entry through the Data Entry Package.

The Export and Import Divisions validate data at various levels. The level of processing depends upon the stages of publications, i.e., at (i) Principal Commodity (PC) Level Trade data or at (ii) 8-digit item (HS Code) commodity level trade data.

Context

To support the core business application, DGCIS has established an ICT landscape, progressively over the last decade. It has a datacentre and as well as a disaster recovery centre both located in Kolkata. To maintain the entire ICT setup, DGCIS incurs a significant expenditure towards annual maintenance by engaging an IT vendor.

DGCIS is now actively considering reducing the recurring operating expenditure by way of migrating its IT system to open-source systems, without compromising the security and efficiency aspects. DGCIS has engaged Deloitte as a consultant to assist in its endeavour of migration,

This Detailed Project Report (DPR) is the culmination of assessment of DGCIS's current state and the different opportunities available towards the migration.

The broad areas of coverage of the Detailed Project Report encompasses the following:

1. **Migrate DGCI&S's databases from Oracle to PostgreSQL or any other Open-Source Database system**
    - Assess the existing ICT system of DGCIS (Database Platform & Structure) and analysis of available open-source Database Platforms
    - Cost- Benefit and Feasibility Analysis of Migration to Opensource Database and preparation of plans for migration

2. **Migrate all its legacy applications to Open-Source Technologies**
    - Assess the existing software packages and analyse the available Open-Source Application Platform & technologies
    - Cost- Benefit and Feasibility Analysis of Migration of legacy applications
    - Redevelopment or customization of application for migration

3. **Migrate some or all applications and Database to Cloud**
    - Feasibility analysis of the IT environment for Cloud migration
    - Assess Cloud platforms for application scalability, availability, etc.
    - Develop phased strategy for feasible cloud migration

4. **Incorporate Machine Learning principles while modifying / redeveloping its applications**
    - Requirement analysis and mapping of processes with relevant principles / algorithms
    - Best Practice Analysis of AI/ML or other emerging Tech application & define aspired end state processes

2. AS-IS assessment of the ICT Systems

This section provides detailed analysis of the different components of the As-Is study conducted

2.1. DGCIS Applications

On a daily basis, Foreign Trade Data are received from Customs and SEZs in the form of Daily Trade Returns (DTRs) which are part of Shipping Bills (for Export) and Bills of Entry (for Import). After validation, foreign trade data are disseminated in various ways – in the form of Quick Estimates and Press Note released by the Department of Commerce **on the 15th of every month for the preceding month**, Principal Commodity Group by country level information for the Brochure publication, 8-digit commodity level publication for *Monthly Statistics of Foreign Trade of India (MSFTI) and quarterly 8-digit level publication SFTIC (Statistics of the Foreign Trade of India by Countries).*

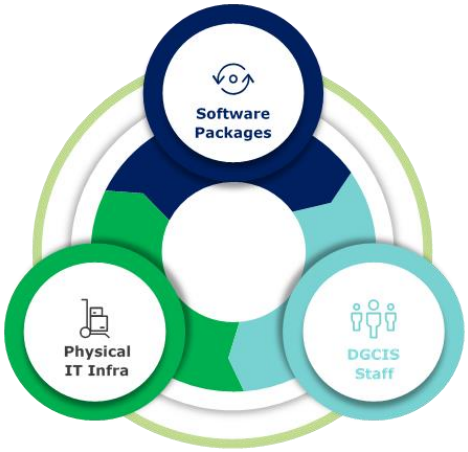


Figure 1: Pillars of DGCIS IT System

Following is a workflow-based representation of the data processing mechanism being followed: The current IT landscape of DGCIS consists of the following elements,

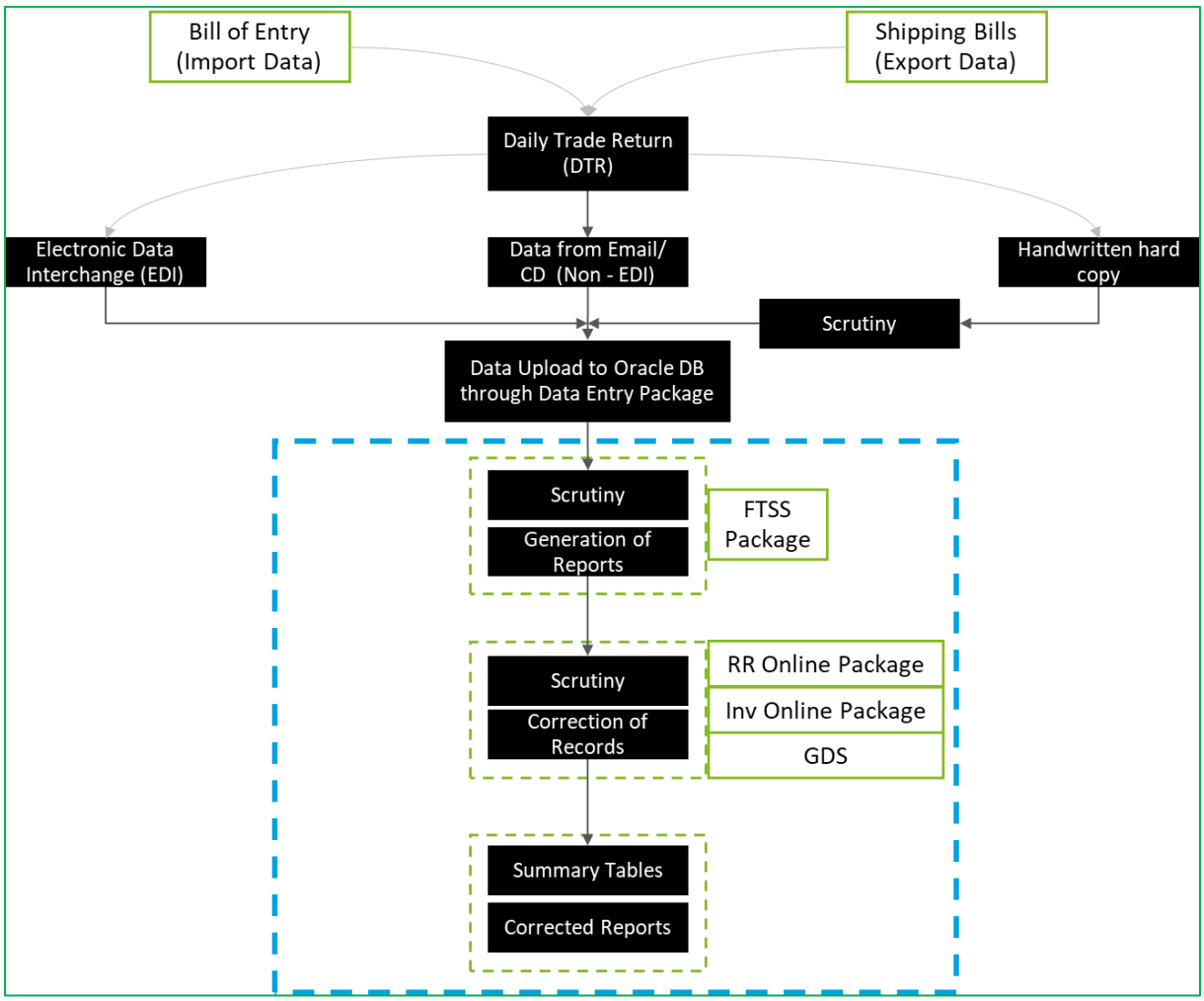


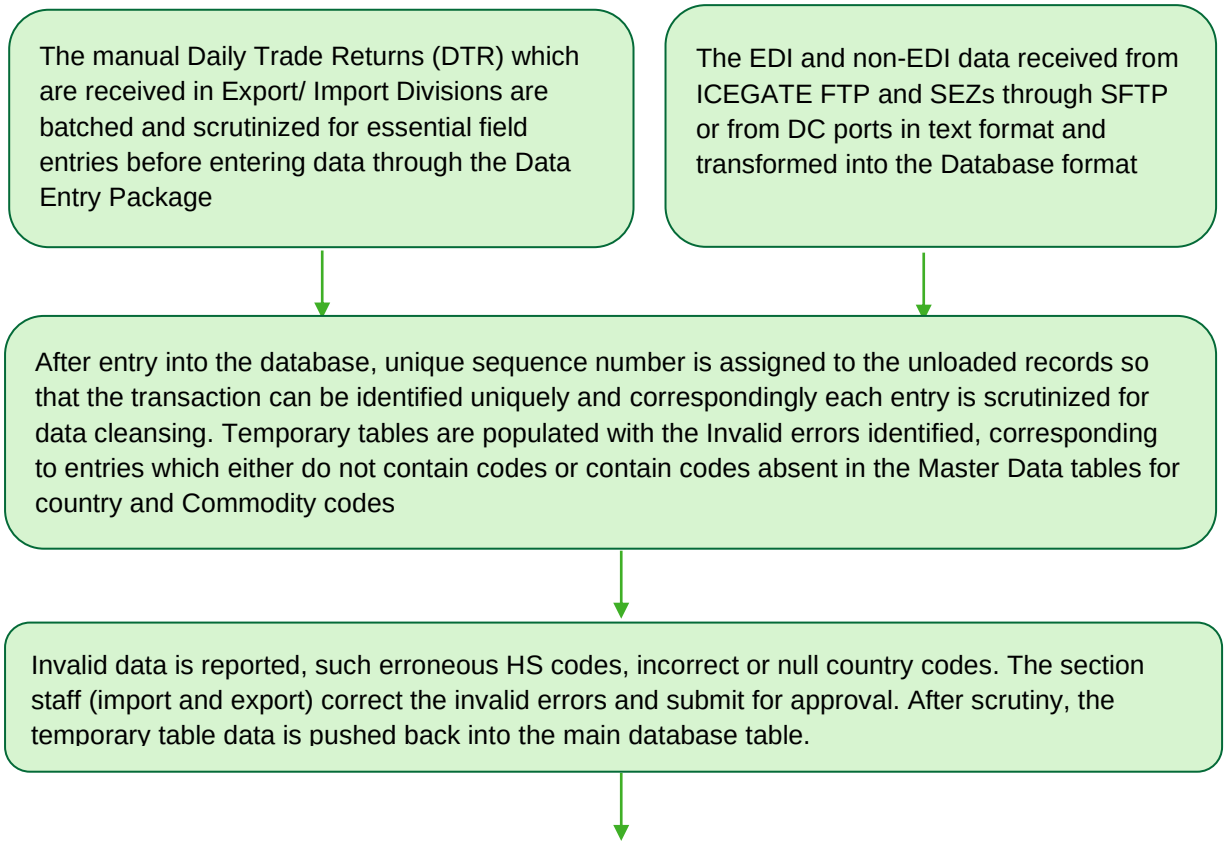
Figure 2: Illustrative Data Processing flow at DGCIS

Software Packages

Internal Data Processing Software packages include:

Sl. No.	Package Name	Functionality
1.	FTSS RAC	The FTSS RAC package is used to prepare the exception reports, summary tables and reports as well as upload the approved data into the system.
2.	RR_Online	The package is used for tallying record to record entries in trade data corresponding to Standard units, Quantity and Rate errors.
3.	Inv_Online	Used to identify and correct Invalid Country and Commodity Code errors in trade (Export and Import) data.
4.	Group Dump System	Used to correct errors in trade data corresponding to Standard units, Quantity and Rate errors which may have been missed at RR stage.
5.	Data Entry Package	Used for uploading manual data into the Export and Import DTR Table.

An illustrative workflow for data processing at DGCIS is provided below:



A Record-to-record (RR) error list is reported, and a temporary table is populated with the entries falling out of bounds of the acceptable criteria. The data is allocated based on the segregation of Principal Commodity level to officers concerned for RR correction. RR correction is concerned with the scrutiny of the Quantity correction of individual data entries based on historical mean rate for the individual commodity/ country combination.

↓

Provisional alpha correction: Following the RR correction, the data is sent for approval and subsequently populated to the main DTR table and uploaded to the GDS system. GDS package is used to generate and correct anomalies or outliers which may have been missed during the RR correction and this correction is done into the database directly, without the use of temporary tables.

↓

Following error correction, the data is aggregated into summary tables and published in the form of Reports such as, Quick Estimates and Press Note released by the Department of Commerce, on the 15th of every month for the preceding month, Principal Commodity Group by country level information for the Brochure publication, 8-digit commodity level publication for Monthly Statistics of Foreign Trade of India (MSFTI) and quarterly 8-digit level publication SFTIC (Statistics of the Foreign Trade of India by Countries).

Module-wise description

The details of various components of the FTSS application are illustrated below:

2.1.1 Data Ingestion Component

This Component handles the input data to the online application. The Foreign Trade data gets generated in customs locations and SEZs in the forms of Daily Trade Return (DTRs) from Bills of Entry (BE) for Imports and Shipping Bills (SB) for Exports submitted by the Importers and Exporters, respectively, in various customs offices and SEZs located all over India.

The DTRs from Customs are received in DGCIS in three different modes, namely,

(i) Electronic Data Interchange (EDI) mode through CBIC ICEGATE SFTP Server and SEZ SFTP Server – The DTRs from SEZs are received online through NSDL Server by DGCIS. This data is hosted on the SFTP host server and accessed through IP and dedicated password. The data is in the form of text flat file with specified data format. This data is formatted in the Database field format and uploaded into the system using a telnet client. Periodicity of this activity is daily, i.e., every day the export and import data of the previous day from each of the SEZs and Ports are updated in the database.

(ii) E-mail (non-EDI) data in the form of Excel files – This data is formatted in the Database field format and uploaded into the system using a telnet client. This activity is done as and when non-EDI data is received from the ports via email.

(iii) Hard copy in handwritten formats – This data received is entered into the Database using a Manual Data Entry module. Except for manual data, all other data are uploaded into the main server by EDP (Electronic Data Processing) Division and separate datasets are maintained for export and import. The manual data are uploaded into the main server by officers of Export and

Import after data entry through the Manual Data Entry module. This activity is done as and when non-EDI data is received from the ports via post.

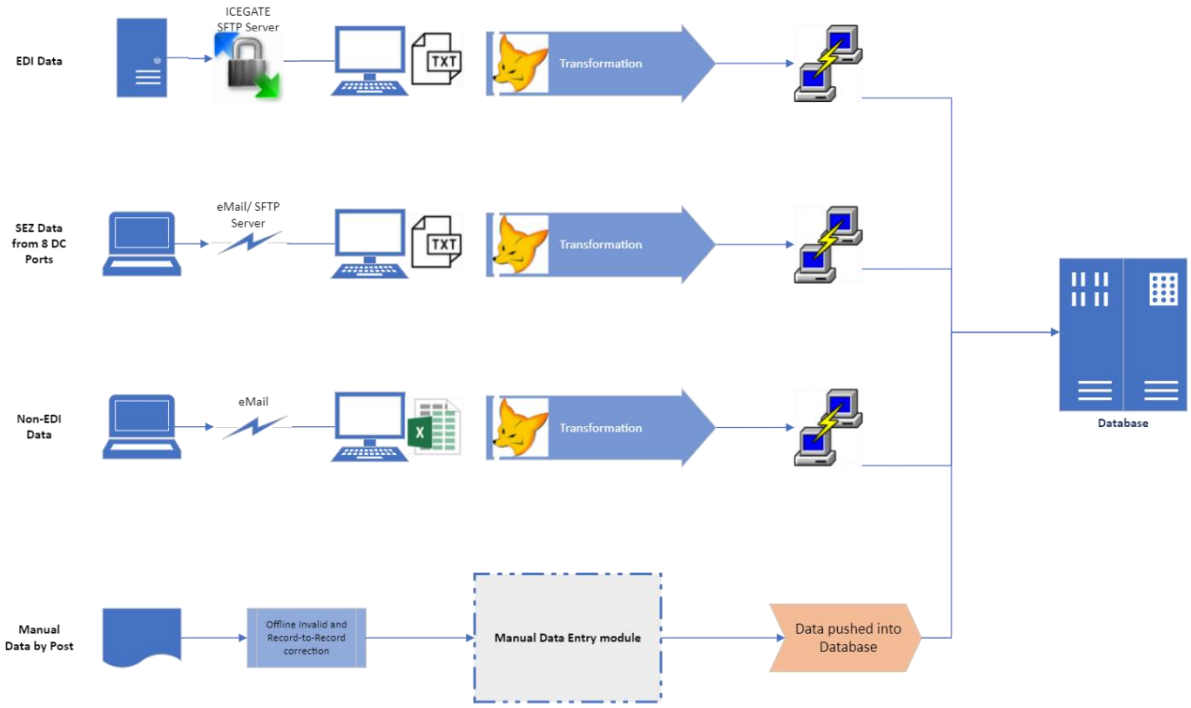


Figure 3: Data Ingestion at DGCIS

2.1.2 Data Record ID (Sequence Number) Generation

After entry into the Database for all DTRs (export and import), a unique Sequence Number is assigned to each entry in the Database. The Sequence number is reset to zero (0) at the beginning of each financial year and each entry in the database is given an incremental sequence number from the last number as present in the Database. Each data entry also contains the date and month of the transaction (Shipping Bill date for export & Bill of Entry date for import).

2.1.3 Invalid Error Generation & Correction Component

After assignment of the Sequence number to each new entry, each of the entries are checked for Invalid Country and Commodity codes (fields in the DTR entry) individually for Export and Import.

User selects the month and year of the database for which the Invalid check is to be run. If the individual Country and Commodity codes in the data entries are not present in the Master Table of Countries and Commodities, a temporary Error table is populated with the Invalid entry for correction.

Error can be of two types:

1. Code does not exist in the Master Table of Commodity/ Country Codes
2. Commodity/ Country Code field is blank

In both the cases, the entries are populated in the temporary table for correction

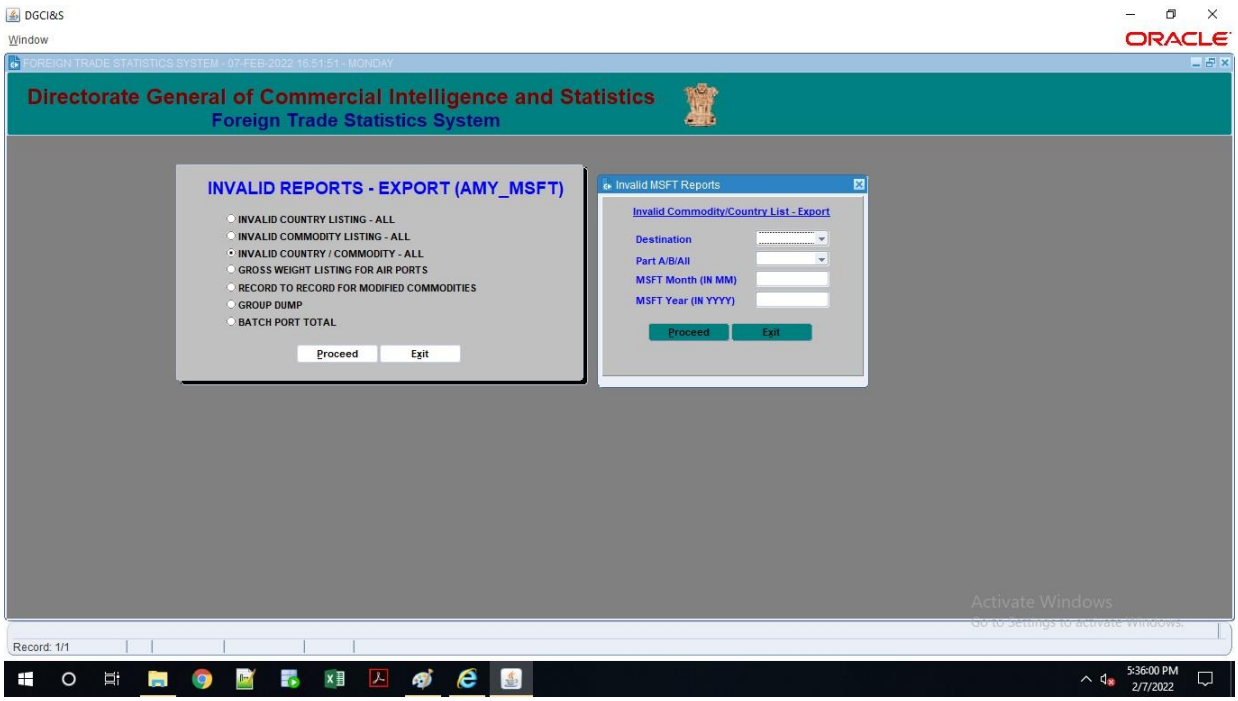


Figure 4: Invalid Error

The temporary table generated for Invalid Country and Commodity codes are distributed for correction amongst the users and the screen for correction is as follows:

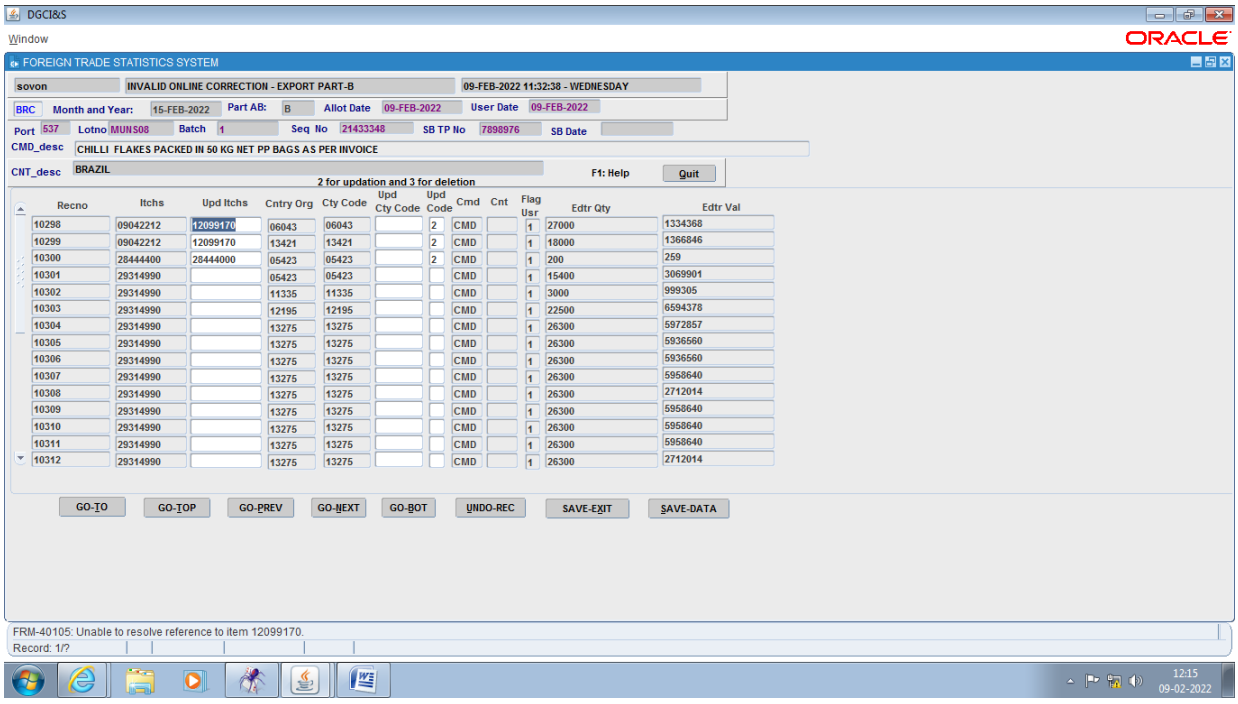


Figure 5: Temporary Table for Error correction

For Invalid Error correction, only Commodity Code (ITCHS) and Country Code are editable for correction, while other fields are non-editable. The user updates the Country and Commodity codes and submits for verification to senior officers and post verification the updated values are pushed into the database corresponding to the original entries.

Error correction for the two error types are as follows:

1. Commodity Code does not exist in the Master Table of Commodity Code – In case of an invalid code entry, the user determines the correct ITCHS Code from the Master Table based on the description of the product or commodity
2. Commodity Code field is blank – In case of a blank code entry, the user determines the correct ITCHS Code from the Master Table based on the description of the product or commodity and updates the Commodity Code for the transaction.
3. Country Code is blank or does not exist in the Master Table of Commodity Code – In case such an error, the user determines the correct Country code based on the description of the item or port of export/ import and updates the Country Code for the transaction.

2.1.4 Auto – Correction/Conversion Component

For each commodity code, a standard measurement unit is defined however, the input data may contain reported unit of quantity different than that of the Standard unit of measurement. In such cases, Stored Procedures are run such that an auto conversion of the unit using the mathematical formula from the reported unit of quantity to the standard unit of quantity.

2.1.5 Group Code Updation Component

All 8-digit Commodity Codes have been classified into 169 Brochure Groups. The commodity codes assigned to each Brochure Group is updated in the beginning of each Financial Year.

After the Commodity Code errors have been corrected, for each individual database entry, Group Code is assigned to the transaction based on the Commodity code, corresponding to the month and year selected.

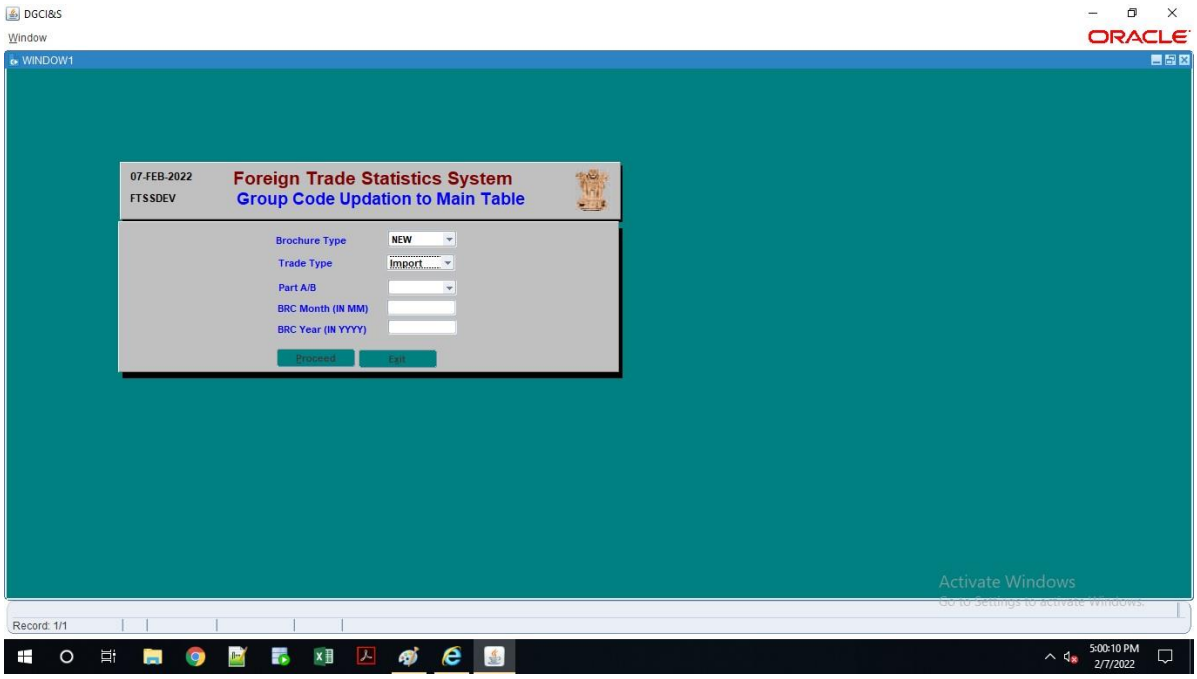


Figure 6: Group Code Updation

2.1.6 Record-to-Record (RR) Error Generation & Correction Component

For all transactions stored in the database, unit value is calculated which is derived by dividing Export/Import Value by the quantity. For all Country Commodity combination, a Historical Mean value is available which are computed on the basis of unit values of historical transactions. The tolerances for each Country Commodity combination are also defined. Upon running of the Record-to-Record check, the transactions where the unit values lie beyond the tolerance range then they are selected for checking.

In this step, those cases are also taken up where the transactions have been reported in units of commercial parlance. These transactions are individually checked, and the reported quantities are corrected to appropriate quantities as per the Standard Unit.

The staff update the quantities of the transactions based on historical reference or if there is a mismatch in the standard units and Commercial units reported based on the description of the commodity provided by the importer or exporter.

2.1.7 Computation of Historical Mean Rates

The benchmark for comparing the current unit values are the historical unit rates. These historical unit rate, which is the mean of the unit values of transactions made in the past months, is computed using the following logic:

1. First the transactions of the past three months are taken for each country x commodity combination. The mean and variance of unit values in these transactions are computed after suitably removing outlier transactions.

2. Then the only those means are taken where the number of transactions is 10 or more. In case 10 transactions are not found in the past three months, then for those country x commodity combinations data for past six months is considered. In case, still there are less than 10 transactions available, then the means are computed on the basis of past 12 months. If still there are less than 10 transactions, then those country x commodity combinations are dropped.

3. Now, the historical rates are computed only country-wise using the same methodology as elucidated above. These rates are used for those transactions for which the country x commodity combinations have less than 10 transactions and have been dropped earlier.

2.1.8 Group Dump System (Provisional Alpha) Error Correction Component

In this step the unit values are checked country-wise for each commodity against the historical rates. In case the current rates are found to be outside tolerance level then each transaction of that country for the specific time period is checked.

2.1.9 Aggregation of Brochure-MSFT

After successful correction of the errors in the dataset, a month-wise aggregation is run based on the parameters as defined below to the Export and Import data. The transactions corresponding to each of the following parameters are aggregated and collated into a summary table for dissemination.

1. Brochure Code-wise Aggregation
2. MSFT-wise Aggregation
3. State-wise Export data Aggregation
4. Scheme-wise data Aggregation

2.1.10 Master Table creation and Maintenance

The following are the list of Master Tables which are maintained at DGCIS and are updated on a regular basis.

1. Country Code Master Table
2. Commodity Code Master Table
3. Port Code Master Table
4. Brochure Code Master Table
5. State/ Region Master Table
6. Scheme Master Table
7. Lot Master Table
8. Chapter Master Table
9. Unit History Master Table

10. Sensitive Commodity Master Table
11. Section Master Table
12. Dollar Master Table

2.2. Data Centre Architecture

DGCIS has an on-premises data centre which is located at the DGCIS main office in Kolkata. The Data centre is equipped with the required IT and Non-IT infrastructure including the core components, equipment and software for IT operations and storage of data and applications. These include storage systems; servers; network infrastructure such as switches and routers; and various information security elements, such as firewalls.

To maintain the uptime of the IT equipment two 20KVA Online UPS, with 2 hours battery backup each, are configured in failover mode and have been deployed in the DC along with 25KVA Stabilizer. Rittal smart rack has been installed and configured in the DC to hold the servers. Biometric enabled access control card system secures the access to the DC. Different zones such as Server Zone, DMZ Zone etc. are configured to access the data maintained as per security levels. The following diagram depicts the current infrastructure at DGCIS Data Centre.

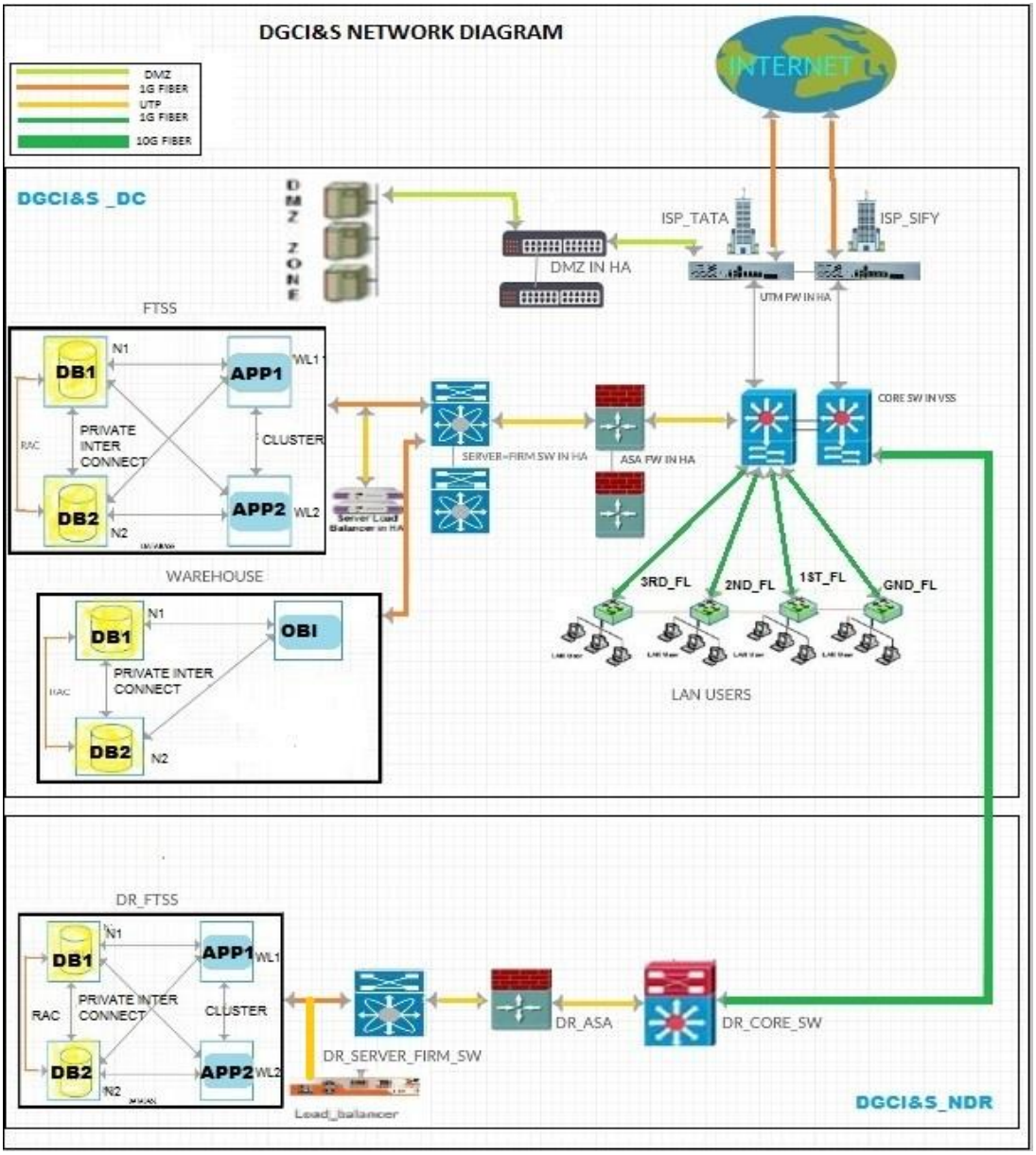


Figure 7: Network Infrastructure at DGCIS DC & DR

2.3. Compute Architecture of DC and DR

The Compute architecture of DC is configured and installed on Oracle SPARC and Sun Rack servers, consisting of eight (08) physical servers at DC and four (04) physical servers at DR. There are multiple Oracle SPARC and Sun servers which run either on Sun Solaris10 or 11.3 .

To access the application and database within the local area network, end users are required to login to the Active Directory server and through dedicated username and password, they can access different modules of the application.

As mentioned above in DC architecture section, different zones have been configured and mapped with application, database, and other servers. The dissemination web portal application is configured in separate application and database servers, which are hosted in the DC in the DMZ Zone. The EXIM Analytics Server is also hosted at the DC in the DMZ Zone. Export / Import directory and Service Sector Databases are configured on Sun server X4 and X4170, hosted at the DC.

Internet Access is not available to all users at DGCIS. LDAP Server is used to authenticate DGCIS users for Internet Usage. For all users apart from DG and DDGs, Internet Access is provided via proxy and authenticated by LDAP server. It may be noted that the FTSS application is not Web-based and does not utilize Internet Access.

DGCIS has four Oracle's SPARC M7 processor based T7-1 servers in the Production Environment. These servers provide a resilient system and enables DGCIS to respond to its demands with extreme security and performance. These are installed and configured in a Solaris LDOM virtual environment at DC. The four Oracle SPARC T7-1 at DC and two SPARC Enterprise T2000 servers at DR have been configured with management console for remote Management and Administration.

The following tables detail out the servers installed and configured at DC and DR:

Server Details

Servers Installed at DC Site			
Sl. no	**Server Role**	**Description**	**Type of Server**
1	Control Domain -1	Server Management Console to manage and administer the physical server.	Physical (Oracle SPARC T7-1)
2	Production Database Server - Primary	Primary Production DB Server (ftssidb)	Virtual
3	Warehouse Database Server - Primary	Primary Warehouse Production DB Server (ftsswhdb)	Virtual
4	Control Domain -2	Server Management Console to manage and administer the physical server.	Physical (Oracle SPARC T7-1)
5	Production Database Server - Secondary	Secondary Production DB Server (ftssidb)	Virtual
6	Warehouse Database Server - Secondary	Secondary Warehouse Production DB Server (ftsswhdb)	Virtual
7	Control Domain -3	Server Management Console to manage and administer the physical server.	Physical (Oracle SPARC T7-1)

Servers Installed at DC Site			
Sl. no	**Server Role**	**Description**	**Type of Server**
8	WebLogic Application Server-Primary	Primary Web logic application Production Server (WLS_FORMS)	Virtual
9	Test Server-	Testing server (Currently not in use)	Virtual
10	Bigdata Application Test Server	Test server for Bigdata application (Currently not in use)	Virtual
11	Application Test server	Test server for application (Currently not in use)	Virtual
12	Print Server	Manages the print request from end users	Virtual
13	Staging server	Test server for application (Currently not in use)	Virtual
14	Big data DB Test Server	Test server for Bigdata DB (Currently not in use)	Virtual
15	Control Domain-4	Server Management Console to manage and administer the physical server.	Physical (Oracle SPARC T7-1)
16	WebLogic Application Server-Secondary	Secondary Web logic application Production Server (WLS_FORMS)	Virtual
17	LDAP Server	Directory Server used for Internet user's authentication	Virtual
18	OBI Application Server	Business Intelligence production application server (bi_server1)	Virtual
19	Database Server	Dissemination DB Server	Physical (SUN FIRE X4170 M3(X3-2))
20	Backup Server	Used to take backup of data at disk and Tape through Net backup software (Veritas)	Physical (Oracle SERVER X5-2)
21	Database Server	Export-Import Directory DB Server	Physical (SUN SERVER X4-2)
22	Database Server	Service Sector DB Server	Physical (SUN FIRE X4170 SERVER)
23	Database Server		Virtual

Servers Installed at DR Site			
1	Database Server	Primary Production Database server	Physical (Sparc enterprise M4000)
2	Database Server	Secondary Production Database server	Physical (Sparc enterprise M4000)
3	Control Domain -5	Server Management Console to manage and administer the physical server.	Physical (Sparc enterprise T2000)
4	Application Server	Primary Application Server	Virtual
5	Control Domain - 6	Server Management Console to manage and administer the physical server.	Physical (Sparc enterprise T2000)
6	Application Server	Secondary Application Server	Virtual

Physical server configuration:

The following table details out the configurations of the physical servers at DC and DR.

Environment	Location	Make / Model	CPU/ Speed	Memory (GB)	RAID	Local HDD	OS with Ver	NIC	HBA
Production	DC	Oracle Sparc T7-1	one Oracle SPARC M74.13 3 GHz	512	1	6*600 Gb & 1.2*2TB	Solaris 11.3	Four 10 GbE + Two Sun Dual Port 10 GbE PCIe 2.0	16 Gb Fiber Channel PCIe Universal FC HBA, QLogic (QTY 3)
Production	DC	Oracle Sparc T7-1	one Oracle SPARC M74.13 3 GHz	512	1	6*600 Gb & 1.2*2TB	Solaris 11.3	Four 10 GbE + Two Sun Dual Port 10 GbE PCIe 2.0	16 Gb Fiber Channel PCIe Universal FC HBA, QLogic (QTY 3)
Production	DC	Oracle Sparc T7-1	one Oracle SPARC M74.13 3 GHz	512	1	6*600 Gb & 1.2*2TB	Solaris 11.3	Four 10 GbE + Two Sun Dual Port 10 GbE PCIe 2.0	16 Gb Fiber Channel PCIe Universal FC HBA, QLogic (QTY 3)
Production	DC	Oracle SPARC T7-1	one Oracle SPARC M74.13 3 GHz	512	1	6*600 Gb & 1.2*2TB	Solaris 11.3	Four 10 GbE + Two Sun Dual Port 10 GbE PCIe 2.0	16 Gb Fiber Channel PCIe Universal FC HBA, QLogic (QTY 3)

Environment	Location	Make / Model	CPU/ Speed	Memory (GB)	RAID	Local HDD	OS with Ver	NIC	HBA
Production	DC	Sun Fire X4170 M3(X3-2)	one intel i386 2400 MHz	32	1	4 * 600 Gb	Solaris 10	two 1000 Mbps	one dual port 4Gb
Production	DC	Sun Fire X4170 Server	one intel i386 2533 MHz	12	1	6 * 500 Gb	Solaris 10	four 1000 Mbps	one dual port 4Gb
Production	DC	oracle SERVER X5-2	one intel i387 1200 MHz	64	1	6*600 Gb	Solaris 11.3	two 10GbE	16 Gb Fiber Channel PCIe Universal FC HBA (Qty 2)
Production	DC	Sun Server X4-2	two intel i386/i387 2600 MHz	128	1	4 * 300 Gb	Solaris 10	four 1000 Mbps	one dual port 4Gb
Production	DR	Sparc Enterprise M4000	two Sparcv 9 2150 MHz	48	1	2 *146	Solaris 11.3	four 1000 Mbps	two dual port 8 GB
Production	DR	Sparc Enterprise M4000	two Sparcv 9 2400 MHz	48	1	2*146	Solaris 11.3	four 1000 Mbps	two dual port 8 GB
Production	DR	Sparc Enterprise T2000	one Sparcv 9 1000 MHz	16	1	2*72 & 2*146	Solaris 10	four 1000 Mbps	two dual port 8 GB
Production	DR	Sparc Enterprise T2000	one Sparcv 9 1000 MHz	16	1	2*72 & 2*146	Solaris 10	four 1000 Mbps	two dual port 8 GB

Virtual server configuration:

The following table details out the configurations of the Virtual servers at DC and DR.

Environment	Location	Total Core	Server Role	Memory(GB)	RAID	Storage Space allocated
Production	DC	9	Production Database Server	356	1	Yes
Production	DC	3	warehouse Database Server	60	1	Yes
Production	DC	9	Production Database Server	356	1	Yes
Production	DC	3	Warehouse Database Server	60	1	Yes
Production	DC	12	WebLogic Application Server	192	1	Yes
Production	DC	2	Test Server	16	1	Yes
Production	DC	4	Bigdata AppTest Server	16	1	No
Production	DC	2	App Test server	32	1	Yes
Production	DC	1	Print Server	12	1	Yes
Production	DC	2	Staging server	20	1	Yes
Production	DC	2	Big data DB Test Server	16	1	No
Production	DC	12	WebLogic Application Server	192	1	Yes
Production	DC	4	LDAP Server	16	1	Yes
Production	DC	6	OBI Application Server	60	1	Yes
Production	DC	4	Database Server	16	1	Yes
Production	DR	2	Application Server	10	1	Yes
Production	DR	2	Application Server	10	1	Yes

The following table provides the details regarding existing platform used in present DC and DR architecture:

Sl. No.	Platform parameters	Remarks
1	OS currently deployed on the servers	Oracle Solaris 11.3
2	Count of Physical Server where Sun Solaris/ Other OS is currently installed	12
3	Count of Virtual Server where Sun Solaris/ Other OS is currently installed	17
4	Type of Virtualization currently installed and configured	LDOM
5	Existence of HA configured on the Virtual Servers (Y/N)	No
6	DGCIS application is hosted/ Installed on which Platform?	Solaris / Windows Server
7	Oracle DB is hosting / installation Platform	Oracle Solaris 11.3
8	Disk Partition details of OS running on Virtual /Physical mode	zfs file system partitions
9	Performance of Server at peak time in percentage	Load: 2.50 CPU Utilization%: 3%
10	Existence of any centralized platform for controlling and monitoring Virtual host	No
11	Middleware platform deployed in the DC and DR	Oracle WebLogic Server

2.4. Production Database Server Architecture

DGCIS has deployed two production Database servers, namely, Production_Node1 and Production_Node2 which are configured as RAC cluster in Active-Passive mode. It is connected with WebLogic application server to run the Forms and report services.

Oracle Golden Gate Replication software is configured at Production Node1 and Production Node2 for replicating data to Warehouse OBI database server.

The Warehouse Database server is also configured as RAC cluster as OBIDB_Node1 and OBIDB_Node2 in Active – Passive mode.

Middleware: For FTSS application, based on Oracle Forms, two WebLogic application servers are configured in the DC and for Oracle Business Intelligence Suite Services a single WebLogic application server is configured.

Oracle Database: Production and Warehouse oracle databases are configured as 2 node RAC (Real Application Cluster), which provides High Availability, Fault Tolerance and Load balancing.

Oracle Golden Gate: Database objects are being replicated with Oracle Golden Gate utility between DC and DR.

Oracle RMAN Backup script is configured and running at different time slot to take the backup of data. At 11 PM logical backup of disk is taken and gets copied to DR site. Oracle RMAN is used to backup to tape at 7PM. Object level backup is taken at 20.20PM, 21.45 PM and 22.00 PM

Oracle WebLogic: Oracle Forms and Business Intelligence Application runs on the WebLogic (middleware) Server

Oracle Database Deployment Architecture

Following picture details out the on-premises Oracle Database Deployment Architecture.

The diagram below illustrates the following,

1. All the below mentioned servers are configured in Virtual mode under Sun Solaris LDOM virtualization.

2. The two-production database servers I.e., Production_Node1 and Production_Node2 hosted at DC are configured with RAC cluster connected with WebLogic application Server1 and WebLogic application Server2 which in turn are configured as active-standby mode. Oracle forms and reports services are configured on these WebLogic application servers.

3. At DC, OBI Database servers (Warehouse Database Server) OBIDB_Node1 and OBIDB_Node2 are also configured with RAC cluster. These are connected with one WebLogic application server where business intelligence suit services are running and configured.

4. At DC, production database servers and OBI database servers are configured through replication software I.e., Oracle Golden Gate which backup both production and OBI database to DR through replication software.

5. The end users' access and connect the dissemination database server, Import-Export directory database server and Service Sector database server through Web portal configured with apache tomcat hosted at DR.

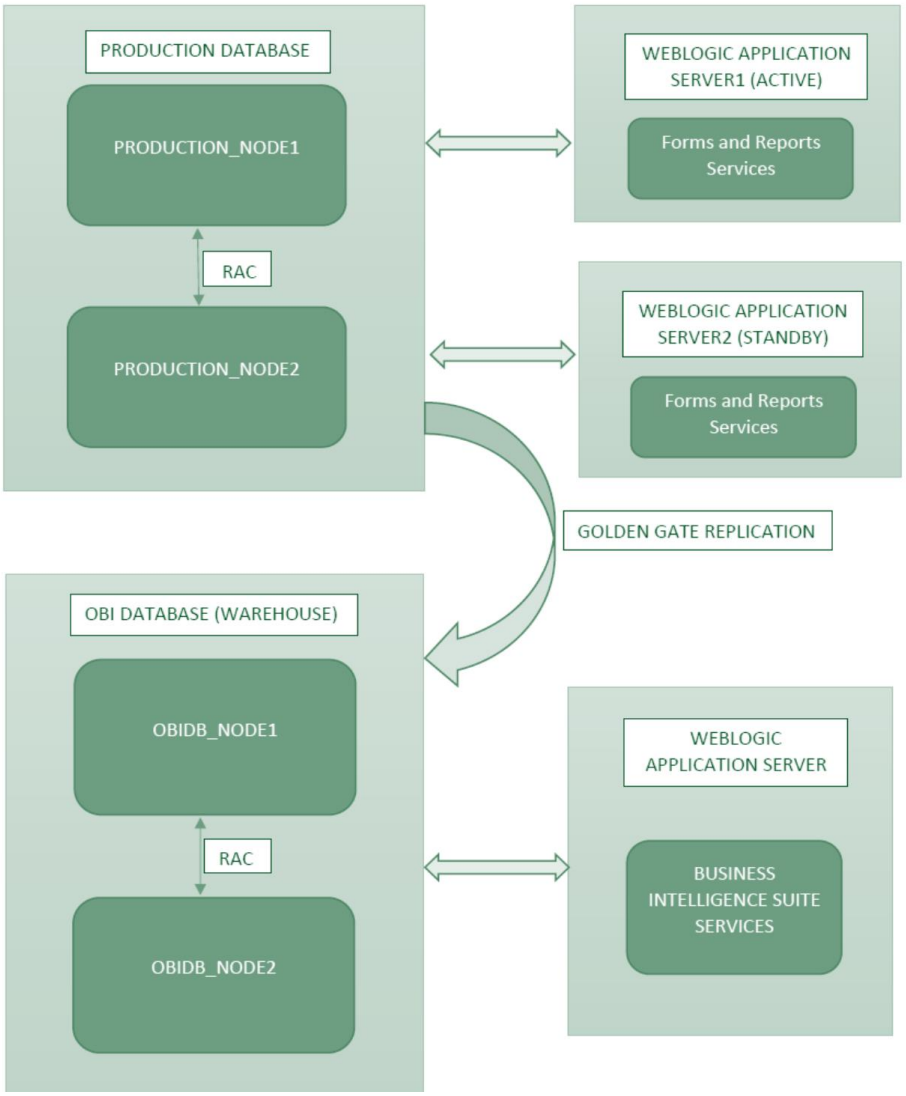


Figure 8: Database Architecture (1)

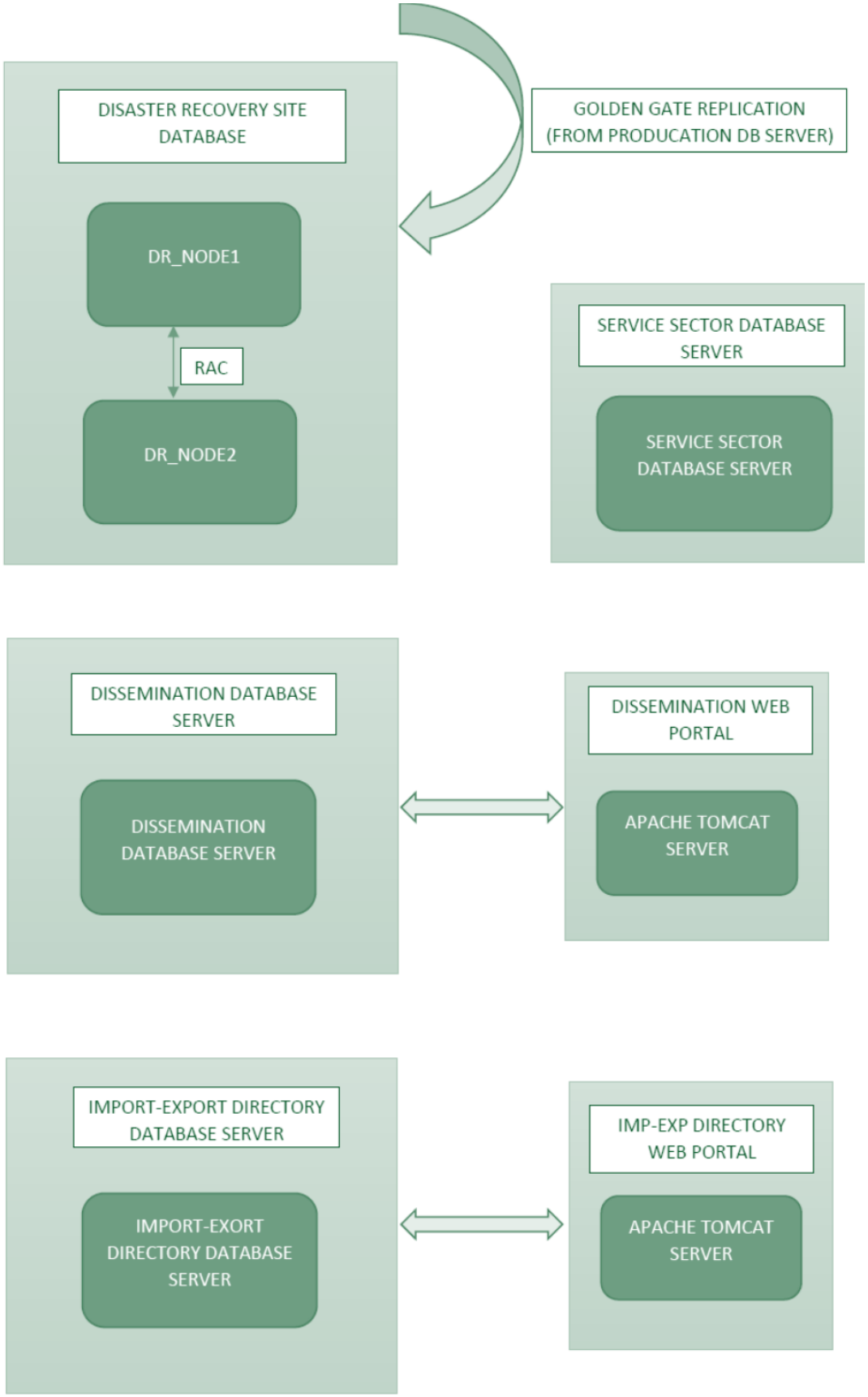


Figure 9: Database Architecture (2)

The following diagram depicts how the end users connect and access the Oracle database servers which are configured in a HA mode through Oracle RAC cluster. The end users are configured in management VLAN placed behind the core switch, server farm switch and load balancer and access the application and database server after successful authentication through active directory server.

Production Web logic application servers at DC are configured in an active and standby mode. These application servers are connected to Production DB Servers.

Single WebLogic application server (Business Intelligence Suit) support the Warehouse DB servers (OBI DB server). Tables are replicated from production DB servers to Warehouse DB servers (OBI DB server) though Golden Gate software at DC.

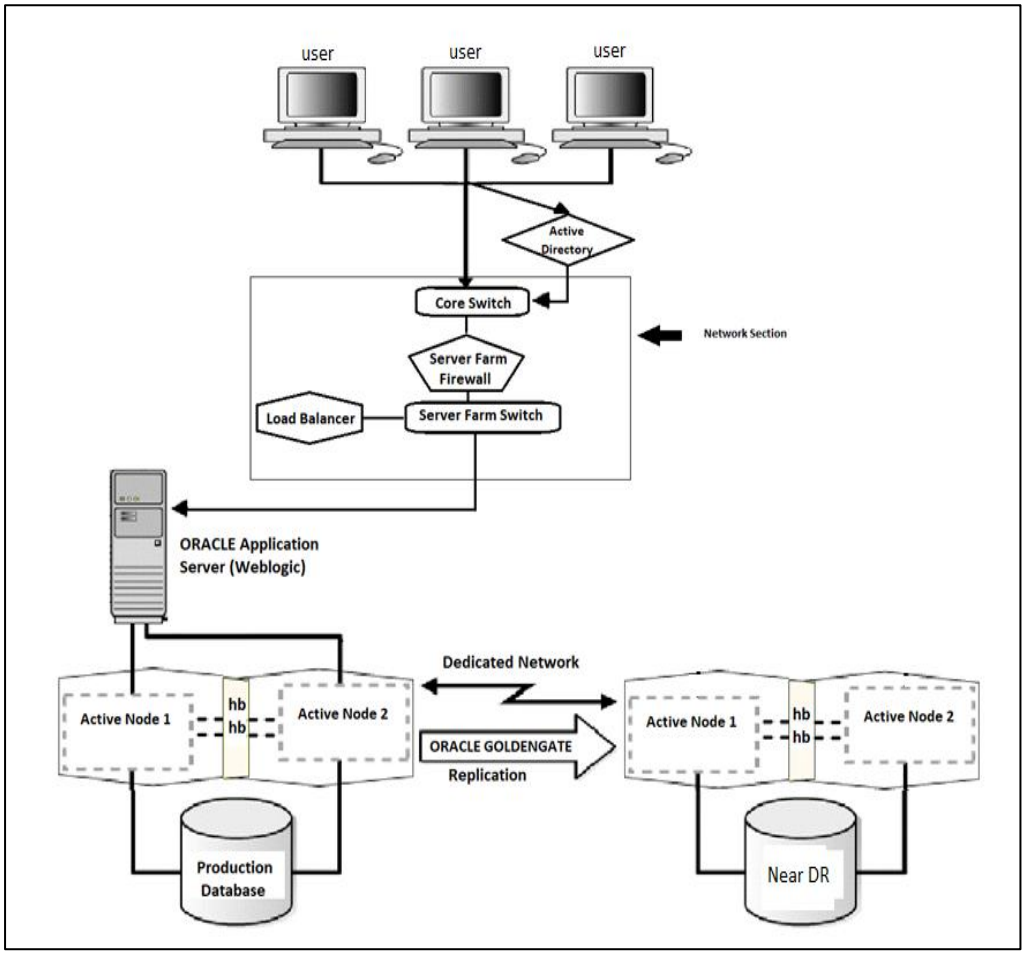


Figure 10: Server Architecture at DGCIS DC & DR

Existing Database details

The following table provides the details regarding the existing Databases;

Database details	Remarks
General information	
Version of Oracle database	12.1.0.2.0
Edition of the database: Standard / Enterprise	Enterprise
Database Size	1.5 TB
Type of Data	Alpha-numeric Data
Count of schemas in the database	30
Count of tables in the database	5251

Database details	Remarks
Count of triggers in the database	700
Count of Stored procedures in the database	606
Count of functions in the database	280
Size of system global areas (SGAs) and program global areas (PGAs) or Automatic Memory Management (AMM) usage, in megabytes	Memory Target: 160 GB Automatic Memory Management
Peak time of database usage during the day	Peak Time: 10:30 - 14:00
Configuration of database in High Availability (HA) mode	Yes (Oracle 2-Node RAC)
RTO and RPO requirements for database	Not Defined
Database growth size (daily & monthly)	Daily: 0.58 GB Monthly: 17.43 GB
Current Database Transaction Load - Peak	12
Current Database Transaction Load - Concurrent	7
Count of Users access DB Server concurrently	50-70
Supporting tools used for entire database management	No tools are being used
Infrastructure	
Operating system used for the database	Oracle Solaris 11.3
Count of CPU cores	9 Cores each per server
Memory size of the server	320 GB
Usage of local storage (Y/N)	No
Usage of storage types - Network-attached storage (NAS) or storage area network (SAN)	SAN Storage
RAC database – count of nodes	2 Nodes
Usage of partitioning features (Y/N)	Yes
Usage of multi-tenant database (Y/N)	No
Count of LUN associated with Oracle Database server	65
Type of licensing model	It is processor perpetual license, (core based)
Count of cores or processors currently being used	18 cores are being used currently
Database backups	
Database back frequency	Daily
Tools used to take the backup and or Archive	NetBackup backup solution
Existence of present data archival policy	No data archival policy
Retention period for archive logs and backups	15 Days
Usage of backups to clone database (Y/N)	No
Storage of backup?	In Tape Cartridge
RAID configuration used for database server	RAID 5
Database security	
Usage of Oracle Database Vault (Y/N)	No
Usage of data masking (Y/N)	No
Usage of Secure Sockets Layer (SSL) (Y/N)	No
Usage of Oracle Advanced Security features such as Transparent Data Encryption (TDE)	No
Usage of Oracle Advanced Compression	No

Database details	Remarks
Database high availability and disaster recovery	
Usage of Oracle Data Guard (Y/N)	No
Usage of Domain Name System (DNS) alias for database connectivity (Y/N)	No
Usage of replication tools such as Oracle Golden Gate, Quest Share Plex, or Oracle Streams	Oracle Golden Gate replication tool is used
Database - High Availability (Y/N)	Yes
ASOP Documentation if available	No

Schema Size of Existing Database

The following table provides the details regarding the Schema Size of Existing Database.

Schema Name	Size(GB)
FTSSIMP	1307.48486
DGCIS_NEWDEV	41.4019165
SYS	16.9324341
DGCIS	11.5568237
SYSMAN	4.89581299
ADMNRAC	2.31695557
FTSSANCI	0.536437988
SYSTEM	0.417419434
APEX_040200	0.189453125
AUDSYS	0.080932617
MDSYS	0.076904297
XDB	0.066894531
DGCISAI	0.059082031
SQLTXPLAIN	0.058105469
DGCIS_EXTR	0.028320313
ORDDATA	0.01574707
OLAPSYS	0.014953613
WMSYS	0.007019043
DVSYS	0.004333496
OGGADMIN	0.00378418
CTXSYS	0.003723145
GSMADMIN_INTERNAL	0.001342773
DBSNMP	0.001281738
OUTLN	0.000549316
SCOTT	0.000488281
ORDSYS	0.000427246
OE	0.000427246
OJVMSYS	0.000366211
LBACSYS	0.000305176
TSMSYS	0.000244141

The following table provides the General Information of existing Oracle DB

Sl. No.	Description	Remarks
1.	Database Name	Production DB OBI DB DR DB Dissemination DB IMP_EXP Dir D Service Sector DB
2.	Version of Oracle database	Production DB- 12.1.0.2.0 OBI DB- 12.1.0.2.0 DR DB- 12.1.0.2.0 Dissemination DB- 11.2.0.1.0 IMP_EXP Dir D- 11.2.0.1.0 Service Sector DB- 11.2.0.1.0
3.	Edition of the database:	Enterprise
4.	Size of the database	Production DB-1615.58 GB OBI DB-259.61 GB DR DB-1144.21 GB Dissemination DB-226.59 GB IMP_EXP Dir D-263.79 GB Service Sector DB-97.38 GB
5.	Type of data used	alpha-numeric
6.	Count of schemas do you have in the database	Production DB-30 OBI DB-20 DR DB-27 Dissemination DB-24 IMP_EXP Dir D-28 Service Sector DB-23
7.	Count of tables in the database	Production DB - 5252 OBI DB -1030 DR DB - 4804 Dissemination DB - 2843 IMP_EXP Dir D - 3154 Service Sector DB - 2774
8.	Count of triggers in the database	Production DB-700 OBI DB-580 DR DB-652 Dissemination DB-628 IMP_EXP Dir D-658 Service Sector DB-622
9.	Count of Stored procedures in the database	Production DB-600 OBI DB-58 DR DB-583 Dissemination DB-234 IMP_EXP Dir D-387 Service Sector DB-184
10.	Count of functions in the database	Production DB-280 OBI DB-229 DR DB-268 Dissemination DB-259 IMP_EXP Dir D-259

Sl. No.	Description	Remarks
		Service Sector DB-260
11.	Existence of database links that point to other databases (Y/N)	No
12.	Peak time of database usage during the day or any reporting session	Working Hours (10am to 5pm)
13.	Database growth size (daily(D)& monthly(M))	Production DB- .58 GB(D) 17.32 GB(M) OBI DB-229- .09 GB(D) 2.79 GB(M) DR DB-268-.41 GB(D)12.26 GB(M) Dissemination DB-.03GB(D) .93 GB(M) IMP_EXP Dir D- .04 GB(D) 1.08 GB(M) Service Sector DB-.02(D) GB .65 GB(M)
14.	Current Database Transaction Load - Peak	Production DB-12 OBI DB-7 DR DB-8 Dissemination DB-0 IMP_EXP Dir D-0 Service Sector DB- 2
15.	Current Database Transaction Load - Concurrent	Production DB- 7 OBI DB-2 DR DB-2 Dissemination DB- 0 IMP_EXP Dir D- 0 Service Sector DB-2
16.	No. of Users access DB Server concurrently	Production DB-50-70 OBI DB-12-20 DR DB- 0 Dissemination DB-12-20 IMP_EXP Dir D-0 Service Sector DB-2

Details of Database Infrastructure

The following table provides the details regarding Database Infrastructure:

Sl. No	Database Name	Operating System	CPU cores	Memory size	Local storage	Storage type	RAC DB Nodes	Usage of partitioning features	Count of LUN associated with Oracle DB	Licensing model - Core / Processor / any other	Cores or processors currently in use
1	Production DB	Solaris 11.3	9 cores each	320 GB	No	SAN	Yes, 2 Nodes	YES	65	Core Based	18
2	OBI DB	Solaris 11.3	3 cores each	60 GB	No	SAN	Yes, 2 Nodes	YES	22	Core Based	6
3	DR DB	Solaris 11.3	4 cores each	48 GB	No	SAN	Yes, 2 Nodes	YES	56	Core Based	8
4	Dissemination DB	Solaris 10	1 Core	32 GB	No	SAN	No	No	4	Processor Based	1
5	IMP_EXP Dir DB	Solaris 10	1 Core	12 GB	No	SAN	No	No	0	Processor Based	1
6	Service Sector DB	Solaris 10	2 Core	128 GB	No	SAN	No	No	5	Core Based	2

DC Database and DR Database

Sl. No	Database Name	Usage of Oracle Active Data Guard	Usage of Domain Name System (DNS) alias for database connectivity	Tool used for replication	Database - High Availability (Y/N)
1	Production DB	No	Yes	Golden Gate	Y
2	OBI DB	No	Yes	Golden Gate	Y
3	DR DB	No	Yes	Golden Gate	Y
4	Dissemination DB	No	No	No	N
5	IMP_EXP Dir DB	No	No	No	N
6	Service Sector DB	No	No	No	N

Database Backup

The following table provides the details regarding Backup processes of the Databases:

Sl. No	Database Name	DB backup frequency	Tools used to take the backup and or archive	Existence of data retention policy	Retention period for archive logs and backups	Usage of backups to clone database	Backup Storage	RAID configuration used for database server
1	Production DB	Daily	NetBackup	No	15 Days	No	Tape	RAID 5
2	OBI DB	Daily	NetBackup	No	15 Days	No	Disk/Tape	RAID 5
3	DR DB	Not Scheduled		No		No		RAID 5
4	Dissemination DB	Daily	NFS	No	4 Days	No	Disk	RAID 5
5	IMP_EXP Dir DB	Daily	NFS	No	4 Days	No	Disk	RAID 5
6	Service Sector DB	Daily	NFS	No	4 Days	No	Disk	RAID 5

Database Supported Platforms

The following table provides the details regarding Database Supported Platforms:

Sl. No	Database Name	Server OS	Count of Physical Server with Sun Solaris / Other OS is currently installed	Count of Virtual Server with Sun Solaris/ Other OS is currently installed	Type of Virtualization currently installed and configured	Usage of HA configured on the Virtual Servers (Y/N)	Application hosting/ Installation Platform	Operating System	Disk Partition details of OS running on Virtual /Physical mode	Performance of Server at peak time in percentage	Middleware platform deployed in the DC and DR
1	Production DB	Solaris	12	17	LDOM	No	Solaris/ Windows Server	Solaris	ZFS File System Partitions	Load: 2.5 CPU Utilization: 3%	Oracle WebLogic Server/Oracle Forms and Reports Server/ Oracle Business Intelligence Server
2	OBI DB	Solaris									
3	DR DB	Solaris									
4	Dissemination DB	Solaris									
5	IMP_EXP Dir DB	Solaris									

2.5. Network Architecture

DC and DR are both located in the same premises of DGCIS Kolkata Office. While the DC and DR network is connected through a 10G fiber connectivity backbone, DC building floors are connected with 1G fiber connectivity. Currently Two (2) ISP viz. Tata (30Mbps) and Sify (50Mbps) are used as primary and secondary link respectively. All active equipment are connected either through 1G ethernet or 1G fiber connectivity. In DR, all active equipment are connected either through 1G ethernet or 1G fiber connectivity.

Core switches, the backbone of whole network system of DGCI&S, are responsible for routing and forwarding at the highest level. DC to DR connectivity is established by DC to DR site core switch, which is configured in VSS (Virtual Switching System) mode and provides fault tolerance and high availability. All web applications are broadcasted to public network via DMZ network of firewall in order to provide security to web applications. DMZ zones are connected with DMZ switches which are configured in HA mode.

Nexus 9000 series switch is configured as a Server farm switch at DC in HA mode. All servers are connected with Server farm switch. DR Catalyst 4507 switch acts as the core switch and is connected to DC Catalyst 4507 core switch through fiber connectivity. All floors are connected to DC Catalyst 4507 core switch through fiber connectivity. All servers at DR are connected through Nexus C3172 switch which acts as the server farm switch. Network L2 switches are installed and configured in each floor of the building.

Two load balancers are configured in HA mode to distribute network traffic across a number of servers. One load balancer at DR is configured to distribute network traffic across a number of servers.

Access points are installed and configured in each floor of the building to maintain the redundancy of the LAN.

DGCIS uses a separate network to access e-Office through NIC Net. This connection is through DGCIS Router (Peplink30). End users can access the e-Office network through Net Gear wireless access point which is installed in each floor of the building. Class A IP address are used in the network i.e., for NIC Net 10.173.X.X and for DGCIS 10.6.X.X

Following diagram provides an overview of the architecture of current network systems deployed at DGCIS:

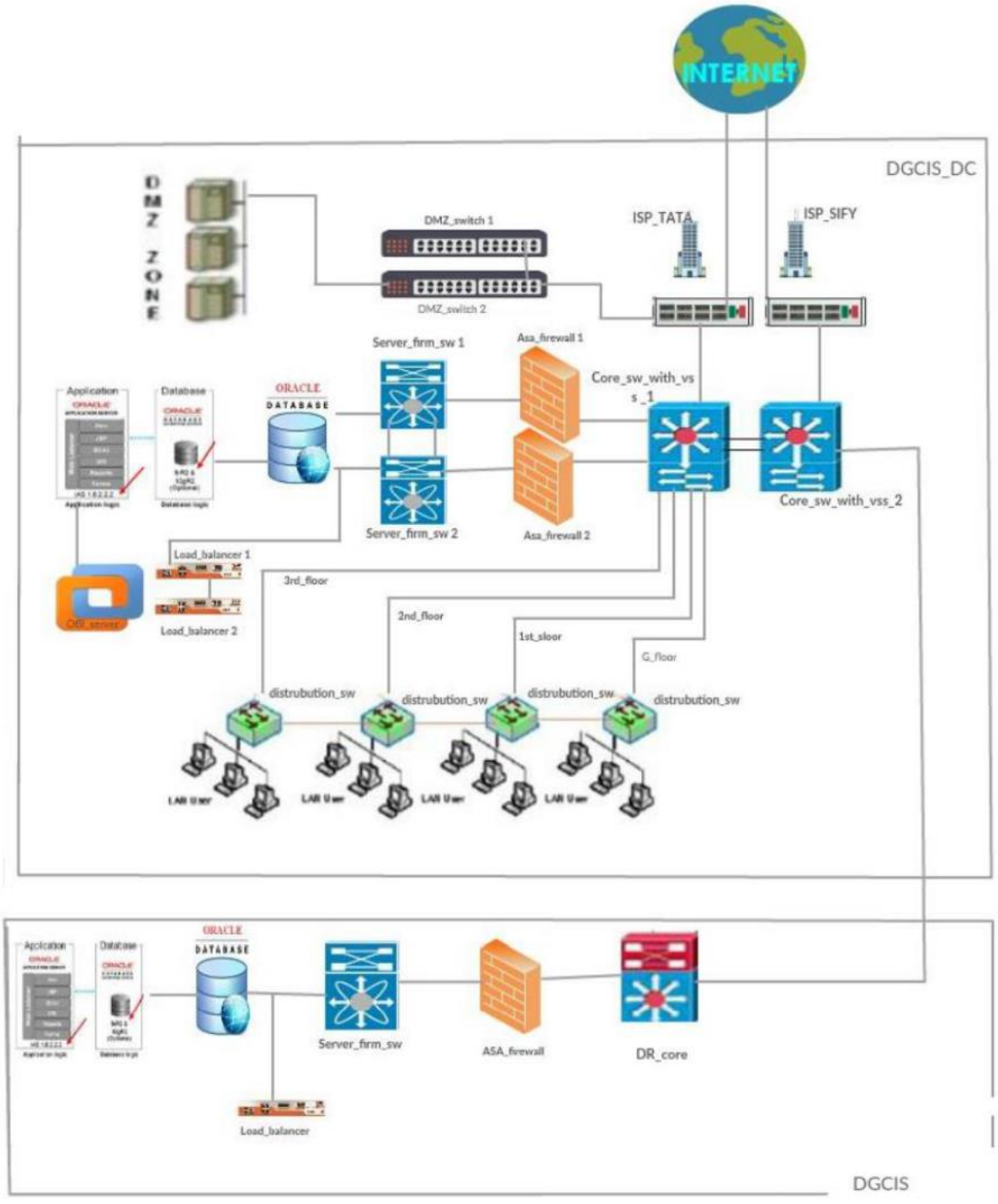


Figure 11: Network Architecture at DGCIS DC & DR

Switches and Access point at DC and DR:

The following table provides the details of the network switches and access points at DC and DR:

Sl. No	Switch Description with (Model)	Quantity	Make	Location
1.	Cisco Catalyst 2960 (L2 Switch)	18	Cisco	DC
2.	Cisco Catalyst 2960 G (L2 Switch)	1	Cisco	DC
3.	Cisco Small Business (L2 Switch)	4	Cisco	DC

Sl. No	Switch Description with (Model)	Quantity	Make	Location
4.	Cisco Catalyst 3560 G (L3 Switch)	2	Cisco	DC
5.	Cisco Catalyst 4507 R-E (Core-Switches)	1	Cisco	DR
6.	Cisco Nexus c9372TX (Server farm Switch)	1	Cisco	DC
7.	Cisco Nexus c9372TX (Server farm Switch)	1	Cisco	DC
8.	Cisco Nexus c3172T (Server farm Switch)	1	Cisco	DR
9.	Cisco-c4507R+E (Core-Switch)	2	Cisco	DC
10.	Cisco Catalyst 2960 G	1	Cisco	DC
11.	ZyXEL GS-4024 (Layer3 - Switch)	1	Zyxel	DC

Access Points				
Sl. No	**Access Point Description with (Model)**	**Qty**	**Make**	**Location**
1	Motorola-AP-6511 (Access Point)	27	Motorola	DC

Load Balancers

Sl. No	Description with (Model)	Qty	Location	Make
1	Array SLB-2600 (Server Load Balancer)	2	DC	Array
2	Array APV 1600 (Server Load Balancer)	1	DR	Array

Router

Sl. No	Router Description	Location	Make
1	Peplink 30 (Router)	DC	Peplink

2.6. Security Architecture

DGCIS has two NextGen Firewall where two ISP links viz. Tata and Sify terminate and all inbound and outbound traffic of DGCIS flow through this firewall. Cisco ASA firewall acts as the perimeter firewall to secure east west traffic which is placed between core switch and server farm switch. Two FortiGate 300D UTM NextGen firewall and two Cisco ASA 5585 are installed in DC whereas one Cisco ASA 5520 firewall is installed at DR. Rules, policies and other features are configured in the firewall to protect the DGCIS network. Fortinet Firewall is configured in High Availability mode; it provides security and protection to whole DGCI&S network with its rich set of security policies. Cisco ASA is placed between the server farm switch & core switch which provides add-on security to server.

Here, in the existing architecture, perimeter firewall has been considered which counts as one of the best practices of security, in which, east west traffic can be monitored and controlled. Only NextGen firewall has been considered as security devices.

Below is the list of firewalls which are deployed in the DC and DR.

Firewall		
Sl. No	Firewall Description with (Model)	Make
1	FortiGate 300D (UTM Firewall)	Fortinet
2	FortiGate 300D (UTM Firewall)	Fortinet
3	Cisco ASA-5585 (ASA- Firewall)	Cisco
4	Cisco ASA-5585 (ASA- Firewall)	Cisco
5	Cisco asa5520 (ASA Firewall)	Cisco

The following table provides the details regarding security measures currently in place:

Sl. No.	Security parameters	Remarks
1	Implementation of third-party external Information Security assessment within the past 2 years (Penetration test, Vulnerability assessment, etc.)	None
2	Process of maintaining incident response procedures	Over Email
3	Process of Implementation of AAA (Authentication, Authorization, Accounting) for all users.	Through Active Directory
4	Frequency of update of security and network diagram / design.	Yes, on Half yearly basis
5	Existence of firewall in DGCI&S's network.	Yes
6	Configuration of routers with ACLs and VLAN	Yes
7	Configuration of firewall with rules, Policy, and port level	Yes
8	Implementation of IDS/IPS technology in the network	Yes
9	Has DMZ architecture been defined in the DGCIS network	Yes
10	Services / features configured in the DGCIS firewall	URL Filtering, Port Blocking, Rules, APT, Policy etc.
11	Antivirus software installed on the DC, DR, and end users' devices	Solaris OS is installed on DC and DR servers, so antivirus software is not required for the said servers. eScan antivirus is installed on all end users' devices.
12	Current process of patch management is presently being configured in the DGCIS network	Instead of central patch management it is done locally.
13	Remote access service in the DGCIS network	Occasionally as an when required by DGCIS users and as approved by concerned authority of DGCIS
14	File and directory level permissions configured on directory server	Yes
15	Process of authentication while entering the DC and DR	Access Card / Biometric
16	End user authentication procedure with server in DC and DR	Access permission provided to users and logging servers through SSH.

2.7. Backup Architecture

Based on DGCIS server architecture, a Veritas Net backup Ver 8.3.0.1 is configured on Solaris 11.0. A single backup server, namely, Oracle Server X5-2 is configured to take the backup of 5 client servers: Production Database Server: 2; Warehouse Database Server: 2 and Database Server: 1.

The backup system is configured for one full backup on a daily basis. No differential or incremental backup has been configured in the system. Two types of backup are taken on a daily basis – (1) file system backup and (2) DB (using Oracle RMAN) backup.

File system backup is directly taken to tape cartridge. Oracle RMAN backup is configured in the database where production backup directory of DB is backed up on tape cartridge. Oracle X5-2 server is used as a backup Server & SL150 as a tape drive. The data retention policy is of 2 weeks. Dissemination data base, Export / Import directory and service sector backup is configured through a script and executed twice a day at 5:10 AM and 2:00 PM respectively.

Details of Backup Software License are as following:

Sl. no	Product Description	Version		Supported OS
1	Netback up	8.3.0.1		Solaris 11

Sl. No	Item description	Qty License
1	Veritas NetBackup 8.3 Shared Storage Option License	8
2	Veritas NetBackup 8.3 Library Based Tape Drive Option License	8
3	Veritas NetBackup 8.3 Enterprise Server Unix License	1
4	Veritas NetBackup 8.3 Client Application And Database Pack Unix License	2
5	Veritas NetBackup V8.3, Enterprise Client, Unix License	4
6	Veritas NetBackup 8.3 Client Application And Database Pack Unix License	2

Details of database backup

The details regarding database backup are presented below;

Sl. No	Database Name	Backup Frequency	Tools used	Retention period	Media	RAID configuration
1	Production DB	Daily	NetBackup	15 Days	Tape	RAID 5
2	OBI DB	Daily	NetBackup	15 Days	Disk / Tape	RAID 5
3	DR DB	Not Scheduled				RAID 5
4	Dissemination DB	Daily	NFS	4 Days	Disk	RAID 5
5	IMP_EXP Dir DB	Daily	NFS	4 Days	Disk	RAID 5
6	Service Sector DB	Daily	NFS	4 Days	Disk	RAID 5

2.8. Storage Architecture

At DGCIS, Oracle FS1-2 storage is configured both in DC & DR SAN environment through SAN switch. The HBA (Host Bus Adapter) is installed and configured with 16 GB fiber channel speed.

The DC Oracle FS1-2 Storage is connected with two SAN switches which in turn are configured in failover mode. Total 24 port licenses have been activated for the mentioned SAN Switch.

Other storages in DC, namely, Oracle ZS3-2 and SUN 6140 Stg are connected with two SAN switches, which in turn are configured in failover mode. Total 8 port licenses have been activated for the above-mentioned SAN Switch.

The DR Oracle FS1-2 Storage is connected with two SAN switches, which in turn are configured in failover mode. Total 12 port licenses have been activated for this SAN Switch.

Total space of Storage of both DC and DR are mentioned in the following table:

Sl. No	Storage Description with (Hostname)	Location	Total RAW Space	Total free space	LUN	RAID	LUN Space (Used)	Server associated with LUN
1	Oracle FS1-2	DC	115 TB	37.9 TB	NR	RAID1, RAID6	44.6 TB	All hosts in DC except Dissemination service sector, Export-import DB Server
2	Oracle ZS3-2	DC	5.5 TB	3.8 TB	NR	RAID6	1.7 TB	dgcisdev2
3	SUN 6140 Stg	DC	21.79 TB	773.9 GB	NR	RAID1, RAID5	21 GB	Dissemination service sector, Export-import DB Serve
4	Oracle FS1-2	DR	115 TB	70.2 TB	NR	RAID1, RAID6	44.8 TB	All hosts in DR

DGCIS Server & Storage Architecture- DC

Following diagram depicts the Server & Storage Architecture of DC ;

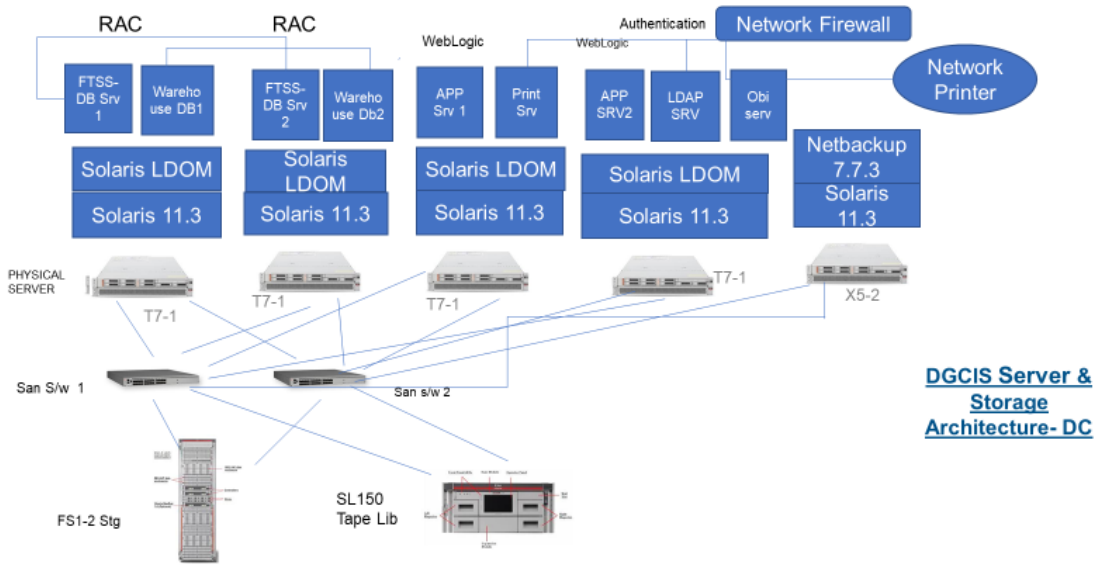


Figure 12: Storage Architecture

With regards to the above-mentioned diagram, the following table provides the SAN details of switch located in DC and DR with active license:

Sl. No	Switch Description with (Hostname)	Location	Make / Model / SL no	Total active license	Failover (Y / N)	OS Ver	Speed	Total Fiber Port used
1	SANSW_TOP	DC	Brocade 6510 48 Port	24	Y	v7.3.1a	16 GBps	24
2	SANSW_BOT	DC	Brocade 6510 48 Port	24	Y	v7.3.1a	16 GBps	24
3	SANSW_TOP	DC	Brocade 6505 16 Port	8	Y	v5.2.0a	16 GBps	8
4	SANSW_BOT	DC	Brocade 6505 16 Port	8	Y	v5.2.0a	16 GBps	8
5	SANSW_TOP	DR	Brocade 6505 16 Port 24 port	12	Y	v8.1.0a	16 GBps	12
6	SANSW_BOT	DR	Brocade 6505 16 Port 24 port	12	Y	v8.1.0a	16 GBps	12

LUN configuration at DC storage

The following table provides the detailed description regarding LUN configuration at DC storage:

Server Name	LUN Name	Space (GB)
prvftssapp1	APP1_Lun0	1650
prvftssapp2	APP2_Lun0	1650
prvftssdb1 & prvftssdb2		
	Backup_Lun0	1000
	Backup_Lun1	1000
	Backup_Lun2	1000
	Backup_Lun3	1000
	ExpDB_CtrlfileLun0	10
	ExpDB_DataHighPrfLun0	200
	ExpDB_DataLun0	400
	ExpDB_DataLun1	400
	ExpDB_DataLun2	400
	ExpDB_DataLun3	400
	ExpDB_DataLun4	400
	ExpDB_DataLun5	400
	ExpDB_DataLun6	400
	ExpDB_DataLun7	400
	ExpDB_DataLun8	400
	ExpDB_FRALun0	500
	ExpDB_FRALun1	500
	ExpDB_IndexLun0	200
	ExpDB_RedoLun0	100

Server Name	LUN Name	Space (GB)
	ExpDB_RedoLun1	100
	ExpDB_VoteLun0	5
	ExpDB_VoteLun1	5
	ExpDB_VoteLun2	5
	ExpDB_VoteLun3	5
	ExpDB_VoteLun4	5
	GG_Lun0	400
	GG_Lun1	400
	GG_Lun2	400
	GG_Lun3	400
	GG_Lun4	400
	GG_Lun5	400
	GG_Lun6	400
	GG_Lun7	400
	GG_Lun8	400
	GG_Lun9	400
	ImpDB_CtrlfileLun0	10
	ImpDB_DataHighPrfLun0	200
	ImpDB_DataLun0	400
	ImpDB_DataLun1	400
	ImpDB_DataLun10	400
	ImpDB_DataLun11	400
	ImpDB_DataLun12	400
	ImpDB_DataLun13	400
	ImpDB_DataLun14	400
	ImpDB_DataLun2	400
	ImpDB_DataLun3	400
	ImpDB_DataLun4	400
	ImpDB_DataLun5	400
	ImpDB_DataLun6	400
	ImpDB_DataLun7	400
	ImpDB_DataLun8	400
	ImpDB_DataLun9	400
	ImpDB_FRALun0	500
	ImpDB_FRALun1	500
	ImpDB_FRALun2	500
	ImpDB_FRALun3	500
	ImpDB_FRALun4	500
	ImpDB_FRALun5	500
	ImpDB_IndexLun0	200
	ImpDB_RedoLun0	100
	ImpDB_RedoLun1	100
prpovm3 / nodejsapp	nodejsapp_Lun0	300
	nodejsapp_Lun1	300
	UAT_Lun0	500
	UAT_Lun1	500

Server Name	LUN Name	Space (GB)
	UAT_Lun2	500
	UAT_Lun3	500
	UAT_Lun4	500
	UAT_Lun5	500
prpovm1 & prpovm2 (whdb1_ldg & whdb2_ldg)	WHDB_BackupLun0	500
	WHDB_BackupLun1	500
	WHDB_BackupLun2	500
	WHDB_DataLun0	200
	WHDB_DataLun1	200
	WHDB_DataLun2	200
	WHDB_DataLun3	200
	WHDB_DataLun4	200
	WHDB_DataLun5	200
	WHDB_FraLun0	200
	WHDB_FraLun1	200
	WHDB_GGLun0	200
	WHDB_GGLun1	200
	WHDB_GGLun2	200
	WHDB_GGLun3	200
	WHDB_RedoLun0	10
	WHDB_RedoLun1	10
	WHDB_VoteLun0	5
	WHDB_VoteLun1	5
	WHDB_VoteLun2	5
	WHDB_VoteLun3	5
	WHDB_VoteLun4	5
prvftssdb1	oswatcherdb1	100
prvftssdb2	oswatcherdb2	100
prpovm4 / whftssobi	Whobi_Lun0	550
	Whobi_Lun1	2000
prpovm3 / whftssstaging	whstaging_Lun0	550
	whstaging_Lun1	200
	whstaging_Lun2	200

2.9. Virtualization Architecture

At present, the virtual architecture is based on SPARC computing environment. Four Oracle SPARC T7-1 physical servers are currently installed and configured at DC with Sun Solaris virtualization and partitioning utility, LDOM, where 15 virtual hosts have been configured. DB and application servers are installed in these virtual hosts. The OS version in production environment is Solaris 11.3.

Virtual Host currently hosted in DC and DR:

The following table provides the details regarding Virtual Host currently hosted in DC and DR;

Production or other	Location	Total Core	Server Role	Memory (GB)	RAID	Storage Space allocated	Name of the App / DB	OS with Ver
Production	DC	9	Production Database Server	356	1	Yes	ftssidb	Solaris 11.3
Production	DC	3	warehouse Database Server	60	1	Yes	ftsswhdb	Solaris 11.3
Production	DC	9	Production Database Server	356	1	Yes	ftssidb	Solaris 11.3
Production	DC	3	Warehouse Database Server	60	1	Yes	ftsswhdb	Solaris 11.3
Production	DC	12	WebLogic Application Server	192	1	Yes	WLS_FORMS	Solaris 11.3
Production	DC	2	Test Server	16	1	Yes		Solaris 11.3
Production	DC	4	Bigdata AppTest Server	16	1	No		Solaris 11.3
Production	DC	2	App Test server	32	1	Yes		Solaris 11.3
Production	DC	1	Print Server	12	1	Yes		Solaris 11.3
Production	DC	2	Staging server	20	1	Yes		Solaris 11.3
Production	DC	2	Big data DB Test Server	16	1	No		Solaris 11.3
Production	DC	12	WebLogic Application Server	192	1	Yes	WLS_FORMS	Solaris 11.3
Production	DC	4	LDAP Server	16	1	Yes		Solaris 11.3
Production	DC	6	OBI Application Server	60	1	Yes	bi_server1	Solaris 11.3
Production	DC	4	Database Server	16	1	Yes	infra	Solaris 11.3
Production	DR	2	Application Server	10	1	Yes		Solaris 11.3
Production	DR	2	Application Server	10	1	Yes		Solaris 11.3

2.10. Software Licenses

Following are the details of licenses available for the present IT infrastructure components:

a. Oracle

Sl. No	Product Description	License Type	Version	RAC Cluster
1	Oracle Database Enterprise Edition ATS for Oracle 10g software, oracle database EE Processor perpetual license	Perpetual license	12.1.0.2.0	Yes
2	Oracle Database Enterprise Edition (Perpetual License)	Perpetual license	12.1.0.2.0	Yes
3	Oracle Database Enterprise Edition (Oracle Business Intelligence Suite Foundation Edition - Processor Perpetual License)	Perpetual license	12.1.0.2.0	Yes
4	Oracle Database Standard Edition (Oracle ATS of Oracle Database SE Oracle 1 - Click Ordering Programmed U0073er plus Perpetual License with Back Support	Perpetual license	11.2.0.1.0	No
5	Oracle Database Standard Edition Oracle ATS for providing on-site maintenance support of SUN Fire X4170 server		11.2.0.1.0	No
6	Oracle Database Enterprise Edition (Web logic) (Perpetual License) Golden Gate (Perpetual License)		11.2.0.1.0	No

b. Backup Software

Sl. no	Product Description	Version	Supported OS
1	Net Backup	8.3.0.1	Solaris 11

Sl. No	Item description	Qty License	Vendor
1	Veritas NetBackup 8.3 Shared Storage Option License	8	Veritas
2	Veritas NetBackup 8.3 Library Based Tape Drive Option License	8	Veritas
3	Veritas NetBackup 8.3 Enterprise Server Unix License	1	Veritas
4	Veritas NetBackup 8.3 Client Application And Database Pack Unix License	2	Veritas
5	Veritas NetBackup V8.3, Enterprise Client, Unix License	4	Veritas
6	Veritas NetBackup 8.3 Client Application And Database Pack Unix License	2	Veritas

4. Key considerations for Solution Architecture

Following sub-sections detail out the key considerations for the envisaged solution architecture.

4.1. Solution Architecture Goals & Considerations

The objective behind the revamped DGCIS System is to provide a comprehensive web based integrated system to cater the functions of DGCIS with enhanced service delivery and transparency. The proposed solution attempts to provide comprehensive, accurate, reliable and one stop source of information of export/ import trade data pertaining to DGCIS. The proposed system shall also integrate smoothly with external systems like ICEGATE for real time or near real time information interchange.

Following set of **application principles** are to be followed while devising the proposed solution:

S.N.	Principle	Rationale	Implications
1.	Scalable	• The more a user is growing with time accordingly application must support them. • The hardware, network related resources like bandwidth etc. may need to be increased. • DGCIS system may need for new features in future that must be added seamlessly • It very much possible that new modules also may be envisaged accordingly DGCIS system must be able to incorporate these.	• Logical separation of layers shall be considered to design the solution. Logical partition of application into interface layer, business layer, data layer makes possible to deploy application across several machines to achieve high level scalability. • Quality of Service (QOS) parameters shall be defined to address non-functional requirements. • By implementing functionalities in respective modules, application can be extendible for newer features straightforwardly in future.
3	Portable	• The different version of OS and database should be supported by DGCIS System.	• DGCIS system shall not be tightly coupled with the platform and shall be able to move to different platform.
4	Secure	• The DGCIS system deals with sensitive and classified data, hence it should ensure robust security at core feature for data in rest and data in motion. • DGCIS system should provide secure mechanism of authorization and authentication. • DGCIS system should provide strong encryption to secure application access. • Should be secure from threats like Cross-Site Scripting, SQL Injection, and other weaknesses	• If the DGCIS system involves data transfer to different external systems, during the data transfer, any leak in confidentiality may lead to communication hurdles among these offices.

S.N.	Principle	Rationale	Implications
5	Ease-of-Use	• DGCIS system should be easy to use by the internal users. • The more a user has to understand the underlying technology, the less productive that user is. • Ease-of-use is a positive incentive for use of applications.	• DGCIS System will be required to have a common ‘‘look and feel’’ and support ergonomic requirements. Hence, the common look and feel standard must be designed and usability test criteria must be developed. • Guidelines for user interfaces should not be constrained by narrow assumptions about user location, language (if required), systems training, or physical capability.

Following set of **data principles** to be followed:

S.N.	Principle	Rationale	Implications
1.	Shared Data	• Timely access to accurate data is essential to improve the quality and efficiency of enterprise decision-making. It is less costly to maintain timely, accurate data in a single application, and then share it, than it is to maintain duplicative data in multiple applications. The speed of data collection, creation, transfer, and integration is driven by the ability of the organization to efficiently share this data across the organization. • Shared data will result in improved decisions since user groups will rely on fewer (ultimately one virtual) sources and timely managed data for decision-making.	• Appropriate rules shall be setup for update and access of data. • Users shall be educated to understand the relationship between value of data, sharing of data, and accessibility to data.
2	Data Accessibility ty	• Wide access to data leads to efficiency and effectiveness in decision-making and affords timely response to information requests and service delivery. • Consider enterprise perspective to allow data access by a wide variety of users	• Accessibility involves the ease with which users obtain information. Centralized architecture of DGCIS System enables the user to maintain data at central repository and will be available to enterprise users through reports or web forms. • The way information is accessed and displayed must be sufficiently adaptable to meet a wide range of enterprise users and their corresponding methods of access. DGCIS System provides user

S.N.	Principle	Rationale	Implications
			specific dashboard based on user type and role played by the user. • Access to data does not necessarily grant the user access rights to modify or disclose the data. This will require an education process and a change in the organizational culture.

4.1.1 Architecture Design Goals

The proposed architecture is based on proven open-source technology. Open-source technology provides greater flexibility to end users and rationalizes cost expenditures which precisely are the key focus of DGCIS's current project.

The details of the defined goals are explained in detail below:

1) **Workflow Management**: The architecture supports the workflow to authorize and approve service.
2) **Web based Access:** A secure multi layered architecture is proposed for accessing DGCIS System through the Intranet / Internet.
3) **Ease of Deployment and maintenance:** The solution is built on layered architecture which provides a methodology of identifying the deployment patterns along with a clear break-up of the roles and responsibilities of each layer. It allows developer to modify the functionalities at one layer without affecting other layers. Hence, the solution shall allow easy & quick deployment with no impact on the other components or the system as a whole.
4) **Modularity:** Application shall be developed on modularity principle and allow module level implementation of application based on the requirement.
5) **Alerts and Notifications:** The solution can be made to allow users to sign up for e-mail and SMS notification. This can include both key performance indicator changes and changes in information. This feature will be configurable during implementation.
6) **User Friendly:** DGCIS System shall be easy to use, learn or understand. It will have simple user interface, well organized, intuitive with minimal requirement of explanation and reliable.
7) **Reusability:** The solution shall re-use components to reduce the timeframe to develop new functionalities of DGCIS applications.
8) **Personalization:** The ability for groups and individual users to customize the way that the information is displayed. Filtering content to the information that a group is interested in and being able to change the location of the information on the screen is considered an important way in which application creates a user –friendly experience.
9) **Dashboard Features:** The solution can be made to support dashboard feature to streamline the task management and alerts.
10) **Security Management:**

    Following are key considerations for security management,

    - Secure access over intranet/ Internet
    - Provide data privacy, confidentiality, and access control mechanism
    - Use of digital signature to authorize end users (optional)

- Data encryption for to safeguard from data theft.

4.1.2 Conformance to Standards

The solution needs to be based on and compliant with the industry standards applicable for all the aspects of DGCIS System including but not limited to project management, design, development, security, installation, and testing.

Following table summarize the said standards:

Application	Standard
Application Development	W3C Specification
Information access/transfer Protocols	SOAP, HTTP/HTTPS
Interoperability	Web Services, Open Standard
Information Security	ISO 27001 certified System
Operational Integrity & Security Management	ISO 17799 certified System
IT Infrastructure management	ITIL specification
Framework for IT Governance	Control Objectives for Information and related Technology (COBIT) framework
Service Management	ISO 20000 specifications
Project Documentation	IEEE/ ISO Specifications for documentation

4.1.3 Architecture Principles

Architecture Principles (AP) are agreed set of guiding principles that define the organization's approach to managing its technological assets. Essentially, Architecture Principles provide an essential communication link between the business and technology to help bridge the organizational gap and strengthen the alignment.

APs can be thought of as more detailed value statements or interpretations of the organization's general value statements to make them more applicable to technology. APs should represent the few points of stability upon which the organization can construct and maintain its Technical Architecture.

There are various quality-of-service-parameters around which these principles revolve and those are:

S.N.	Principle	Sub-Principle	Description
1	Availability	Manageability	The ability to gather information about the state of something and to control it
		Serviceability	The ability to identify problems and take corrective action, such as to repair or upgrade a component in a running system
		Performance	The ability of a component to perform its tasks in an appropriate time
		Reliability	Resistance to failure
		Recoverability	The ability to restore a system to a working state after an interruption
2	Assurance	Security	The protection of information from unauthorized access
		Integrity	The assurance that data has not been corrupted

S.N.	Principle	Sub-Principle	Description
		Credibility	The level of trust in the integrity of the system and its data
3	Adaptability	Interoperability	Suitable for global audience (for instance, interoperability of calendaring or working days functions may be key to the usefulness of a system)
		Scalability	The ability of a component to grow or shrink its performance or capacity appropriately to the demands of the environment in which it operates
		Portability	Of data, people, applications, and components
		Extensibility	The ability to accept new functionality

4.2. Open Source & GoI Perspective

Government of India has been promoting the use of open-source technologies and has been keenly encouraging its adoption in the e-Governance movement of the country. Department of Electronics and Information Technology (DeitY), Government of India has formulated The "Policy on Adoption of Open-Source Software for Government of India" to enable effective adoption of OSS and encourage the formal adoption and use of Open-Source Software (OSS) in Government Organizations. The policy has been approved and notified vide Gazette notification dated 27.03.2015.

It has been observed in recent past that many Central Government entities and State governments are increasing their engagement on open source for greater control on the product being developed. Governments using open-source software, open standards, and open data policies, as part of 'Digital India' initiatives to enhance crowd sourcing. Open-Source Software (OSS) is preferred in e-Governance systems over Closed Source Software (CSS). However, GOI does not make OSS mandatory for future developments.

Open Source refers to the "Availability of Source code" for the end-user to study and modify the software and to redistribute copies of either the original or modified software.

Following factors are typically considered for adoption of open technology:

- Cost Reduction
- Quality Improvement
- Reduced time to Market
- Full Ownership and Control
- Freedom to use & reuse
- Innovation
- No vendor Lock-in
- Availability of OSS stack
- Technological Compatibility based on Standards
- Enhanced security
- Support from OSS community
- Growing OSS community
- wider choices on OSS
- Enhanced competition

Operational support for software and Source code level supports are required during the project life cycle. These supports depend upon the license obtained for the project. There are different types of licensing options available in the market. With only open-source licensing without premium services, no vendor lock-in exists. The OSS solution is managed / driven mostly by a community / foundation. Other type of licensing

may introduce vendor lock-ins. Some of Challenges in OSS Adoption are Lack of dedicated support from vendor, OpenSource licenses issues and lack of accountability etc.

Fundamental differences between Open-Source Systems and Proprietary Systems are mentioned below:

Sl. No.	Attribute	Open-Source Systems	Proprietary Systems
1.	**Source Code**	Open-source systems are those whose source code is available openly on the internet and programmers can modify it to add new features and capabilities without any cost.	Proprietary software is a computer software where the source codes are not publicly available, only the company which has created can modify it.
2.	**Development**	Systems are developed and tested through open collaboration.	Systems are developed and tested by the individual or organization by which it is owned not by public.
3.	**Installation**	Open-source systems can be installed into any user machine without the need for specific licensing or royalties.	Proprietary systems can be installed into any computer without valid license and the proper environment as mandated by the individual or organization by which it is owned.
4.	**Licensing**	Users do not need to have any authenticated license to use this software.	Users need to have a valid and authenticated license to use this software.
5.	**Software Management**	Open-source software is managed by an open-source community of developers.	Proprietary software is managed by a closed team of individuals or groups that developed it.
6.	**Functionalities**	Functionalities of Open-source systems are dependent on the developer community and may lead to trickier usage and may lack user-friendly features, affecting productivity in the workplace	Proprietary systems are easier to use and learn, leading to faster work processes, due to robust testing and analysis before market entry.
7.	**Usability**	A product developed within open-source communities will appeal to more users and have lots of features. Unskilled end users, however, may find it difficult to navigate them and take full advantage of what they have to offer.	Proprietary technology appeals to specific users and has a smaller number of features than open-source software. Dedicated user manuals and comprehensive documentation are generally available for end-user ease.
8.	**Security**	As open-source code is available to everybody, it increases the possibility of finding more vulnerabilities easily. It is also worth noting that open-source communities fixed security vulnerabilities twice as quickly as commercial software vendors do.	Proprietary software is considered secure as it is developed in a governed condition of the employees having a frequent direction. However, getting rid of the possibility of backdoor Trojans as well as lowering the threat of any other bugs or obstacles can be troublesome in proprietary software.
9.	**Support**	Open-source systems support would be dependent on the vendor who develops it and may require additional maintenance support contract for continuous improvement and patches and bug-fixing.	Proprietary systems are more accessible and includes generally include technical support in their costing. Most companies offering these programs provide dedicated

Sl. No.	Attribute	Open-Source Systems	Proprietary Systems
			sources, 24/7 assistance and user manuals.
10.	**Vendor Lock-in**	Users of Open-source systems have the freedom to pick and choose the best of the available software/ systems and not be bound by vendor lock-in standards.	With proprietary systems, the organization obligate and restrict the user with associated products which will by default be proprietary in nature and there is no getting out of that loop of dependency on these costly software vendors.
11.	**Flexibility**	As organizations aim at deriving more business values from less, open-source software can deliver high flexibility, lower IT costs and increased opportunities for innovation.	With proprietary software, companies are required to upgrade both software and hardware on a timely basis. Updates must be installed for the proper working. However, not all updates are flexible with all the versions of the software.

4.2.1 GoI advisory / guidelines on OSS

The **Policy on Adoption of Open Source Software for Government of India** (GoI) (https://meity.gov.in/writereaddata/files/policy_on_adoption_of_oss.pdf)also acknowledges this and aims to "Government of India shall endeavour to adopt Open Source Software in all e-Governance systems implemented by various Government organizations, as a preferred option in comparison to Closed Source Software. The source code shall be available for the community/adopter/end-user to study and modify the software and to redistribute copies of either the original or modified software"

Policy on Collaborative Application Development by Opening the Source Code of Government Applications.[3] The policy intends to increase the pace of e-governance application development and rapid roll-out/implementation by adopting an open-source development model based on current worldwide practices like GitHub and Source Forge. By this policy, the Government of India wants to promote re-use of existing developed applications. By opening the source code, the Govt. of India wants successful, scalable, high-quality eGov applications to be developed in a collaborative manner. It also wants new applications to be developed to encourage creativity — both inside and outside the Government by encouraging collaborative development between Govt. departments/agencies and private organizations, citizens, and developers to create innovative eGov applications and solutions. eGov application source open approach including the use and release of application source code to public can reduce costs and development time and improve the overall quality and security through increased transparency and mass peer review.

List of various technology options available for the project implementation are shown below:

4.2.2 Operating System

According to Statista Report on "Operating system distribution for software development worldwide in 2018 to 2021" (https://www.statista.com/statistics/869211/worldwide-software-development-operating-system/),

[3] (https://www.meity.gov.in/content/collaborative-application-development-opening-source-code-government-applications)

the following is the most popular Operating Systems amongst developers. Most of the open-source operating systems today, uses Linux kernel, such as Ubuntu, Red Hat Enterprise Linux, and CentOS .

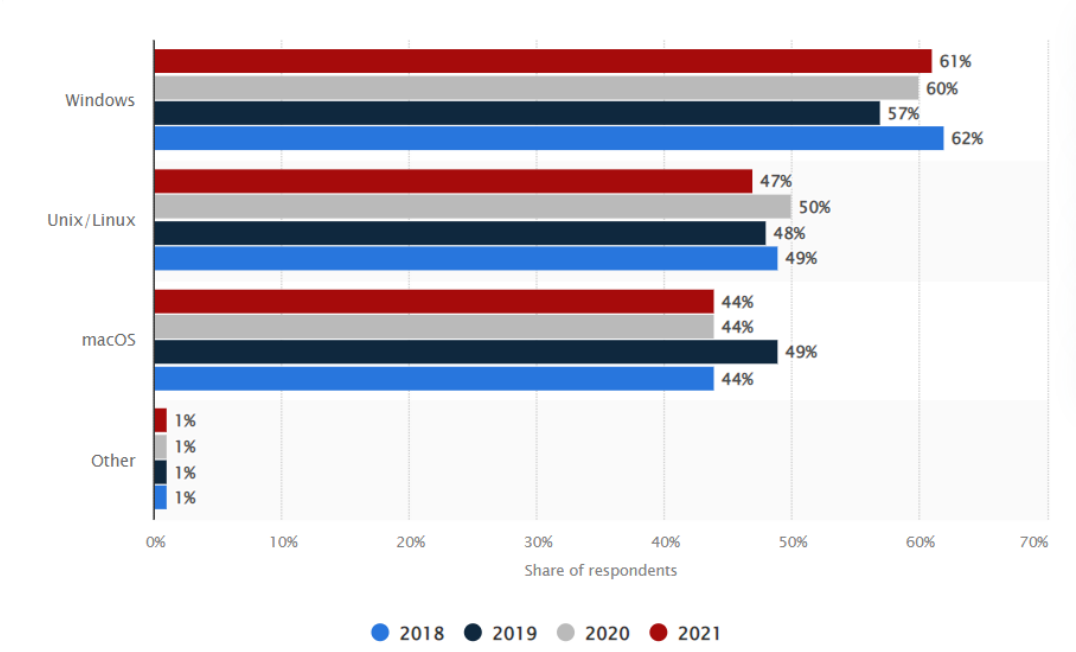


Figure 15: Operating System Popularity amongst Developers

The Red Hat State of Enterprise Open-Source report 2022 (https://www.redhat.com/en/enterprise-open-source-report/2022) found that businesses typically choose open-source software because it's cheaper, with 33% of enterprise users citing its lower total cost of ownership (TCO) as its chief benefit. There is a shift in thinking, however, with 29% turning to open source because it gives them access to the latest innovations – a reference to the crucial role of open-source technologies in supporting microservices and containers in the cloud, or its use in the burgeoning field of machine learning.
Linux distributions may be community-developed, like Debian, Slackware, and Gentoo. Other distributions are commercial and intended for enterprise use, including **Red Hat Enterprise Linux and SUSE Linux Enterprise Server**. Many distributions use a combination of community- and corporate-supported development, such as Red Hat's Fedora, openSUSE from SUSE and Ubuntu from Canonical.

Vastly used Linux distributions for enterprise applications are as follows:

- Red Hat Enterprise Linux Desktop
- SUSE Linux Enterprise Desktop
- Ubuntu desktop for the enterprise
- CentOS

Currently, at DGCIS the primary OS used is Solaris 10/11. Solaris is a proprietary Unix operating system originally developed by Sun Microsystems. As it is a licensed version, the price is quite expensive for the commercial operating system and DGCIS must renew licenses on a regular basis for proper functioning, patch installation and other upgradation and maintenance activities.
Both Linux and Solaris are UNIX-like operating systems with virtual memory, paging, system calls, processes, kernels, buffers, caches, resource controls, mapped files, multiprocessor support, CPU scheduling and support, and other features in common with UNIX. Linux and Solaris each have their own set of command-line options. It is relatively simple to utilize another an organization is already familiar with one. Detailed differences between deployment in RedHat Enterprise Linux and Solaris 11 can be found at: https://www.oracle.com/solaris/technologies/solaris11-redhat-mapping-guide.html

4.2.3 Database Options

Over decades of evolution, research and development, many opensource databases have emerged as cost effective enterprise grade solution for many complex applications. In the last few years, many companies have been turning away from the constraints and limitations of proprietary software and adopting open-source software. The basic differences between Open-Source databases and Commercial databases are enumerated below:

Features	Open-source database	Commercial database
Flexibility	Open source offers more flexibility to users	Proprietary software is less flexible and often comes with restrictions
Maintenance	Developed and maintained by a community	Developed and maintained by the organization that published it
Support	May not have the support or capacity of a proprietary database	Single contact point for any problems that occur
Licenses	Free to view, download, modify, distribute, and reuse	Does not allow access to the source code or modifications
Compatibility	No guarantee that opensource software will work in each user's environment	Compatible with the user's environment
Cost	Zero, upfront licensing costs	Expensive to license and maintain proprietary software
Access to data	With an open format, data sets can be returned from simple SQL query statements	Data cannot be accessed and viewed directly. Custom or proprietary tools must be used to access your data
Top databases	MySQL, PostgreSQL, MongoDB, Cassandra	Oracle, Microsoft SQL Server, DB2, Microsoft Access

As per the "Ranking of the most popular open source database management systems (DBMS) worldwide, as of January 2022" by Statista, following are the most 2 most common databases used by professional developers (https://www.statista.com/statistics/1131602/worldwide-popularity-ranking-database-management-systems-open-source/) in comparison with Oracle, which is the current Database used in DGCIS:

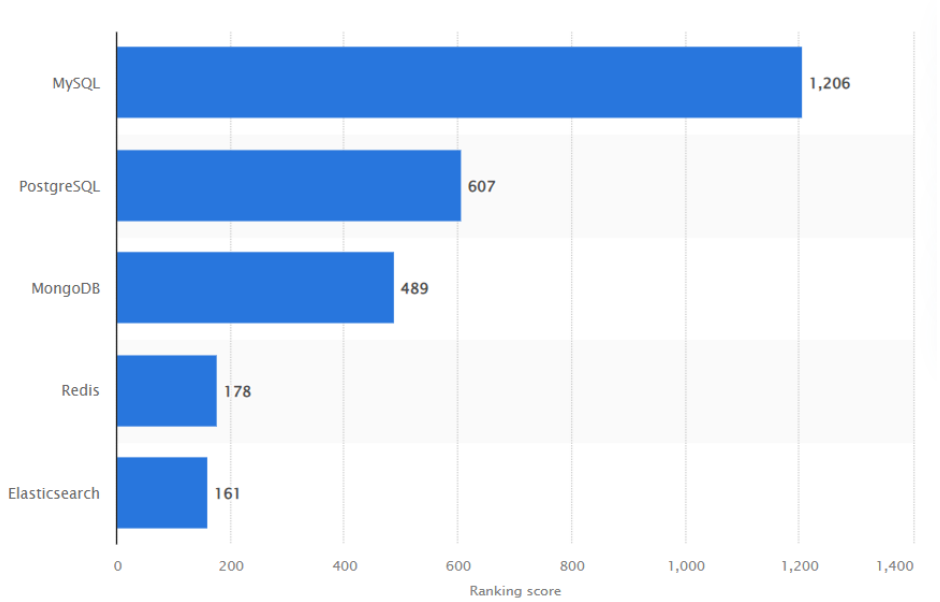


Figure 16: Open-Source Database Popularity amongst Developers

S.N.	Parameters	Oracle	PostgreSQL	MySQL
1.	**Description**	Widely used RDBMS	Based on the object relational DBMS Postgres	Widely used open-source RDBMS
2.	**Primary database model**	Relational DBMS	Relational DBMS	Relational DBMS
3.	**Additional database models**	Document store Key-value store	Document store Key-value store	Document store Key-value store
4.	**DB-Engines Ranking**	Score - 1348.80 Rank #1 Overall #1 Relational DBMS	Score - 373.27 Rank#4 Overall #4 Relational DBMS	Score - 1298.83 Rank #2 Overall #2 Relational DBMS
5.	**Website**	www.oracle.com/database/index.html	www.postgresql.org	www.mysql.com
6.	**Technical documentation**	docs.oracle.com/en/database	www.postgresql.org/docs/manuals	dev.mysql.com/doc
7.	**Developer**	Oracle	PostgreSQL Global Development Group	Oracle
8.	**Initial release**	1980	1989	1995
9.	**Current release**	12 Release 2 (12.2.0.1), March 2017	10.0, October 2017	5.7.20, October 2017

S.N.	Parameters	Oracle	PostgreSQL	MySQL
10.	**License**	Commercial	Open Source	Open Source
11.	**Cloud-based (Only available as a cloud service)**	No	No	No
12.	**Implementation language**	C and C++	C	C and C++
13.	**Server operating systems**	AIX HP-UX Linux OS X Solaris Windows z/OS	FreeBSD HP-UX Linux NetBSD OpenBSD OS X Solaris Unix Windows	FreeBSD Linux OS X Solaris Windows
14.	**Data schema**	Yes (Schema-less in JSON and XML columns)	Yes	Yes
15.	**Data Typing**	Yes	Yes	Yes
16.	**XML support**	Yes	Yes (specific XML-type available, but no XML query functionality)	Yes
17.	**Secondary indexes**	Yes	Yes	Yes
18.	**SQL**	Yes	Yes (standard with numerous extensions)	Yes (with proprietary extensions)
19.	**APIs and other access methods**	ODP.NET Oracle Call Interface (OCI) JDBC ODBC	native C library streaming API for large objects ADO.NET JDBC ODBC	ADO.NET JDBC ODBC
20.	**Supported popular / widely used programming languages**	C C# C++ Java JavaScript Perl PHP Python R Ruby Visual Basic	.Net C C++ Delphi Java info Perl PHP Python	C C# C++ Java JavaScript (Node.js) Perl PHP Python Ruby
21.	**Server-side scripts (Stored Procedures)**	PL/SQL	user defined functions	Yes (proprietary syntax)
22.	**Triggers**	Yes	Yes	Yes
23.	**Partitioning methods**	horizontal partitioning	no, but can be realized using table inheritance	horizontal partitioning, sharding with MySQL Cluster or MySQL Fabric

S.N.	Parameters	Oracle	PostgreSQL	MySQL
24.	**Replication methods**	Master-master replication Master-slave replication	Master-slave replication	Master-master replication Master-slave replication
25.	**Consistency concepts (Methods to ensure consistency in a distributed system)**	Immediate Consistency	Immediate Consistency	Immediate Consistency
26.	**Foreign keys**	Yes	Yes	Yes
27.	**Transaction concepts**	ACID	ACID	ACID
28.	**Concurrency**	Yes	Yes	Yes (table locks or row locks depending on storage engine)
29.	**Durability (Support for making data persistent)**	Yes	Yes	Yes
30.	**In-memory capabilities**	Yes (Version 12c introduced the new option 'Oracle Database In-Memory')	No	Yes
31.	**User concepts (Access control)**	fine grained access rights according to SQL-standard	fine grained access rights according to SQL-standard	Users with fine-grained authorization concept (no user groups or roles)

* Reference:

1. https://db-engines.com/en/system/MySQL%3BOracle%3BPostgreSQL

Among various versions of PostgreSQL available in the market, “PostgreSQL Enterprise Advanced DB” has developed database compatibility for Oracle based on popular features across many versions of Oracle. EDB’s goal has always been to create a critical mass of compatibility for the most popular features regardless of Oracle version to enable EDB Postgres Advanced Server to support Oracle workloads and provide end users significant cost savings for a large portion, or in some cases all, of their Oracle footprint. In selecting new features for every software release, EDB focuses on the most popular features whose value to customers meets one or more of the following criteria[1]:

- **Reduced Technical Risk:** This refers to objects or code created in Oracle that can be migrated and executed “as is” against or inside an EDB Postgres Advanced Server database and behave or produce the identical result as they would in Oracle.
- **Reduced Re-training Risk:** This means that knowledge, skills, and tools most frequently used with Oracle can also be used with EDB Postgres Advanced Server significantly reduce the learning curve needed to be productive quickly in either creating new applications or migrating old ones.
- **Reduced Integration Risk: This** means that EDB Postgres Advanced Server databases and applications can integrate well with existing Oracle infrastructure and non-database software that will be retained or cannot be changed for the foreseeable future.

[1]Source: https://www.enterprisedb.com/: Technical comparison report of edb-postgres-enterprise-and-oracle-enterprise

Since, DGCIS officials are well versed with the Oracle database and its features, PostgreSQL Enterprise Advanced DB is the most suitable option among other opensource database options to migrate.

4.2.4 Programming Language to be considered (Front-end and Back-end)

The proposed application and the modules shall be developed on open languages and scripts. The application development can be segregated into two parts, one is front-end web application design & development, and another is the backend development, i.e., the server-side application.

The front-end webpages shall be designed on HTML/HTML5 along with Cascaded Style sheets (CSS) and JavaScript. The following table gives a brief on how these programming languages and tools shall help to design and develop the front end of the DGCIS application.

Sl. No	Language	Usage
1	**HTML/ HTML5**	HTML makes up the layout and structure for the DGCIS application web pages and forms. It would also help DGCIS to design and develop a responsive web application so that the same application can be accessed from both laptop/desktop and mobile, without distorting the overall look and feel.
2	**CSS**	Cascaded Style Sheet (CSS) is to be embedded inside the HTML/HTML5 and to be used to enrich the overall user interface design of the application. It would help DGCIS to manage the design part in a structured way. So that same design code blocks can be used in multiple web pages to provide a uniform design to the entire application.
3	**Java Script**	JavaScript is a scripting language used at presentation layer (i.e., at client side) to add interactive elements such as buttons and toggles to the web application. JavaScript shall be used for validation purpose which will validate the user input at local machine (i.e., at client side) before sending a request to the server. This is will help DGCIS to enhance the performance of the web pages.

As DGCIS users have previous understanding and basic experience of Python and Java, it is better if these two languages can be used to develop the backend and the server-side application. Java shall be used to develop the business logics and APIs and Python to be used to develop and implement the machine learning principles. Python also has an extensive in-built library to integrate AI in web development. These handy third-party libraries are one of the main reasons for the popularity of Python in the industry.

While deciding on the technology to be adopted, DGCIS should consider the following factors:

- Availability of Technically skilled manpower to support the development and operations
- Readily Availability of Development and technical support from companies in market
- Ease of Integration with other systems and systems management
- Ease of inhouse capabilities to train and manage the application on its own

However, at the same time, the option of selection of open technology may be left to vendor itself with a provision to train all the manpower at DGCIS for self-sustenance of operations. Further, DGCIS should consider training their core resources on whatever stack is adopted.

4.3. Cloud versus Data Centre models

The Cloud presents an opportunity for Information Technology (IT) & IT Enabled Services (ITES) sector by opening up a new avenue of providing Cloud based services to global organizations ranging from Software

as a Service (SaaS) based application services, Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).

However, on one hand where Cloud promises to change the way Indian businesses and Government leverage technology to their benefit, on the other hand it also presents challenges relating to security and privacy of information.

A comprehensive policy for adoption of Cloud in India is thus the need of the hour. It is important for all stakeholders in India to understand the implications of this disruptive technology and harness it for the good of the nation.

A comparison of cloud, collocated servers and dedicated servers are shown below:

Cloud	Collocated Servers	Dedicated Servers
✓ The cloud is a virtual environment that eliminates the costs involved in expanding storage space, memory, and processor power. ✓ All the compute resources are shared and provides flexibility to scaleup and down resources at a very short notice ✓ Down time is negligible, however data security can be a concern ✓ Information on the cloud is easily accessible from different devices with only a few clicks. Here, data is centralized to ensure that vital information is available to anyone with clearance to access it. ✓ Highly Cost effective and saves a lot of capital investment involved in setting up new data centre and server purchases. All CapEx is converted to OpEx ✓ Faster deployments ✓ Compartmentalizing resources by function allows for scalability, management, and resource segmentation. This can be achieved cost effectively in the cloud.	✓ Collocating servers in a common environment benefits smaller organizations that wouldn't afford to invest in setting up data centres ✓ All compute resources are purchased upfront and installed at the shared datacentre. It is very difficult to scale up at a very short notice. ✓ Shares the Rackspace, Cooling and other common monitoring services shared resources to run and manage the infrastructure ✓ Expensive as CapEx is required to Purchase new Hardware. ✓ However, it can be offered on a OpEx model by Some cloud vendors but with a lock in period. ✓ Colocation is an excellent option for businesses that wish to outsource data management while retaining control of their hardware. ✓ It Offers higher data security than cloud environment as infrastructure is not shared.	✓ Customers has an inhouse datacentre ✓ With dedicated servers' hardware and management is carried out by the internal team ✓ All compute resources are purchased upfront and installed at the shared datacentre. It is very difficult to scale up at a very short notice. ✓ Involves high Capital Costs ✓ Scalability is not possible at a short notice. You have to buy hardware factoring in future requirements. ✓ Managing the entire infrastructure ✓ requires manpower and resources ✓ Businesses using dedicated servers still need the IT capacity and expertise to manage the ongoing maintenance ✓ Initially for setting up, dedicated servers can take considerably longer, even weeks in some circumstances. ✓ Has a risk of hardware obsolescence

4.3.1 Cloud Computing

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud model promotes availability and is composed of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service); three service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)); and four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud).

Key enabling technologies include:

1. Fast wide-area networks,
2. Powerful, inexpensive server computers, and
3. High-performance virtualization for commodity hardware.

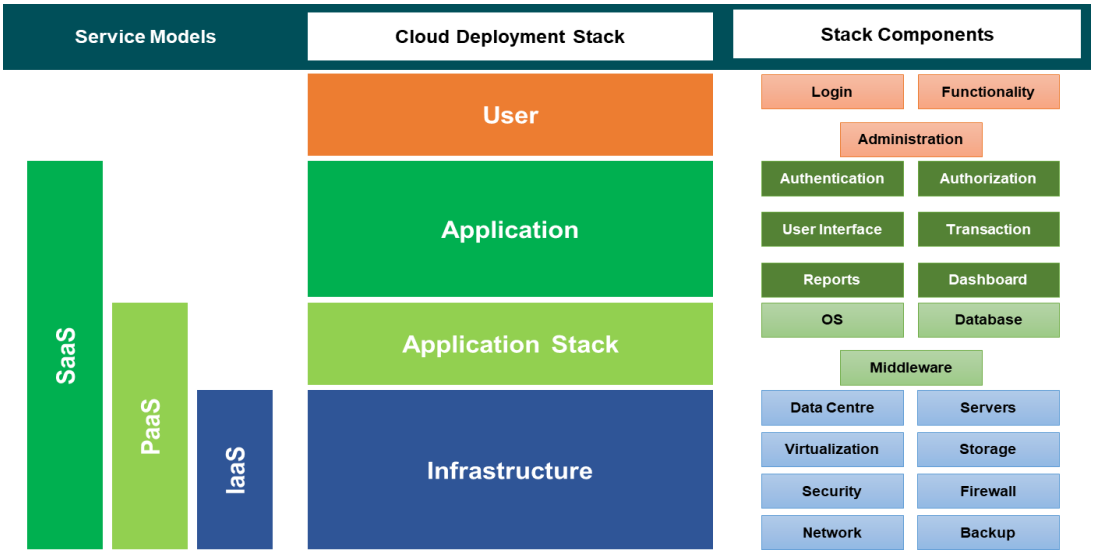


Figure 17: Cloud Infrastructure components

The Cloud Computing model offers the promise of massive cost savings combined with increased IT agility. It is considered critical that government and industry begin adoption of this technology in response to difficult economic constraints. However, cloud computing technology challenges many traditional approaches to datacentre and enterprise application design and management. Cloud computing is currently being used; however, security, interoperability, and portability are cited as major barriers to broader adoption.

The long-term goal is to provide thought leadership and guidance around the cloud computing paradigm to catalyse its use within industry and government. Cloud Computing aims to shorten the adoption cycle, which will enable near-term cost savings and increased ability to quickly create and deploy enterprise applications.

DGCIS aims to foster cloud computing systems and practices that support interoperability, portability, and security requirements that are appropriate and achievable for important usage scenarios.

The fundamental economics of Cloud computing depends on the ability of cloud service provider (CSP) to operate large and efficient data centres in order to service a large customer base. In order to maximize on the economic efficiency, many cloud vendors have created a geographically distributed data centre strategy.

4.3.2 Cloud Computing - Government of India Perspective

In order to utilize and harness the benefits of Cloud Computing, Government of India has embarked upon a very ambitious and important initiative – “GI Cloud” which has been coined as **MeghRaj**. The focus of this initiative is to evolve a strategy and implement various components including governance mechanism to ensure proliferation of Cloud in government. DeitY has announced MeghRaj Policy to provide strategic

direction for adoption of cloud services by the Government (http://deity.gov.in/content/gi-cloudinitiative-meghraj). The aim of the cloud policy is to realize a comprehensive vision of a government private cloud environment available for use by central and state government line departments, districts, and municipalities to accelerate their ICT-enabled service improvements.

As per the MeghRaj policy, Government of India has already setup GI Cloud, Government of India's cloud computing environment. GI Cloud is a set of discrete cloud computing environments spread across multiple locations, built on existing or new (augmented) infrastructure, following a set of common protocols, guidelines and standards issued by the Government of India. MeghRaj cloud service offerings for a combination of the Deployment Models (Public Cloud, Virtual Private Cloud and Government Community Cloud):

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Disaster Recovery as a Service (DRaaS)
4. Dev / Test Environment as a Service (DevOps)
5. Virtual Desktops as a Service (VDaaS)

The Government Departments are advised to select appropriate cloud service offerings based on the risk & security profile of their applications / data / services. The Government of India cloud was maintained by NIC across India through its National Data Centre. In this regard various types of services offered by NIC or empanelled Cloud service provider are: -

- Infrastructure as a Service
- Platform as a Service
- Software as a Service
- Vulnerability assessment Service
- Load balancer as a Service
- Public IP Service
- Antivirus Service
- Resourcing monitoring as a Service
- Web application firewall Service
- Backup Service
- Storage as a Service
- Application performance management Service
- Data analytic as a Service
- GoI Search as a Service
- e-Granthalaya as a Service
- Chatbots as a Service
- Agile as a Service
- DR as a Service
- Security as a Service
- Software defined network

In this respect, MeitY (Ministry of Electronics and Information Technology) has provisionally empanelled the Cloud Service Providers for a variety of Cloud deployment models and Cloud Service offerings. The empanelment of the Cloud service offerings of CSPs has been done for a combination of the Cloud Deployment models and Service models as mentioned below:

- **Public Cloud** – A shared multi-tenant IT infrastructure which is made available over Internet. It is owned and operated by a Cloud Service Provider delivering Cloud Services to the Government Departments

- **Virtual Public Cloud** – A logically separated Cloud Infrastructure to protect data, applications and VMs and provide robust virtual isolation for the Government Departments

- **Private Cloud** – A Cloud with IT Infrastructure resources which will be dedicated for two or more Government Departments that have common privacy, security, and regulatory requirements

MeitY has empanelled the following 18 companies for providing cloud computing services to government departments[4]:

1. Amazon Internet Services Pvt. Limited
2. Bharat Sanchar Nigam Limited (BSNL)
3. CtrlS Data Centres Limited
4. Cyfuture India Private Limited
5. ESDS Software solution Pvt. Limited
6. Google Cloud India Pvt Ltd
7. IBM India Private Limited
8. ITI Limited
9. Microsoft Corporation (India) Private Limited
10. Netmagic IT Services Private Limited
11. Nxtra Data Limited
12. Oracle India Pvt. Ltd
13. Pi Datacentres Pvt. Ltd.
14. RailTel Corporation of India Limited
15. Reliance Corporate IT Park Limited
16. Sify Technologies Limited
17. Tata Communications Limited
18. Webwerks India Pvt. Limited

4.4. IT Cloud Migration Roadmap

In today's tech world, cloud computing is becoming a mainstream component of enterprise IT. Cloud makes a compelling business case and addresses the operational, tactical, and strategic requirements of organizations by providing customer-specific solutions. A cloud Data Centre is significantly different from a traditional Data Centre; there is nothing similar between these two computing systems other than the fact that they both store data. In case there are any failures, cloud services provider will make sure that there is a backup of data available. The main difference between the cloud vs. data centre is that a data centre refers to on-premises hardware while the cloud refers to off-premises computing. The cloud stores the data in the public or private cloud, while a data centre stores data on own hardware. To utilize benefits of on-premises infrastructure and the flexibility of cloud environment, organizations are actively analysing Hybrid deployment of their IT infrastructure to secure their sensitive data and also not missing out on the advantages cloud deployment provides.

As DGCIS is planning to revamp the entire IT system, it is suitable time to invest in cloud First strategies and architectures and migrate the IT system on cloud. The Cloud based environment provides dynamic computing allocation based on dynamic computing load requirements and the service charges is on a subscription basis.

DGCIS needs a scalable architecture to support on-demand capacity and ever-increasing amounts of data. Public cloud shall address scalability requirements. Cloud allows organizations to augment data centre capacity and to take advantage of value-added services and rapid development and delivery of services.

[4] https://www.meity.gov.in/writereaddata/files/CSPs%20Details_04.01.2022.pdf

4.4.1 Cloud Migration options

The different methods for moving to the cloud are as follows:

- **Rehost:** Redeploying to an IaaS environment and changing the application's configuration to work in a new virtual hardware environment.
- **Refactor:** Redeploying to PaaS, thereby making use of familiar languages and frameworks while at the same time taking advantage of the cloud characteristics running on top of the provider's infrastructure.
- **Revise:** Modifying an existing codebase to meet cloud adoption or legacy modernization goals. Then rehosting or refactoring it to the cloud.
- **Rebuild or Re-Architect:** Discarding existing code and re-architecting the application for a new software framework.
- **Replace:** Discarding an existing application and using a proprietary pay-as-you-go SaaS solution instead.

Re-architecting is far more time-consuming and expensive than rehosting. However, rebuilding applications from scratch will make service infrastructure more streamlined, agile, and better able to take advantage of cloud scalability and elasticity. For example, Automate resource provisioning, which will reduce the time and cost of expanding infrastructure to support future growth. Over time, Re-architecting will be a better financial investment.
Re-architecting is a lower risk strategy because retrofitting a legacy application might not necessarily work. As DGCIS is revamping the existing IT Eco-System hence all the applications is needed to be developed fresh, also new software framework should be considered while rearchitecting the entire ecosystem.

4.4.2 Cloud migration assessment checklist

A common perception is that migrating existing workloads to the government empanelled cloud, especially those with a lot of data, is complex, time consuming and risky. With the right planning, however, enterprise IT organizations can rapidly establish good migration practices to accelerate migrations and lower risk. Plus, migration technology is evolving quickly to support the enterprise. The four key parts of the migration process: Assess, Plan, Migrate, and Optimize.

Phase – 1: Assess

Following are the key activities to be conducted during the assess phase:

- Define the resources and capacity required by the DGCIS application
- Creation of exhaustive list of applications envisaged to be hosted on Cloud (e.g., who is using what and how often)
- Identification of key stakeholders and involving them in the process of migration
- Determine which applications/ modules are cloud-eligible and which applications/ modules are cloud-desirable
- Understand application interdependencies and network configurations
- Specification of security and compliance requirements
- Validation of SLA and high availability requirements

Phase – 2: Plan

Following are the key activities to be conducted during the Plan phase:

- Pick a strategy for each application/ module: rehost, re-platform, or rebuild
- Plan and design the cloud infrastructure including services like networking, security, etc.
- Identify key capabilities for migrating workloads
- Support for complex, multi-tier apps
- Pre-migration testing & validation
- On-prem rollback
- Post-migration customization
- Create migration plan for both application and DB

Phase – 3: Migrate

Following are the key activities to be conducted during the Plan phase:

- Migrate according to the plan created
- Use a phased approach, and for each phase:
- Execute migration wave
- Validate in cloud and apply lessons to next wave

Phase – 4: Optimize

Following are the key activities to be conducted during the Optimize phase:

- Monitor application and cloud usage
- Implement bursting or scaled usage to optimize user experience
- Empower IT to successfully manage ongoing operations
- Monitor cloud costs and adjust as needed

Post Migration Testing

Following are the key activities to be conducted during the Post Migration Testing phase:

- Test data migration and synchronization
- Measure performance
- Validate security controls required
- Evaluate your cloud footprint costs
- Document necessary changes to be done as part of the actual migration
- Plan the time required for application cutover
- Consider cloud instance right-sizing recommendations

4.4.3 Cloud Framework and Assessment Criteria

The table below describes the assessment criteria and the inception, implementation, and Operation maintenance phase of CSP: -

Assessment Criteria	Inception Phase	Implementation Phase	Operation Phase
Phase Description	✓ Idea Assessment ✓ Business case validation ✓ Business Requirements ✓ CSP assessment and selection ✓ Application development	✓ Solution design ✓ Build ✓ Production deployment ✓ Testing ✓ Commitment to operate	✓ Application in production ✓ SLA ✓ Ongoing support & maintenance ✓ Reporting & Auditing ✓ Continuous improvements
Availability of local data centre	✓ Validate data sovereignty requirements. Do not proceed if these are non-compliant.	✓ Monitor and track local datacentre availability and development.	✓ Deploy the data centre in compliance with data sovereignty requirements.
Security	✓ Ensure CSP should meet the security requirements.	✓ Validate security architecture.	✓ Ensure security features are in place before deployment. Conduct VAPT, Patch management etc. for better security control.

Assessment Criteria	Inception Phase	Implementation Phase	Operation Phase
Flexibility	✓ Key criteria for selecting CSP. Ensure support for business continuity.	✓ Agree on variable resilience requirements depending on criticality.	✓ Ensure adherence to resilience requirements. Preparedness for unplanned activities.
Storage	✓ Assess data storage capacity requirements.	✓ Define data strategy.	✓ Ensure data storage is in line with data strategy.
Certification and Auditing	✓ Checks on CSP provider accreditation. Review the existing auditing supported by CSP.	✓ Valid certification. Determine any additional auditing requirements.	✓ Ensure provider certification maintained. Conduct continuous auditing and ensure governance process is in place.
Solution	✓ Review and validate CSP offerings and solution components	✓ As per architecture ensure right solution needs to be implemented.	✓ Support and upgrade.
Adaptability	✓ Ensure CSP commitment to deliver assessment criteria.	✓ Agree on framework for changes and modifications.	✓ Extend support this should include as a part of standard operations.
Portability	✓ Key design principle accepted widely available components to ensure low exit barriers.	✓ Implementation of selected components during build phase.	✓ Ensure ongoing support and avoid components that directive strict coupling with the provider.

Government India has enlisted 18 Cloud service providers (CSP) in India who complies with the cloud deployment guidelines published by GoI. Among these 18 CSPs, the following image illustrates that Amazon AWS, Microsoft Azure and Google holds the leaders' position of the Magic Quadrant for Cloud Infrastructure and Platform Services published by Gartner (2021), whereas Oracle cloud positions as niche player.

Figure 18: Gartner Magic Quadrant for Cloud Infrastructure

4.5. Maintenance of project documents:

The following documents are required to be maintained by DGCIS, which would help during the development stage of the project:

System Design Document

The System Design Document is a required document for each application. It should include a high-level design, provide what the system is intended for and must contain detailed descriptions of the architecture and system components.

Business Process Documents

The Business Process Document provides a sequence of the activities necessary to perform specific business services and is used to standardize procedures and establish best practices. Document should depict the functional flow of the process. In case of DGCIS, Process flow should include all recent notification changes.

Use Case Documents

The Use Case Document is a business document which provides a story of how a system, and its actors, will be utilized to achieve a specific goal. An effective Use Case should provide a detailed step-by-step description of how the system will be used by its actors to achieve the planned outcome.

Software requirement Specifications (SRS):

The SRS is a description of a software system to be developed. It lays out functional and non-functional requirements and may include a set of use cases that describe user interactions that the software must provide.

Hardware/Networking details

Proper documentation must be maintained with all the Hardware/Infra related/Site specific details. **Issue Logs.** Written issue log should be present to document all issues happened in pasts with reason/resolution properly recorded in it.

Security Policy

The Security Policy is a statement of the types and levels of security over information technology resources and capabilities that must be established and operated in order for those items to be considered as secure.

Disaster Recovery Plan

In worst case, a plan must be ready to keep business process running. It is generally required in cases when some natural calamity occurs.

5. Functional Architecture of the proposed solution

The purpose of the functional specification is to:

- Define the scope of business objectives, business functions and facilitate a common understanding of what the functional requirements are for all parties involved.
- Provide the business users with a documented end-to-end functional solution to the approved business requirements in a format that they can understand and sign off.
- Provide the technical delivery teams with a functional solution, which is of sufficient detail to enable development and implementation of the solution.

After studying all the processes currently being followed in DGCIS (AS-IS Study) and listing down the challenges being faced, this section provides the details for proposed system integrations and improved process in DGCIS.

The main activities of DGCIS are collection, compilation, validation, and dissemination of merchandise Foreign Trade data. The main functionality of the DGCIS system is to capture export-import data from all the ports across India, consolidate the data into a single database, clean and validate the data based on parameters, aggregate the data into groups and generate periodic reports of the export-import conducted by India on a regular basis.

This chapter elaborates the future functionalities that DGCIS system shall perform. Since the existing flow of the system is stable and efficient, during designing the to-be state of the DGCIS system, no major deviations have been considered in the existing flow. In the to-be situation more emphasize has been provided in automating the manual complex and time taking tasks with the help latest technologies and adopting various Artificial intelligence and machine learning principles. The following subsections suggest the changes required in the to- be system.

5.1. Data Ingestion Component

This Component will handle the input data to the online application. As illustrated in Section 2.1 earlier, the Foreign Trade data gets generated in customs locations and SEZs in the forms of Daily Trade Return (DTRs) from Bills of Entry (BE) for Imports and Shipping Bills (SB) for Exports submitted by the Importers and Exporters, respectively, in various customs offices and SEZs located all over India.

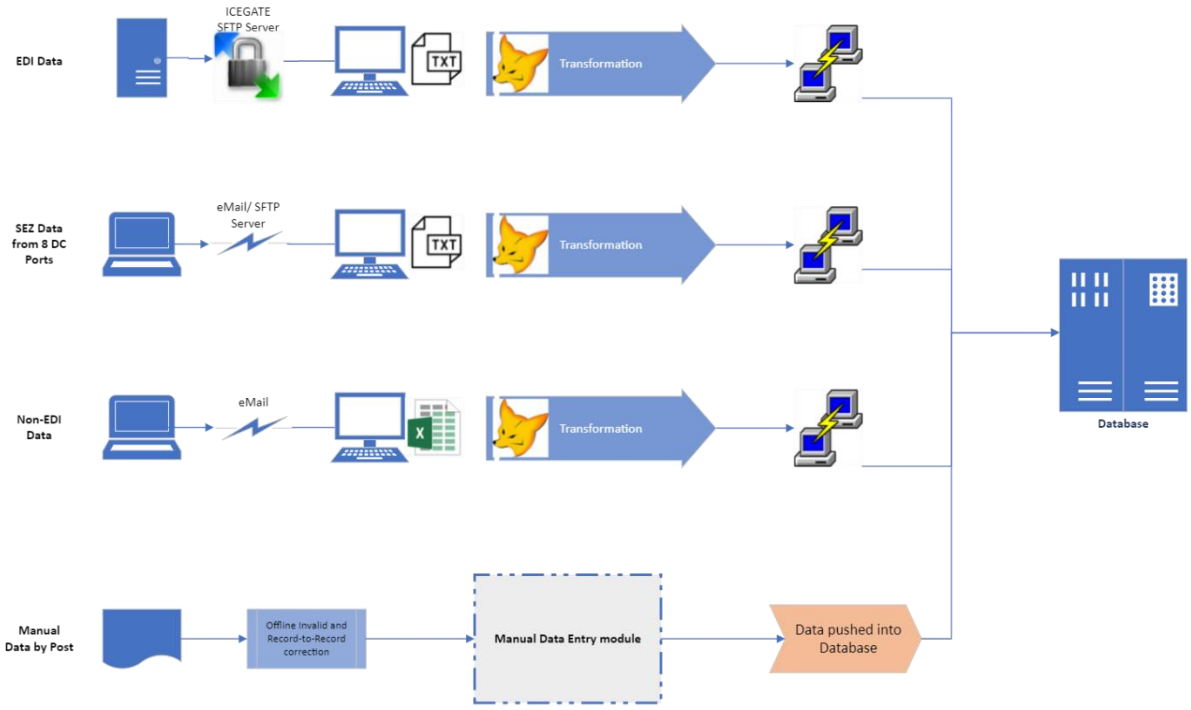


Figure 19: Data Ingestion at DGCIS

The Data Ingestion Component of the proposed Solution Application is expected to automate the above-mentioned cases as much as possible through the following 3 modules:

i. **Data sharing through API:** A webservice based functionality needs to be developed in the system to get the DTR data from the ICEGATE system though API. The API should be developed in the DGIS system, which can be consumed by any applications to share the DTR date with DGCIS. This would minimize the manual interventions of DGCIS and the data sharing agencies / organisations in future.

ii. **Data Download Scheduler** – In addition to the above functionality, there would be another functionality in the proposed system to share the data over SFTP, like it is being done in the current system. Additionally, this module, would schedule DTR data download from the hosted servers of ICEGATE and SEZ (NSDL) through SFTP at specified timelines and automatically perform the data transformations from the Flat files and populate the Database.

iii. **File Upload Module** – This Module would provide the facility to the users to upload the Non-EDI data received from the ports in the form of Excel files. The Module would perform similar data transformation from the excel files and populate the Database.

iv. **Manual Data Entry Module** – For the physical or Hard-copy DTR data received from Ports, a Manual Data Entry Module would be available for the user to input the Database fields manually.

5.2. AI-ML engine Component

The AI-ML engine component would be developed in the Solution which would be utilized to identify and correct the errors that are present in the database entries. The different cases of errors that have been identified and the possible AI-ML solutions have been explored in the subsequent section 6. The Historical transaction data and the correction data would be provided by DGCIS to develop the baseline suggestion/ correction algorithm. The component would also learn based on the corrections performed by users in the database entries.

5.3. Data Record ID (Sequence Number) Generation

After entry into the Database for all DTRs (export and import), a unique Sequence Number would be auto generated by the system and assigned to each entry in the Database. Each data entry sequence

ID should contain the financial year, date and month of the transaction (Shipping Bill date for export & Bill of Entry date for import).

5.4. Invalid Error Generation & Correction Component

After assignment of the Sequence number to each new entry, each of the entries would be checked by the AI-ML engine component for Invalid Country and Commodity codes (fields in the DTR entry) individually for Export and Import. The component will flag the data entry as an erroneous entry with a description flag defining the type of error flagged. The component will also generate a possible correction option and store the corrected data along with the original data for verification.

The user will have the option to auto-fill the AI-ML corrected data into the database or verify the correction made by the AI-ML engine and update the data manually, if required. This will also help the AI-ML component to learn and update the correction algorithm for future errors. The probable error correction possibilities are explained in the subsequent section.

5.5. Auto – Correction/ Conversion Component

For each commodity code, a standard measurement unit is defined, however, the input data may contain reported unit of quantity different than that of the Standard unit of measurement. In such cases, the system would automatically convert the unit using the mathematical formula from the reported unit of quantity to the standard unit of quantity.

5.6. Group Code Updation Component

All 8-digit Commodity Codes have been classified into 169 Brochure Groups. The commodity codes assigned to each Brochure Group is updated in the beginning of each Financial Year. Immediately after the Commodity Code errors have been corrected, Group Code will be automatically assigned to the transaction based on the Commodity code, corresponding to each entry in the database.

5.7. Record-to-Record (RR) Error Generation & Correction Component

The system would store the historical mean values for all commodity codes, which is calculated which is derived by dividing Export/ Import Value by the quantity in each transaction. For all Country Commodity combination, a Historical Mean value is available which are computed on the basis of unit values of historical transactions. The tolerances for each Country Commodity combination are also defined.

Upon running of the Record-to-Record check, the transactions where the unit values lie beyond the tolerance range would be selected for checking. These transactions would be individually checked by the AI-ML component. The AI-ML engine would generate a possible correction option for each erroneous entry and store the corrected data along with the original data for verification.

The user will have the option to auto-fill the AI-ML corrected data into the database or verify the correction made by the AI-ML engine and update the data manually if required. This will also help the AI-ML component to learn and update the correction algorithm for future errors.

5.8. Computation of Historical Mean Rates

The system should store the historical mean rate for each country-commodity combination in the database. The Historical Mean Rate is the mean of the unit values of transactions made in the past months for each country commodity combination.

The system would automatically run the historical mean rate calculation at the beginning of each month for each country commodity combination, to refresh the rates and keep the record up to date.

5.9. Group Dump System (Provisional Alpha) Error Correction Component

The system would allow users to view the Group-wise or Commodity-wise list of transactions for each month selected by the user. The Mean value of the selected transactions and the historical mean value for the country-commodity combination would also be displayed adjacently. In case the current rates are found to be outside tolerance level then each transaction of that country for the specific time period would be displayed in a separate window for verification and manual correction facility for the transactions would be made available.

5.10. Aggregation of Brochure-MSFT

After successful correction of the errors in the dataset, the user would have the option of generating month-wise, quarter-wise or annual data aggregation of the trade data. The user would also be able to generate individual commodity-wise reports, if required, for both Export and Import data.

The transactions corresponding to each of the following parameters would be aggregated and collated into reports for dissemination.

1. Brochure Code-wise Aggregation
2. MSFT-wise Aggregation
3. State-wise Export data Aggregation
4. Scheme-wise data Aggregation
5. Commodity-code wise Aggregation

5.11. Master Table creation and Maintenance

The following are the list of Master Tables that would be maintained at DGCIS and updated on a regular basis.

1. Country Code Master Table
2. Commodity Code Master Table
3. Port Code Master Table
4. Brochure Code Master Table
5. State/ Region Master Table
6. Scheme Master Table
7. Lot Master Table
8. Chapter Master Table
9. Unit History Master Table
10. Sensitive Commodity Master Table
11. Section Master Table
12. Dollar Master Table

6. Probable applications of AI-ML – Trade data validation and error rectification

DGCIS Systems continuously receive, store and process data related to the Trade data from ports concerning all the importers/ exporters across the country. Over a period of time, this data is gathered to provide a lot of statistics comprehension for useful analysis both for compliance as well as to prepare out the interesting patters and exceptions. It is desirable to make use of an appropriate Business Intelligence tool amalgamated with applications of Artificial Intelligence and Machine Learning to analyse and correlate the data and generate reports in various forms which would provide required inputs and enable the policy makers of the DGCIS to develop productive information which will definitely help in better functioning of DGCIS procedures.

6.1. Use Cases for AI/ML in DGCIS' Application

Following are the different AI-ML use-cases basis our initial analysis and discussion with stakeholders:

Case – 1: Blank / Incorrect Country Code

The Data sources for DGCIS' FTSS application are as following:

1. Electronic Data Interchange (EDI) through ICEGATE SFTP Server
2. SEZ Data through e-mail/SFTP server
3. Non-EDI Data through e-mail
4. Manual Data by post

Among the above-mentioned Data sources, the EDI and SEZ data (pts. 1 and 2 above) have pre-decided structures, templates in place and hence the fields are well defined. Thus, the error concerning Incorrect / Blank Country Code does not occur for these data sources. However, for non-EDI and manual data sources, such error may be encountered.

Following are different scenarios under the mentioned case:

a. In the following import data row, the highlighted cell for country code is blank:

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	UoM	Qty	Value	Currency	Rate	Description
1	08133000		Kgs	100	15000	AUD	150	Apple from Australia

Possible application of AI-ML: In the above example, through parsing and analysing the Description field's string or text into logical syntactic components, the AI-ML engine can suggest the COO to be **Australia** and corresponding Country Code can be recommended by the engine by mapping it to be Country Master Table, having the following Structure:

Country Master Table

Code	Country
001	**Afghanistan**
002	**Albania**
003	**Algeria**
004	**Andorra**
005	**Angola**

006	**Antigua and Barbuda**
007	**Argentina**
008	**Armenia**
009	**Australia**
010	**Austria**

Possible Recommendation: The following possible recommendation can be given as an output of the AI-ML engine.

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Recommendation from AI-ML engine	Unit of Measurement	Qty	Value	Currency	Rate	Description
1	08133000		009 (Australia)	Kgs	100	15000	AUD	150	Apple from Australia

If the User accepts the above recommendation, the COO field would be updated, and the AI-ML engine would be trained accordingly .

b. In the following import data row, the highlighted cell for country code is blank and the description contains misspelled Country description

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate	Description
1	11023447		Kgs	100	7000	EUR	70	Pineapple from **Armnia**

Possible application of AI-ML: In the above example, through parsing and analysing the Description field's string or text into logical syntactic components, the AI-ML engine would identify misspelled country name of **Armenia** and thus suggest the correct COO and corresponding Country Code can be recommended by the engine by mapping it to be Country Master Table.

Country Master Table

Code	Country
001	**Afghanistan**
002	**Albania**
003	**Algeria**
004	**Andorra**
005	**Angola**
006	**Antigua and Barbuda**
007	**Argentina**
008	**Armenia**
009	**Australia**
010	**Austria**

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Recommendation from AI-ML engine	Unit of Measurement	Qty	Value	Currency	Rate	Description
1	11023456		008 (Austria)	Kgs	100	7000	EUR	70	Pineapple from **Armnia**

If the User accepts the above recommendation, the COO field would be updated, and the AI-ML engine would be trained accordingly .

c. In the following import data row, the highlighted cell for country code is erroneous, that is, such country code does not exist the Country master table

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate	Description
1	08133000	**1509**	Kgs	100	15000	AUD	150	Apple from Australia

Possible application of AI-ML: In the above example, the AI-ML engine would look-up the COO Code in the country master table and once found unavailable, the engine through parsing and analysing the Description field's string or text into logical syntactic components, would suggest the correct COO - **Australia** and corresponding Country Code can be recommended by the engine by mapping it to be Country Master Table.

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Recommendation from AI-ML engine	Unit of Measurement	Qty	Value	Currency	Rate	Description
1	08133000	**1509**	009 (Australia)	Kgs	100	15000	AUD	150	Apple from Australia

If the User accepts the above recommendation, the COO field would be updated, and the AI-ML engine would be trained accordingly .

Case – 2: Blank / Incorrect Commodity Code

Following are different scenarios under the mentioned case:

a. In the following import data row, the highlighted cell for commodity code is blank:

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate	Description
1		009	Kgs	100	15000	AUD	150	Apple from Australia

Possible application of AI-ML: In the above example, through parsing and analysing the Description field's string or text into logical syntactic components, the AI-ML engine could suggest the Commodity to be **Apple** and corresponding ITCHS code can be recommended by the engine by mapping it to be Commodity Master Table.

Possible Recommendation: The following possible recommendation can be given as an output of the AI-ML engine.

S. No.	Commodity Code (ITCHS)	Recommendation from AI-ML engine	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate	Description
1		08133000 (Apple)	009	Kgs	100	15000	AUD	150	Apple from Australia

If the User accepts the above recommendation, the ITCHS field would be updated, and the AI-ML engine would be trained accordingly .

b. In the following import data row, the highlighted cell for commodity code is blank and the description contains misspelled Commodity description

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate	Description
1		009	Kgs	100	15000	AUD	150	**Aple** from Australia

Possible application of AI-ML: In the above example, through parsing and analysing the Description field's string or text into logical syntactic components, the AI-ML engine could suggest the Commodity to be **Apple** and corresponding ITCHS code can be recommended by the engine by mapping it to be Commodity Master Table.

Possible Recommendation: The following possible recommendation can be given as an output of the AI-ML engine.

S. No.	Commodity Code (ITCHS)	Recommendation from AI-ML engine	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate	Description
1		08133000 (Apple)	009	Kgs	100	15000	AUD	150	**Aple** from Australia

If the User accepts the above recommendation, the ITCHS field would be updated, and the AI-ML engine would be trained accordingly.

c. In the following import data row, the highlighted cell for Commodity code is erroneous, that is, such ITCHS code does not exist the Commodity (ITCHS) master table

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate	Description
1	**081335673**	009	Kgs	100	15000	AUD	150	Apple from Australia

Possible application of AI-ML: In the above example, the AI-ML engine would look-up the ITCHS Code in the Commodity master table and once found unavailable, the engine through parsing and

analysing the Description field's string or text into logical syntactic components, would suggest the correct Commodity –**08133000 (Apple)** and corresponding ITCHS Code can be recommended by the engine by mapping it to be Commodity Master Table.

S. No.	Commodity Code (ITCHS)	Recommendation from AI-ML engine	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate	Description
1	**081335673**	08133000 (Apple)	009	Kgs	100	15000	AUD	150	Apple from Australia

If the User accepts the above recommendation, the ITCHS field would be updated, and the AI-ML engine would be trained accordingly .

Case – 3: Deviation of Commodity Unit Rate beyond acceptable limits

At present, for a particular Country-Commodity combination, DGCIS records historic Commodity Unit Rate and stores such rates as Historic Mean Rates derived from at least ten such transactions for the particular Country-Commodity combination.

For a given trade record, if the unit rate falls beyond the acceptable limits (defined by 10% to 1000% of the Historic Mean Rate), then the quantity of the commodity is manually adjusted by DGCIS officials to bring the unit rate within the acceptable limit range.

In the following import data row, Rate (highlighted) is less than 10% of Historic Mean Rate for Import of Country-Commodity Combination and hence does not fall within the acceptable limits:

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate (Value /Qty)	Historic Mean Rate for Import of Country-Commodity Combination
1	08133000	009	Kgs	100	15000	AUD	150	1600 AUD/Kgs

Possible application of AI-ML: In the above example, the AI-ML engine would adjust the quantity of the commodity in such a manner that the unit rate falls within the acceptable range by considering several factors such as ITCHS Code, Gross weight etc. (10% to 1000% of the Historic Mean Rate)

Possible Recommendation: The following possible recommendation can be given as an output of the AI-ML engine.

S. No.	Commodity Code (ITCHS)	Country of Origin (COO)	Unit of Measurement	Qty	Value	Currency	Rate (Value /Qty)	Historic Mean Rate for Import of Country-Commodity Combination
1	08133000	009	Kgs	**75**	15000	AUD	**200**	1600 AUD/Kgs

If the User accepts the above recommendation, the Quantity field would be updated, and the AI-ML engine would be trained accordingly.

From the next such transaction onwards, the AI-ML engine would be trained towards modifying the quantity for that particular Country-Commodity Combination in similar manner.

The above-mentioned probable applications of AI-ML is summarized as following:

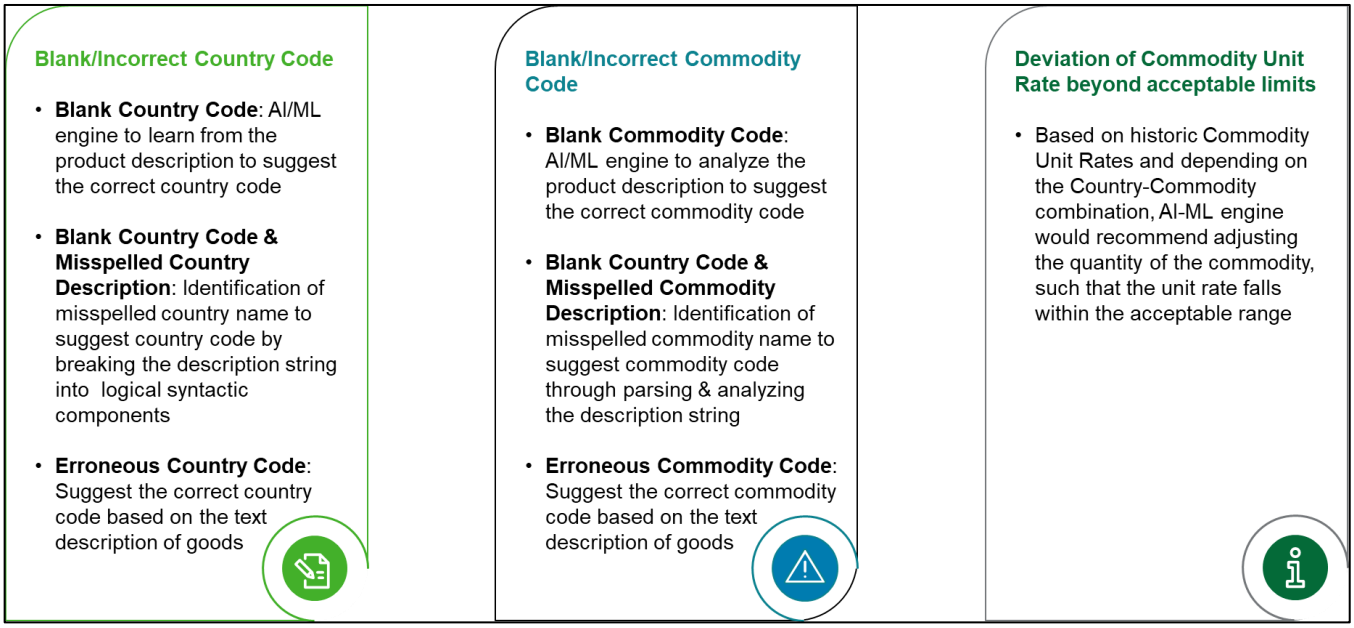


Figure 20: Probable applications of AI/ML

6.2. Probable applications of AI-ML

The above-mentioned scenarios are typical case of "data classification" based supervised learning. The target data are categorical data; i.e., there is only one correct answer (like country name, country code, HS Code). As per various case studies, we understand that various organizations have solved these problems by adopting the following ML principles. E.g.

- Decision tree
- Random Forest
- Support Vector Function

Following are different application scenarios of AI-ML basis our assessment:

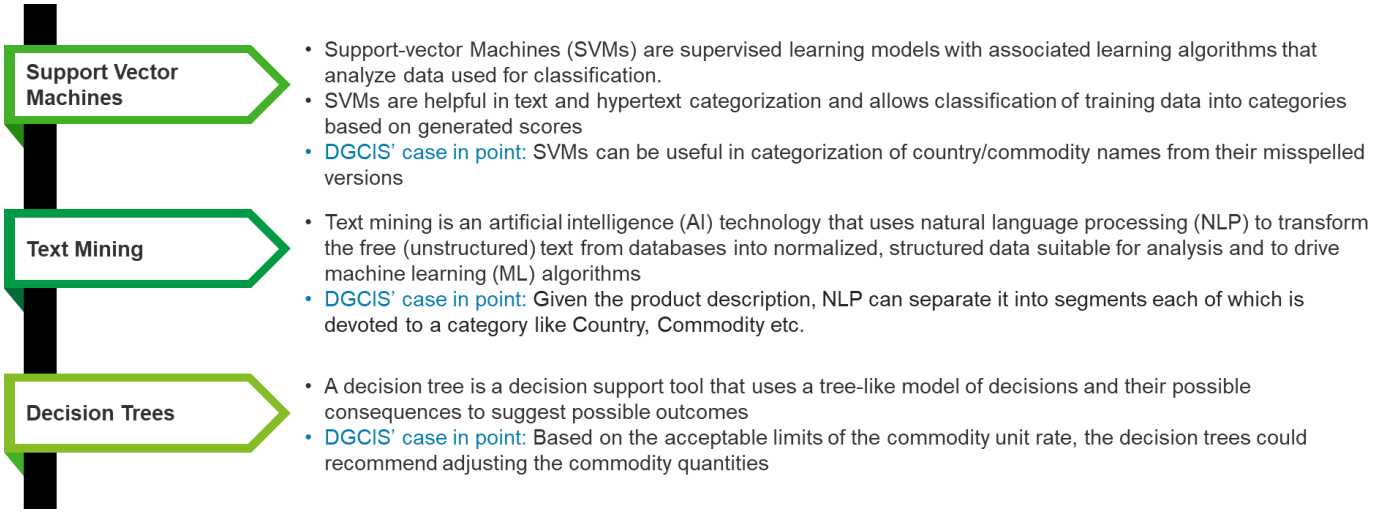


Figure 21: Application scenarios of AI-ML

Model try-out – As mentioned above, various models must be tried and tested with sample data to observe the level of accuracy and basis the initial assessment final model to be adopted

- **POC setup** – it is required to setup a POC to check the output of various models. The PoC can be done either by the vendor once they are onboarded or can be done by some government institutions (preferably IITs) on G2G basis.
- **Increase confidence level** - Initially we may get the confidence level of 60-65%, which can be increased to 90-95%
- **Hyper parameter tuning** – to be used to determine the parameters whose value control the learning process, e.g.
    - If the architecture is correct
    - What is the rate of learning
    - How many branches are required
- **Test and training data preparation** – Considering last 3 yrs. Data i.e., around 25 million transaction per year
    - 80% data would be used for training purpose
    - 20% data would be used for testing purpose

The above application of AI-ML solutions would help in reduction of manual interventions to rectify incorrect trade data received by DGCIS from different sources.

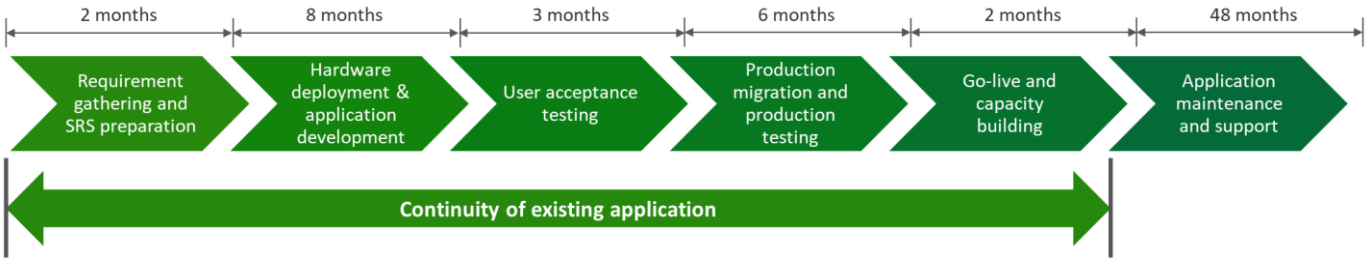
7. Implementation Roadmap

This section provides details about the timelines for project implementation and other functionalities associated for successful completion of the project. The transformation from current system to the redeveloped online system will require a lot of effort and involvement of employees across DGCIS. For this a phased approach is proposed for the project. In this model, the Roles & Responsibilities of all stakeholders will be fixed, and a joint effort from all of them will be required. It is highly recommended to do a parallel run of the application with sample data and this should be done 2 quarters continuously before actual go Live of the application.

Activities to be taken up during the Implementation Phase include:

- Preparation and submission of System Requirement Specification document (SRS)/ Fit Gap Document / Design Documents for Sign-Off
- Application Development/ customization, integration, and configuration of Core Components/ application Modules
- Infrastructure or Supply, Installation and Commissioning of Hardware / Devices
- Production Movement (including data migration)
- Application Software Testing
- User Acceptance Testing
- Hosting of application
- Training & Capacity Building of stakeholders on software application developed and new processes
- Deployment of the Application
- Handholding for the application deployed
- System operationalization and stabilization
- Solution and Application cum Maintenance Support

The Duration of Project Implementation is 18 Months and Operation and Maintenance Support for further 4 years post implementation.



The detailed breakdown for the Implementation Workplan is given in the figure below.

7.1. Indicative Implementation Workplan*

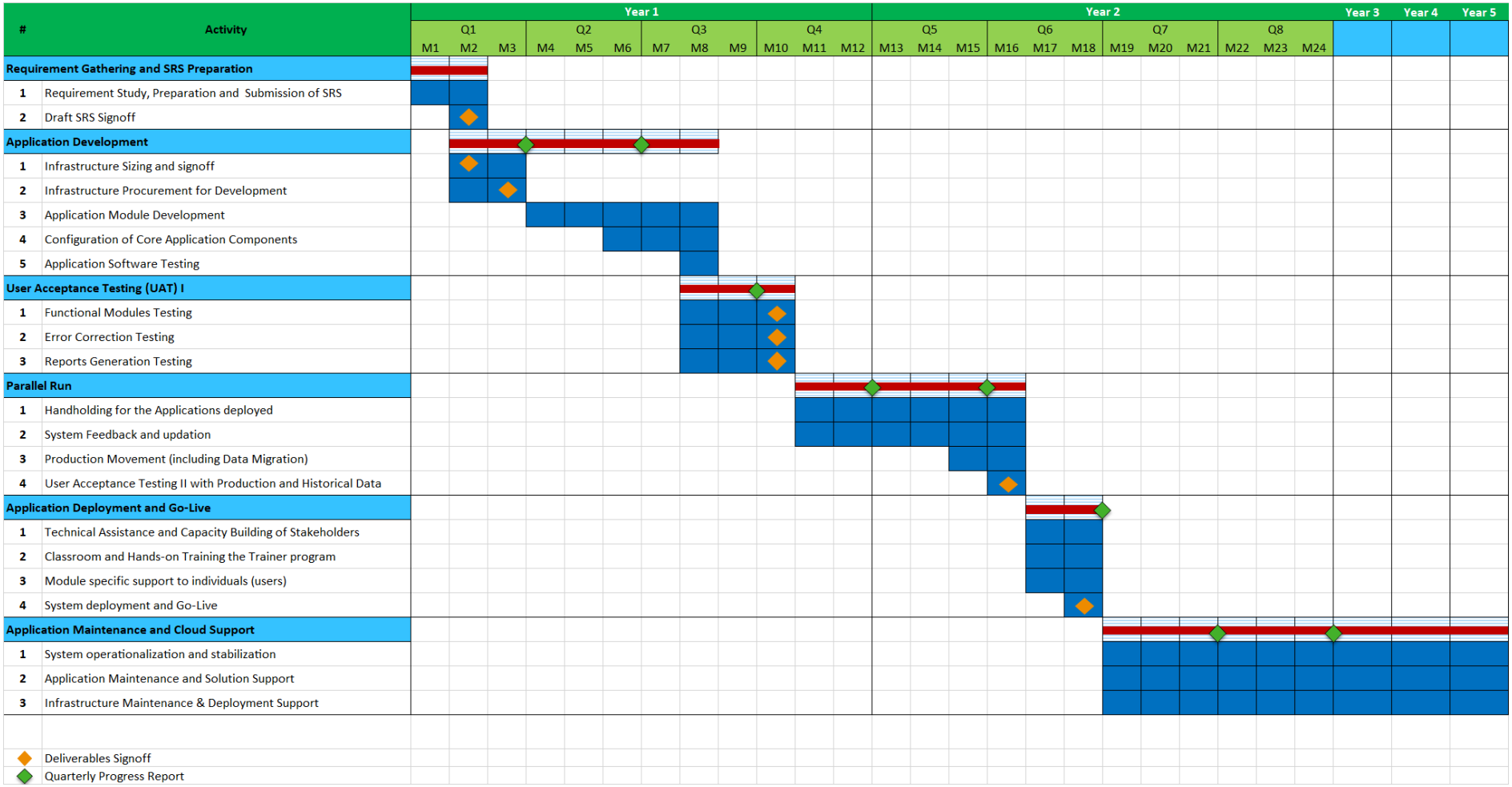


Figure 22: Implementation Workplan for DGCIS solution

* The timelines presented above are indicative in nature. The exact timelines would be dependent on the option / scenario to be selected during project implementation.

7.2. Training & Capacity Building

To improve the effectiveness of the capacity building and training exercises the DGCIS employees and staff should not be treated as a homogenous entity. Since the responsibilities of different working groups are varied, hence their roles with regards to risk assessment and corresponding mitigation processes would be different. Hence it is essential to form specific groups of employees based on their work-responsibilities, levels and roles.

The Stakeholders of DGCIS can be classified as follows:

- **Band A:** This band may comprise of officers based at the Ministry, DDGs, Directors and other Officers and all the people who are involved in various strategic level decisions
- **Band B:** This band may comprise of officers/ employees who would be responsible for system administration.
- **Band C:** This band may compromise of the staff and employees involved in the functional modules and operational work (Export division, Import Division, Data Dissemination Division, etc.)

The training requirements can be classified into 2 categories –

- **System Admin Training:** In order to understand the detailed technical architecture of the system, the users would have to undergo a thorough training. This training would also cover aspects on database, application and infrastructure administration.
- **End User Training:** This training would be targeted towards the end users to equip them with understanding of using the applications on a day-to-day basis.

Indicative Training Modules

The training would consist of an initial orientation workshop, to generate awareness about the project and acquaint the staff at DGCIS with the new changes with implementation of IT project. It would also address the participants with a formal introduction to the project and address their concerns/ doubts regarding the new system.
Subsequent to the orientation workshop, the following training matrix could be implemented.

	Training Modules	Bands	Remarks
System Admin Training			
1.	System Admin Training	Selected personnel depending on their responsibilities	Special training to be provided to selected persons on the management of the applications and infrastructure
End User Training			
2.	Awareness Workshop	Selected personnel depending on their responsibilities	The training would be provided from management perspective specifically highlighting the top management reporting (like dashboard, MIS reporting).
3.	Application Training	Selected personnel depending on	Module specific training would be provided to the target audience who are involved in that particular function/process.

	Training Modules	Bands	Remarks
		their responsibilities	
4.	Handholding to DGCIS Users	Selected personnel depending on their responsibilities	Handholding Officers to support user community for a period of 2 Quarters post go-live.

Training Facility

Training facility would include the infrastructure required for conducting the training. Typically training facility would include location/space for training, projector and laptop/ desktop for each participant which would be used during the training. The training facility would be provided by DGCIS. The training documentation and end user manual would be provided by System Implementer.

Training Effectiveness

Training effectiveness would be measured using feedback mechanism. For that, questionnaire would be designed accordingly by System Implementer. The questionnaire would be handed over to the participants after the training and they would rate the training effectiveness in a scale of 1-5 (1 being best). The effectiveness of the training would be measured by average scoring against each effectiveness parameters. In case the average score of the training falls below 3, then the training would be considered as in-effective and hence re-training has to be arranged by System Implementer.

7.3. Governance Framework

The Governance Structure for DGCIS would be a three-layered structure as illustrated in the figure below. The first layer would consist of Steering Committee, second layer would be of Project implementation and the third a Program Management Unit (PMU), to manage the project. Details of the functions performed by the layers are provided below:

7.3.1 Steering Committee

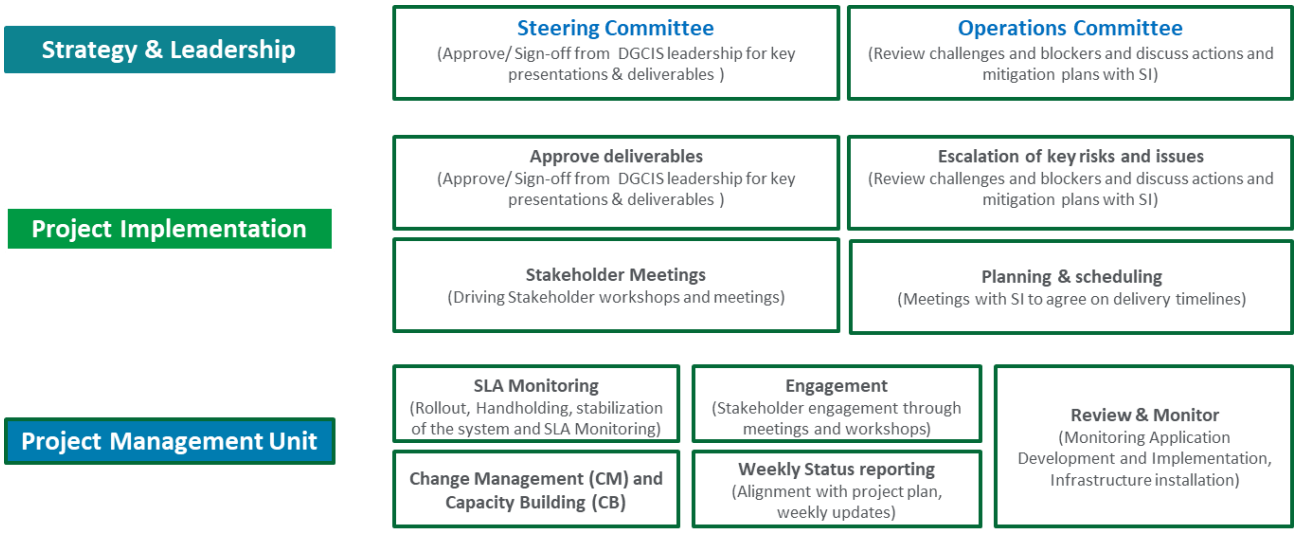


Figure 23: Governance Structure for DGCIS

A Steering Committee comprising of key officials from DGCIS and NIC shall be setup to provide strategic direction and to address policy level issues. It is proposed to setup a dedicated steering committee for the project for implementation phase. Steering Committee comprising of senior officials from DGCIS and NIC will be responsible for the following functions:

- Provide strategic direction and guidance
- Decide on policy level issues that need to be addressed from time to time
- Be the final authority for approving all the deliverables

7.3.2 Operations Committee

An Operations Committee comprising of key officials from DGCIS shall be placed to provide operational level guidance, facilitate coordination between all stakeholders and monitoring of project progress. It is proposed to formulate a dedicated committee for implementation phase. The committee should meet at least once in week for smooth operations.

Keeping in view the significant role, it is proposed to include senior officials of rank at least Joint Director (DGCIS) in operations committee for better coordination with all stakeholders.

These officers will ensure the smooth progress of the project and to that extent will provide relevant support. Project teams comprising of employees from all levels to ensure greater participation, ownership and accountability will also be set up.

Key functions of the operations committee would include:

- Review the progress of development and implementation
- Provide technical and functional support to the implementation teams at a strategic level
- Facilitate state in the implementation of the projects
- Operational review with the Programme Management Unit

7.3.3 Programme Management Unit (PMU)

Considering the criticality of the project, it is required to setup a Project Management Unit (PMU) to monitor the activities performed by the system integrator for the entire duration of the project in order to ensure the envisaged output is obtained.

PMU would be involved in day-to-day monitoring and evaluation of the project. The PMU would comprise of people with different skillsets at build and steer phase.

During RFP and Bid Process Management phase, the focus will be on procurement, technology selection, vendor selection, contracting, so experts in these areas would be required. During the development and Implementation phase, focus shifts to project management, monitoring and evaluation, protocol, and standards management, so experts in these areas would be required. The people required for PMU are Project Manager, Monitoring & Evaluation Expert, Application Expert, Database Expert, IT Infrastructure Expert, , Financial cum Procurement Expert and Documentation experts.

The purpose of this PMU is to:

- Monitor Application Development and Implementation, Infrastructure installation
- Support DGCIS in monitoring the data migration/ digitization work progress and quality compliance
- Rollout, Handholding, stabilization of the system and SLA Monitoring
- Prepare change request management framework for DGCIS Solution; establish change control procedure for carrying out version changes in software application; review and approve patches / upgrades identified by the IA in software applications
- Implement change Management (CM) and capacity building (CB) of DGCIS staff
- Resolve issues with contract management, billing / invoicing and other financial matters
- Set out the procedure for escalating disagreements; and resolving issues escalated in accordance with the escalation procedures as agreed with the System Implementer

- Enable administration and performance management; preparation of all necessary documentation for obtaining approvals and submitting reports to higher authorities
- Define the principles that both Parties wish to follow to ensure the delivery of the Services; ensure the continued alignment of the interests of the Parties;
- Risk identification and subsequent mitigation along with all kinds of issue resolution related to the project

7.3.4 Project Management Requirements

An effective Project Management Plan and commitment to adhere to it is one of the critical success factors to project success. The project plan should include the resource, task, and time plan for the entire duration of the project.
System Implementer would be required to deploy a full time Project Manager for the entire duration of project and a dedicated project team to deliver the project. The project manager shall act as the single point of contact for DGCIS. The System Implementer is required to propose a project team for Implementation as well as Operations & Maintenance phase of the DGCIS System.

The System Implementer would be required to provide periodic reports on the project progress. The formats of the reports would be finalized after commencement of the project. System Implementer would provide ad-hoc report as per need basis. The Project Manager would also be responsible for escalating all issues in a timely manner.

An indicative list of documents required is provided below:

Plan	Frequency
<u>Project Management</u> • Project Organization and Management Plan • System Development Plan with milestones and timelines • Delivery and Installation Plan • Testing Plan and Methodology • Training Plan, Methodology and Training Details • Change Management Plan • Data Migration Plan • Data Digitization Strategy • Any other relevant items related to the DGCIS System Implementation	
<u>Project Monitoring</u> Update on progress – This report should provide the following details: • Tasks completed during the week • Project progress vis-à-vis planned • Cumulative deviations to date from schedule of progress on milestones as specified in the agreed and finalized Project Plan • Pending actions items from previous reporting period • Forecast for the next reporting period • Risk Reporting and Mitigation steps • Corrective actions to be taken to return to planned schedule of progress if any • Proposed revisions to planned schedule • Interventions which the System Implementer expects to be made by the PMU • Other issues and outstanding problems, and actions proposed to be taken • Test results of training • Any other report requested by DGCIS	• Weekly / Monthly / Quarterly status report • As per need basis • The System Implementer provide all the reports requested by DGCIS to assist in Project Monitoring

7.4. Risk Management Plan

Risk is an important element of any project. Risk refers to the uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organization's objectives. Risk management reduces adverse risks by reducing the likelihood of the risk or its effects. It provides an estimate of the magnitude of the unexpected outcomes (the surprise factor) on the project. A project management methodology is not complete without a forward-looking risk management component. This aspect of Project Management runs through all the phases of the Project implementation. All processes are monitored continuously for adherence to quality and any risks or deviations are immediately attended to and rectified. Some of the main objectives of this aspect of project management are:

- Identification of high, medium, and low risk areas and pain points

- Identification of Risk Mitigation Methods and implementation plans
- Tracking, monitoring, and reporting risks to previously defined authorities
- Implementation of alternate strategies at appropriate times
- Observance of all Quality aspects including documentation, process control and strict adherence to Service Level Agreements (SLAs)

Risk management is a continuous activity which integrates recognition of risk, risk assessment, developing strategies to manage it, and mitigation of risk using managerial resources. This exercise involves interaction and exchange of information among various agencies on regular basis. This is an ambitious agenda and requires diligent execution of a milestone-based, phased plan. Role played by each stakeholder is very important to make the project successful. A comprehensive analysis of functions of all the stakeholders reveals that project may face problems if responsibilities given to the stakeholders are not carried out by them. Although, risks are inevitable part of any project, proper risk management strategy helps in minimizing or eliminating the impact of risks on projects.

7.4.1 Risk Assessment

Risk assessment consists of an objective evaluation of risk in which assumptions and uncertainties are clearly considered and presented. There needs to be a periodic review of the prevailing project risks .

Risk assessment is a continuous process, and the Project Management Unit would be primarily responsible to carry out the same. The other stakeholders (Steering Committee, Operations Committee or any other empowered committee) as mentioned in the previous section would also support in periodic review of project risks and evaluate them basis the priority.

The following indicative format may be used to capture project risks and specify the responsibility, duration and completion of the same.

Risk Assessment Matrix

S. No.	Risk Scenario	Impact on Duration	Impact on Cost	Corrective Action	Responsibility	Completion Date	Status
1.							
2.							

Owing to the nature of the project and the far-reaching consequences that it has in functioning, risks associated with delays and those relating to change management issues are envisaged. As part of risk mitigation strategy, periodic reviews with project manager/ DGCIS officer for the project will be conducted.

7.4.2 Risk Mitigation Strategy

Risk Mitigation is the solution of risks using available technological, human, and organizational resources. This section details out the anticipated risks that may arise during the course of project implementation. Predictable impacts and mitigation strategy for some of these risks is listed below (Risks and Mitigation strategy may vary upon actual implementation strategy).

Risk Mitigation Strategy

S. No.	Risk	Impact	Mitigation Strategy
1.	Pre-mature exit of vendor	• Delay in project Implementation • Exit without knowledge transfer to the department • Resource deployment for finalization of replacement vendor	Vendor shall be asked to submit an Exit Management Plan (before a defined tenure from the date of contract signing with the DGCIS. DGCIS and vendor would then collectively finalize the process) with following details: a. Well Defined Transfer Process: A detailed transfer process that could be used in conjunction with a replacement vendor, including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure during the transfer. b. Communication plan: Modalities for communication with the vendor and any related third party as are necessary to avoid any detrimental impact on the project's operations as a result of the transfer. c. Plan for contingent support: Selected vendor shall be asked to submit plans for provision of contingent support to the project and replacement vendor for a reasonable period, agreed by department, after the transfer. d. Penalty: DGCIS shall include adequate penalty clauses in the exit management plan.
2.	Below par / non-performance of vendor	• Effect on the outcome of the project along with participation of other stakeholders in the project	DGCIS shall use performance evaluation framework to evaluate the performance of the vendor and it would provide regular feedback to the vendor. Also, DGCIS shall include clauses to empower it to terminate the agreement on non-performance, nonmeeting of Service Level Agreement (SLA) or non-completion of agreed activities with agreed quality and time.
3.	Resistance from employees	• Problems such as non-performance, delay in work etc.	Proper change management strategy shall be adopted.
4.	Transfer of key officials	• Adverse Effect on the progress of project	Key members and other champions should not be transferred as frequently. Knowledge transfer exercise should be undertaken after appointing a new nodal official.

S. No.	Risk	Impact	Mitigation Strategy
5.	Integration issues with different agencies	• Delay in the data or Data in incorrect format will delay testing.	Proper plan to be designed well in advance so that third party system can be integrated properly ensuring the smooth flow of data.
6.	Co-operation issues with external agencies	• In case of improper response, or delay in response from other agencies, DGCIS's processes will get delayed and, hence impacting Users.	a. Representatives from important agencies to be made members of Steering / Operating Committee b. DGCIS to conduct workshops or meetings with agencies to demonstrate the expected benefits of the project to them c. DGCIS to bring a government order instructing the timely generation and updation of data is required for the successful execution of project.
7.	Issues related to Infrastructure	• Infra structure issues can shut down the application	Archival of overall data shall be scheduled as per plan. Concerned team shall regularly monitor the space/bandwidth parameters to ensure the smooth functioning of application. Team assigned shall also provide their feedback to modify/change any system, which can help afterwards.

Annexure

.

A. High Level Application Architecture

The proposed system shall be developed in Open Technology and shall support n-Tier with Service Oriented Architecture (SOA) to make the system more flexible, easily composed and highly reusable. The proposed technology components will be loosely coupled, web services enabled for functional requirements of the DGCIS. DGCIS functions are defined as a group of services that communicate with each other through either simple data-passing or two or more services coordinating some activity.

Rich Internet Application shall be set up at DGCIS Headquarter, wherein data and information would be collected, stored, retrieved, used, and exchanged in an efficient manner at all levels. The services to be delivered would require automated workflow, document management, alerts and notifications for various actions/activities performed in the system.

The Logical Architecture of the DGCIS application provides clear demarcation of various layers and logical components of the proposed system. The key idea is to provide basis for realizing the system based on "Service Oriented Architecture". This is essentially a collection of services that are well defined, self-contained, and loosely coupled with other services. Providing this type of architecture entails separating out common activities, tasks, and business events into common services, which could then support and be utilized by all participants required to compose the business process. Shown below is the High-level Application Architecture of the DGCIS Application:

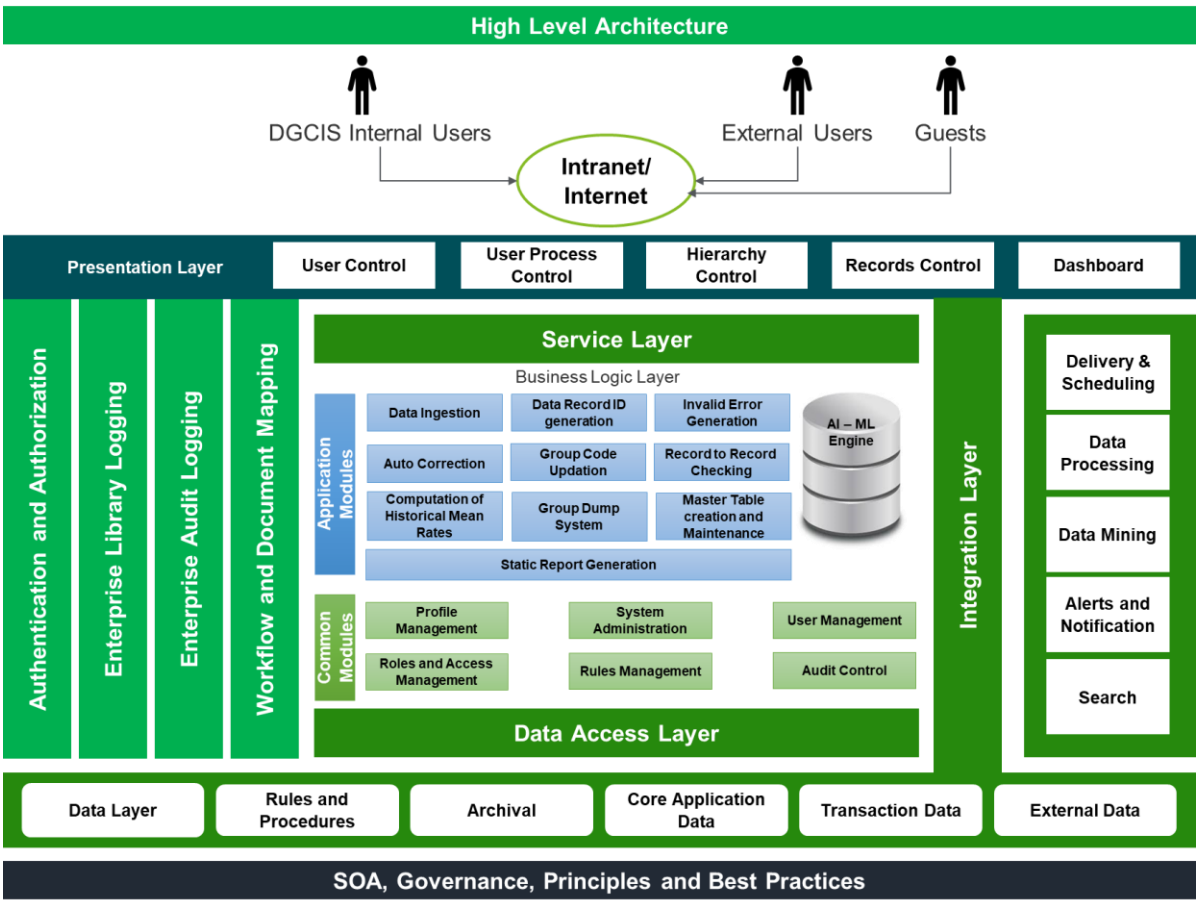


Figure 24: High Level Application Architecture at DGCIS

The solution architecture comprises of mainly seven parts as described below:

S. No	Component	Description
1	**Client Layer**	Client layer would contain web browser for external as well as DGCIS internal users. External users use internet to send request to access the services and internal users would connect via LAN (Intranet) or Internet gateway.
2	**Presentation Layer**	The presentation layer interoperates with the business and data access layers through service layer to form the overall solution. Bootstrap controls may be used for rich, functional, and well-performing user interfaces.
3	**Service Layer**	The Service Layer receives messages from the Presentation Layer. It interprets the message, unpacks the Data Transfer Objects, and organizes and coordinates the interaction between Presentation Layer and Business Layer. In the application, the Service layer exposes the functionalities of various modules to the Presentation layer and to other external applications.
4	**Business Logic Layer**	The business logic is hosted in this layer and the application logic shall be encapsulated as Business Objects in Business Logic Layer (BLL). Business Objects can further be exposed with a layer of Web Services to provide true seamless electronic integration. This layer interacts with Data Access Layer to send/retrieve data from database.
5	**Integration Layer**	This layer can automate complex business processes and provide access to information available with other systems. This integration layer is subset of business logic layer.
6	**Data Access Layer**	This layer is responsible for actually communicating with the Enterprise Database below. It abstracts the kind of database that is in use and provides for consistent view of the data to layers above it. The objective of the DAL is to provide data to business layer. It can be accomplished by exposing a series of data access methods from the DAL that operate on data in the data-tier using database specific code but do not expose any database specific method parameters or return types to the business layer. Any time a business object needs to access the data tier, it can call a method in the DAL instead of calling directly down to the data tier. This pushes database-specific code into the DAL and makes Business Layer of application independent of database.
7	**Database Layer**	All data shall reside on the Data Access layer. User profile, content repository, Metadata and mail messaging data shall also reside on the Database Layer.

Based on this logical layering, several advantages are realized:

- The implementation logic of the business services can be changed without making any changes to the other layers
- Database-specific implementation details are hidden to the Web UI Layer and the Services Layer. Hence, additional data access assemblies can easily be added to communicate with other types of databases. This can be done without making any changes to the Web/UI layer or the Business Services Layer
- Services can be co-located or remotely invoked by the Web layer; enabling more flexible deployment options. For example, The Web servers do not need to have any database connectivity or access, since they only invoke methods in the Business Services Layer
- Different programmers can more easily work as team, each focusing on a specific layer

Each logical layer of the architecture is described briefly in the next sections.

A.1 Presentation Layer

The presentation layer includes the following types of software components that perform specific tasks:

- **User Interface Components:** These components make up the user interface of the application. Users see and interact with these components. User interface components display data to users, acquire and validate data from user input, and interpret user actions that indicate the user wants to perform an operation on the data.
- **User Interface Process Components:** These components organize the user interface elements and control user interaction. Users do not see user interface process components; however, these components perform a vital supportive role to user interface components.

The combination of these two types of components forms the presentation layer of the application. The presentation layer interoperates with the business and data access layers to form the overall solution.

Considering the latest trend, Rich Internet application can be implemented to design the Presentation Layer of proposed solution:

Rich Internet Applications (RIAs) are web applications that offer the responsiveness, rich features and functionality approaching that of desktop applications. Early Internet applications supported only a basic HTML graphical user interface (GUI). RIAs are a result of advanced technologies that allow greater responsiveness and advanced GUIs.

A.2 Services Layer

The Service Layer receives messages from the Presentation Layer. It interprets the message, unpacks the Data Transfer Objects, and organizes and coordinates the interaction between Presentation Layer and Business Layer. In the DGCIS System, the Service layer exposes the functionalities of various modules to the Presentation layer and to other external applications. Web services shall be used to communicate messages between Business layer and Presentation layer.

A.3 Business Logic Layer

The business logic is hosted in this layer and the application logic shall be encapsulated as Business Objects in Business Logic Layer (BLL). Business Objects can further be exposed with a layer of Web Services to provide true seamless electronic integration. This layer interacts with Data Access Layer to send/retrieve data from database.

i. This layer handles all business rules for the application.

ii. The BLL calls the appropriate data access layer method and supply the inputs provided by business service

iii. The BLL is responsible for returns value from the DAL and process the values to pass to business service.

This layer implements business logic of all modules of DGCIS System. It is important to maintain the major business logic in this layer to avoid the complex stored procedure. This will also ensure easy maintenance of business logic component and stored procedures.

A.4 Integration Layer

This layer shall automate complex business processes and provide unified access to information like shipping bill details, Bill of entry, scheme details, Business details etc. that are currently scattered across many systems. This integration layer is subset of business logic layer.

The purpose of integration layer is providing a gateway to interface with external application. DGCIS system and other external systems shall communicate with each other using Web Services. DGCIS data shall be maintained at Central level and send this data to all external systems through XML files using predefined web services. This transmission shall be triggered on user request or predefined interval.

A.5 Data Access Layer (DAL)

This layer is responsible for actually communicating with the Enterprise Database below. It abstracts the kind of database that is in use and provides for consistent view of the data to layers above it. The objective of the DAL is to provide data to business layer. It can be accomplished by exposing a series of data access methods from the DAL that operate on data in the data-tier using database specific code but do not expose any database specific method parameters or return types to the business layer. Any time a business object needs to access the data tier, it can call a method in the DAL instead of calling directly down to the data tier. This pushes database-specific code into the DAL and makes Business Layer of DGCIS System independent of database.

Following are the key advantages of using data access components:

iv. It will minimize the impact of a change in database provider

v. It will minimize the impact of a change in data representation

vi. It will encapsulate all code that manipulates a particular data item in one place. This will greatly simplify testing and maintenance

Following operations will be performed by Data Access Layer:

vii. The DAL is responsible for maintaining transaction, while inserting, deleting, and updating data

viii. The DAL access database via stored procedure or statements depending on the logic provided

ix. The DAL is responsible for maintaining connections and connection pooling. It uses configuration files to read the connection information.

A.6 Cross-Cutting Layer (Security, Exception Handling & Logging)

The basic concepts of security are Authentication, Authorization, Impersonation and Data or functional security. Authentication is the process that enables to identify a user, so that only that user is provided access to the resources. Authorization is the process that enables to determine whether a particular user can be given access to the resources that the user requests. Impersonation is the process that provides access to resources requested by a user under a different identity. Following cross cutting functions are explained below:

Authentication

Authentication enables to restrict a user to access the resources by certain ways. It could be a combination of a username and Digital Signature / Password. The validity of the information provided by the user helps identify the user, so that the user is provided access to the requested resources. The process of successful identification of the user implies that the user is authenticated.

DGCIS system authenticate the user by use of Active Directory/ LDAP, which shall be continued for access to the system. LDAP is used for Internet Access whereas Active Directory is utilized for System or Application access.

Authorization

The process of determining the access to the resources for a particular user is known as Authorization. DGCIS system shall implement the Role based authorization of application resources.

Audit Trail

Objective of audit trail is to obtain sufficient evidence material regarding the reliability and integrity of the application system. To achieve this, the audit trail should contain enough information to allow management, the auditor, and the user:

x. To recreate processing action;

xi. To verify summary totals and

xii. To trace the sources of intentional and unintentional errors.

Exception Handling & Logging

The function of the Exception Handler is to trap the error information and perform the defined operational steps based on the error. The corrective action to be performed may be configured for each type of error and may vary based on the severity of the error.

Reporting Services

The DGCIS system shall provide a report generator to enable timely, regular, and ad-hoc user defined reporting. Following facilities shall be available in the new DGCIS system

xiii. Allow ad-hoc queries or reports to be run by individual users through simple selection and sort functions and displayed on screen, printed, or exported.

xiv. Enable interactive hierarchical relationships (drill-down)

xv. No limit on the number of concurrent users.

xvi. Support multiple languages

xvii. Export data to Excel, Word, CSV, PDF,RTF, HTML, comma/column delimited file

xviii. Facility to email the reports

xix. Reports can be created, managed, and published through web

xx. Can store a list of pre-compiled complex queries

xxi. Capable to render data in Graphics, charts, tables etc.

xxii. Images can be added in background

xxiii. Allow automatic generation and storing, printing, or exporting of selected reports at scheduled dates and times. Example: as part of the end-of-day run or either a daily, weekly, monthly, or quarterly basis.

xxiv. Allow batch reports and to run outside business hours.

xxv. Allow to create report in XML or Excel format.

xxvi. Good performance for users (including the remote users) when generating reports

xxvii. End users have ability to do slice & dice and perform more detailed analysis

DGCIS system would have the provision of two types of reports:
Static Reports: These are generic reports available in predefined formats and design & layout of these reports will not be modified by the application user. Report designer tool shall be used to design these reports in predefined format and same shall be released as a report module.

Ad-hoc Reports: An ad hoc report is created by sending a request or query through the reporting tool to get the specific information in tabular format. Application shall allow user to create a dynamic report by selecting columns & filter criteria and drag them into the canvas in a specific order. Filter criteria and column arrangements of these reports shall be saved for the future reference.