KPMG

cutting through complexity™

IT Strategy Report

Office of Controller General of Accounts

June 2013

Disclaimer and Notice to Reader

This report has been prepared by KPMG ("KPMG" or "We") for National Informatics Centre (NIC) and Controller General of Accounts (CGA) ("National Informatics Centre (NIC)" or "Controller General of Accounts (CGA)" or "You" or "the Client") for the purpose set out in our Work Order with NIC dated November 03, 2011 only and it shall not be copied, circulated, referred to or disclosed, in whole or in part (save for NIC's/CGA's own internal purposes), without our prior written consent. Our reports and comments are confidential in nature and are not intended for general circulation or publication, nor are they to be quoted or referred to be in whole or part, without our prior consent in each specific instance.

This report sets forth our views based on the completeness and accuracy of the facts stated and any assumptions that were included. If any of the facts and assumptions is not complete or accurate, it is imperative that we be informed accordingly, as the inaccuracy or incompleteness thereof could have a material effect on our conclusions.

We have not performed an audit and do not express an opinion or any other form of assurance. Further, comments in our report are not intended, nor should they be interpreted to be legal advice or opinion.
Our views are not binding on any person, entity, authority or Court, and hence, no assurance is given that a position contrary to the opinions expressed herein will not be asserted by any person, entity, authority and/or sustained by an appellate authority or a court of law.

The documentation review was limited to the records/documents produced before KPMG by the staff of the NIC/CGA. Neither KPMG nor any of its partners, directors or employees undertake responsibility in any way whatsoever to any person in respect of errors in this report, arising from incorrect information provided by the NIC/CGA staff. While performing the work, we assumed the genuineness of all signatures and the authenticity of all documents. We have not independently verified the correctness or authenticity of the same.

In performing this engagement and preparing this report, KPMG assumes no responsibility for the accuracy and completeness of the information provided by external sources of information and will not be held liable for it under any circumstances. While information obtained from the public domain has not been verified for authenticity, we have obtained information, as far as possible, from sources generally considered to be reliable.

Our report may make reference to 'KPMG Analysis'; this indicates only that we have (where specified) undertaken certain analytical activities on the underlying data to arrive at the information presented; we do not accept responsibility for the underlying data.

We must emphasize that the realization of the prospective financial information set out within our report (based on secondary sources, as well as our internal analysis), is dependent on the continuing validity of the assumptions on which they are based. The assumptions will need to be reviewed and revised to reflect such changes in business trends, cost structures or the direction of the business as further clarity emerges.

In connection with our report or any part thereof, KPMG does not owe duty of care (whether in contract or in tort or under statute or otherwise) to any person or party to whom the report is circulated to and KPMG shall not be liable to any party who uses or relies on this report. KPMG thus disclaims all responsibility or liability for any costs, damages, losses, liabilities, expenses incurred by such third party arising out of or in connection with the report or any part thereof.

By reading our report the reader of the report shall be deemed to have accepted the terms mentioned hereinabove.

Glossary

ACID - Accounts Informatics Division

CA - Controller of Accounts

CBDT - Central Board of Direct Taxes

CBEC - Central Board of Excise and Customs

CBS - Core Banking System

CCA - Chief Controller of Accounts

CFMS - Challan File Movement System

CGA - Controller General of Accounts

COTS - Commercially off the shelf

CPAO - Central Pension Accounts Office

CPSMS - Central Plan Scheme Monitoring System

CPWD - Central Public Works Department

DDG - Detailed Demand for Grants

DDO - Drawing and Disbursing officer

DG - Demand for Grants

DMS - Date wise Monthly Statements

DSN - Data/ Database Source Name

FA - Financial Advisor

FQ-TQ - Functional Quality- Technical Quality

GePG - Government electronic Payment Gateway

ICAS - Indian Civil Accounts Service

ICT - Information Communication Technology

IFD - Integrated Finance Division

INGAF - Institute of government accounts and finance

ITD - Information Technology Division

NCDDO - Non Cheque issuing DDO

NIC - National Informatics Centre

NPS - New Pension Scheme

NSDL - National Securities Depositories Limited

ODBC - Open Database Connectivity

PARAS - Pension Authorization Retrieval Accounting System

PPO - Pension Payment Order

Pr. CCA - Principal Chief Controller of Accounts

Pr.AO - Principal Accounts Office

RBI CAS - Reserve Bank of India, Central Accounts Section

SDLC - System Development Life Cycle

SRS - System Requirement Specifications

SSA - Special Seal Authority

STQC - Standardization Testing and Quality Certification

UAT - User Acceptance Testing

Contents

1 Executive Summary

KPMG had conducted a current state assessment of the existing IT applications and presented the findings of the same in the Assessment Report. During the assessment phase an FQ-TQ analysis was also conducted which yielded that that the applications COMPACT; COMPDDO; Market Loan package; and State Loan package needed to be retired or replaced. The applications e-Samarth; e-Lekha; COMPACT (REVACT); COMPACT (RAMS); and PARAS needed to be technically enhanced.

The changes in the business environment have brought about change in the stakeholder expectations from the IT Systems deployed at the CGA's organisation. The changing stakeholder needs have been captured in detail during the one-on-one interactions conducted during the assessment phase. The stakeholders need point towards and integrated financial information system that helps them in discharging their duties effectively and efficiently.

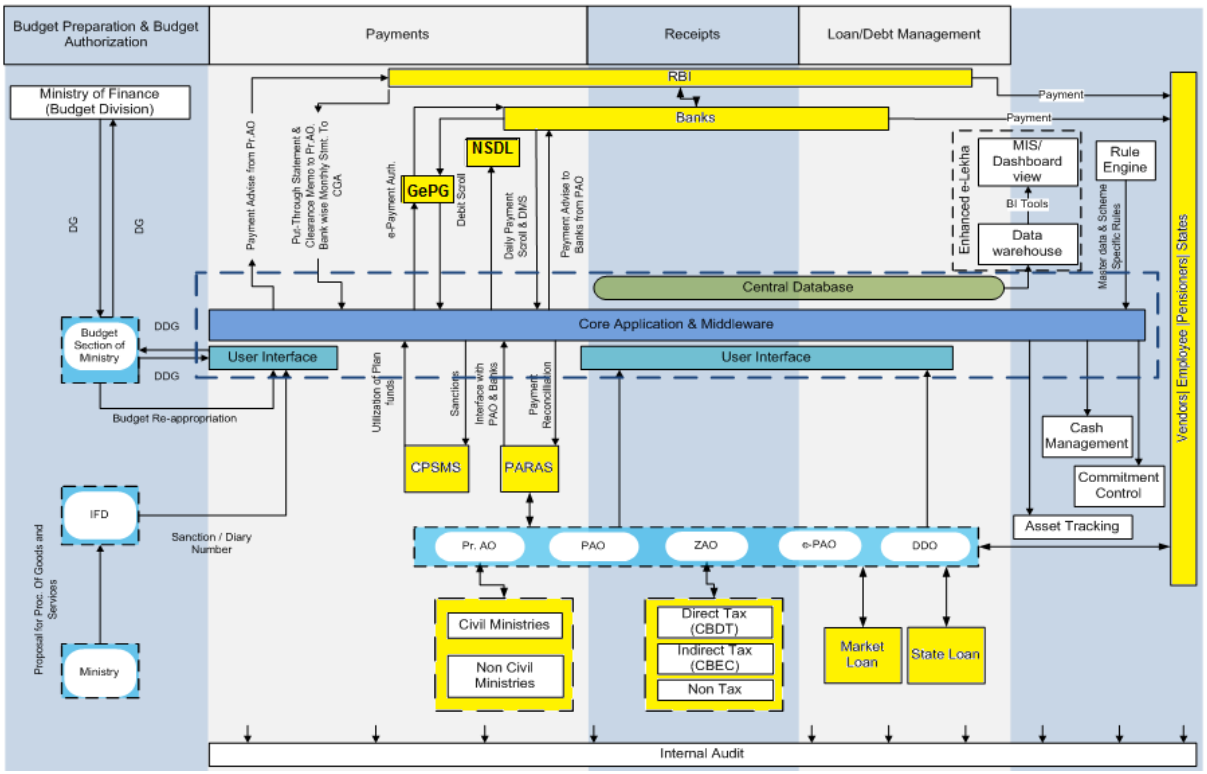
The 14th Report of the Second Administrative Reforms Commission (ARC) recommends that "A robust financial information system, on the lines of SIAFI of Brazil,needs to be created in the government in a time bound manner. This system should also make accessible to the public, real time data on government expenditure at all levels". In addition to the 14th Report of the Second Adminstrative Reforms Commission (ARC), the Technology Advisory Group for Unique Projects (TAGUP) also recommended setting up of an Expenditure Information Network (EIN).

In view of the stakeholder expecations, recommendations of the 14th Report of the second ARC and TAGUP; KPMG recomends setting up of an "**Integrated Government Financial Management System (IGFMS)".** The IGFMS shall include **Budget Preparation and Approval; Budget Execution, Accounting & Fiscal Reporting; Cash Management; Debt Management; Revenue Administration; and Audit Support**. Macro-Economic Forecasting and Personnel Management (except payroll processing and pension payments) shall remain out of scope of the proposed system. The Integrated Government Financial Management shall have suitable interfaces with the other entities and applications e.g. NSDL, RBI, Banks, CPSMS, PARAS etc. for seamless information exchange.

KPMG has studied various systems deployed in the developed and developing countries in order to incorporate the best practices from these countries in the proposed IT System.

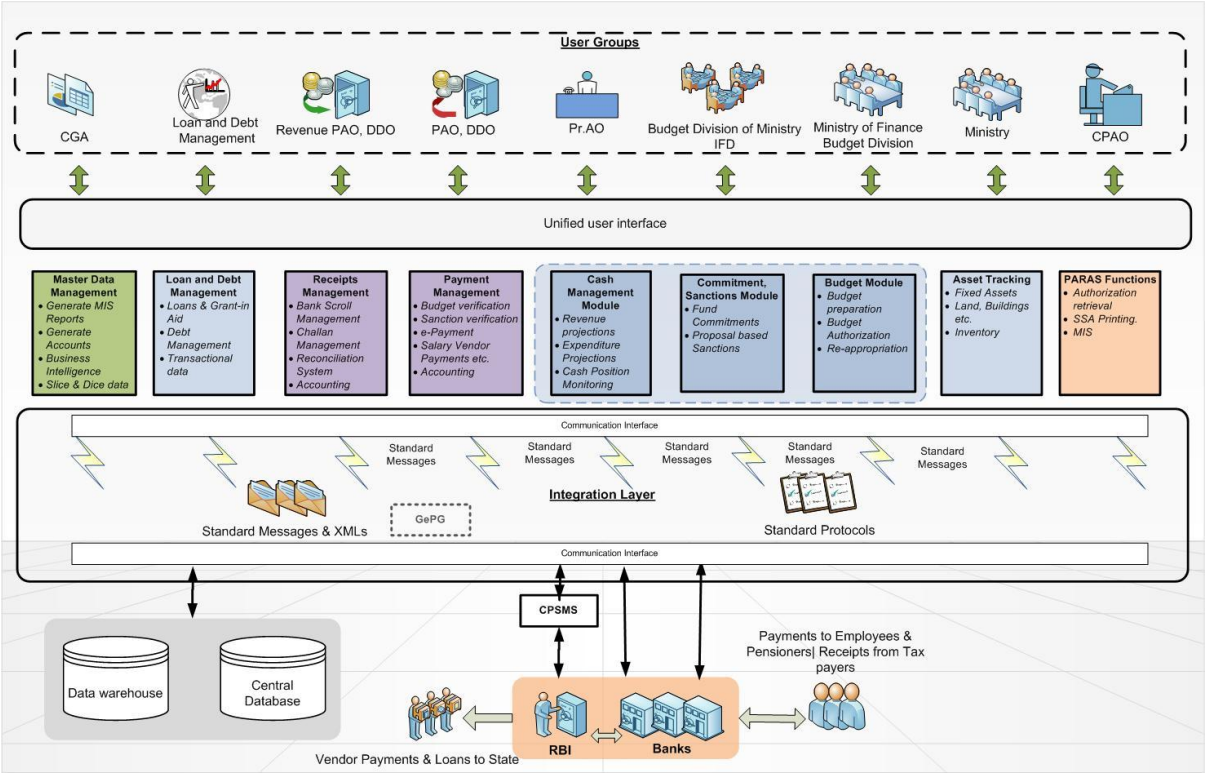
Apart from the best practices the following critical factors of architectural design have been considered in order to develop a robust and technically efficient system – Scalability; Availability; Security; Maintainability; Responsiveness; Efficiency; Adaptability and Standardization.

The Business Architecture, Technology Architecture, Security Architecture, Network Architecture and Deployment Architecture are discussed in detail in Chapter 4 of this document. The proposed Business Architecture is set out in the figure below:



The overall system consists of four core applications for capturing the functionality of budget, payments, receipts and loan & debt management. The additional functionalities like government asset tracking (financial / non-financial), centralized GPF, internal audit tools etc. have been considered while designing the IT systems. In continuation to this, scoping of IT systems further elaborates the functions of the core applications, sub applications and modules, along with the interfaces and actors involved.

The figure below describes various applications of the centralized solution.



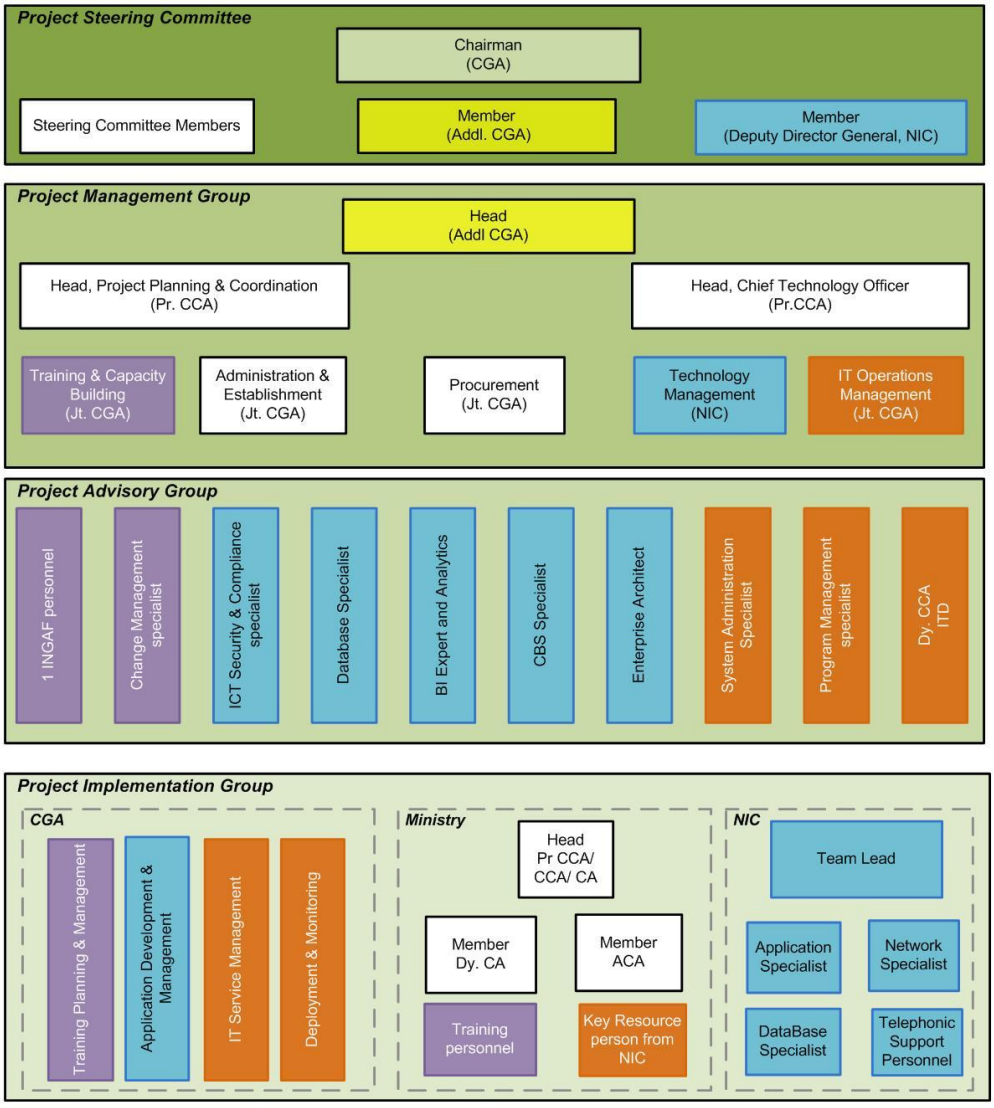
The information/data flow between different applications / entities is captured as part of the scoping of IT systems. It proposed that a data warehouse be created which will have data from all the applications, and with the help of business intelligence tools the system shall have the capability to use the data from the data warehouse and provide dash board view to key stakeholders at CGA and Ministry level.

The proposed system can be developed following two approaches– developing a bespoke application or deploying Commercially-off-the-Shelf (COTS) system. KPMG has detailed out the features of Oracle and SAP solutions that meet the requirements of the CGA's organisation. Both SAP and Oracle have offerings that partially or completely meet the requirements of the CGA's organisation.

It was highlighted in the assessment report that CGA does not have a Business Continuity Plan (BCP) at the moment. The proposed IGFMS bridges the gap through Disaster Recovery Planning which shall enable high availability of systems. The four key options of data recovery have been discussed in the report – storage based solutions; SAN / fabric based solutions; Host based solutions; and Backup and Restore.

The electronic data archival system is critical for any IGFMS for ensuring the availability of historical data in case the need arises. It is recommended that a data archival policy be formulated for the CGA's organisation that confirms to the various ISO standards. Quality assurance and quality control has been recommended for the IT System development process. It is proposed that the CGA's organization conform to one or more standards, such as ISO 9000 or a model such as CMMI. It is further proposed that the CGA's organisation obtain STQC certifications before rollout.

In order to support the rollout of the proposed IT Systems, a four-tier IT Governance structure may be constituted considering the wide scope of work and large number of stakeholders in CGA Accounting organization. This four-tier structure can be divided into the following groups: Project Implementation Unit (PIU); Project Management Group (PMG); Project Advisory Group (PAG); and Project Implementation Group (at CGA and Ministry).



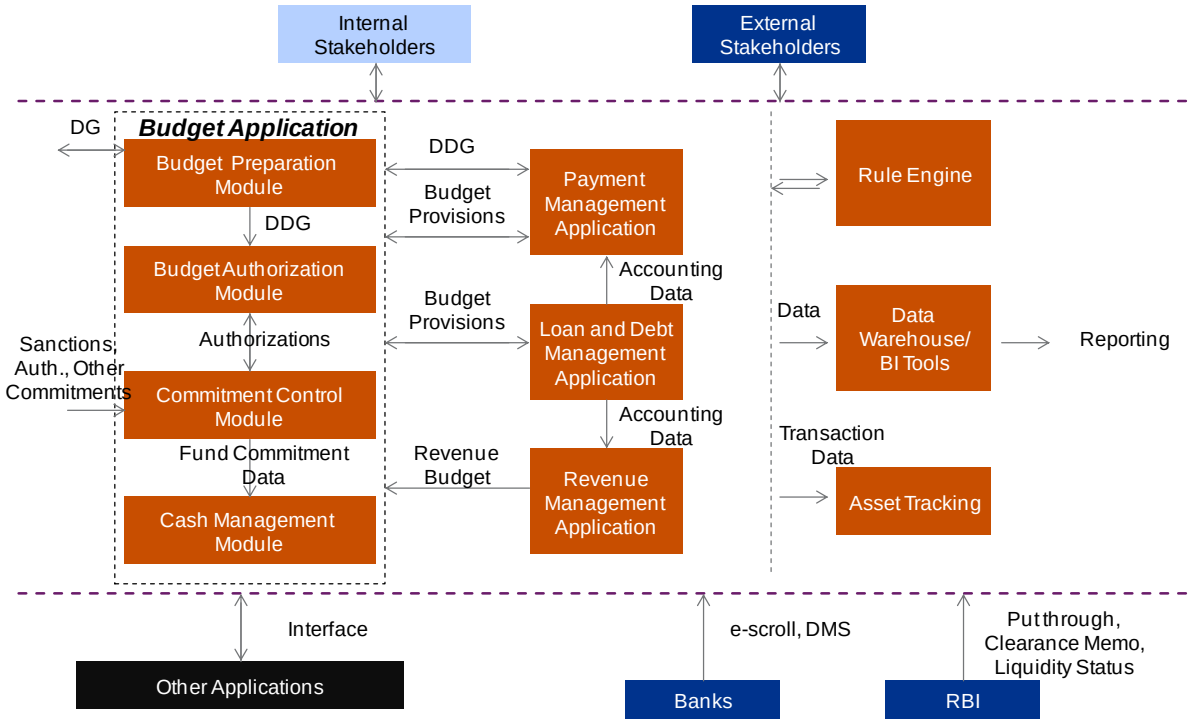
The Project Implementation Unit (PIU) headed by CGA shall function as the apex unit for policy advice and strategic guidance on various project aspects. Project Management Group shall function as Mission Execution Team and shall be assisted by Project Advisory Group which would consist of consultants with experience in various domains ranging from technology, banking and government accounting and shall bring necessary synergy in Project Management Group. At the support level Project Implementation Group shall act as a bridge between the various stakeholders and Project Management Group in implementation of various project components. The implementation group shall have specialist from implementing agency in the areas pertaining to Application Development & Management, IT Services Management, and Deployment & Monitoring and shall be responsible for day to day operational activities. Implementation Group will also have adequate representation from NIC and the respective Ministry.

Once the system is rolled out, the system support and maintenance mechanism of the IT systems becomes a crucial aspect when there is a requirement of an optimal level of service. It has been observed that at the CGA's organization, there is a need to establish a dedicated centralized IT service desk that is available 24 x 7 to provide technical support to the users and respond to all the queries and incidents pertaining to the software systems being employed. Complete in-house model; complete outsourcing model and hybrid model for IT support desk has been discussed in the report.

Change Management plays a critical role in ensuring that the buy-in from various stakeholders and to ensure smooth transition to the new way of working. Thus, introducing radical reforms has to be necessarily accompanied by efforts to change the mindsets of people – both within and outside the department. For instance, the service seekers need to know how to avail services with the new system implemented; the staff should be skilled to operate and work in a significantly newer way. A well-calculated and well-designed strategy has to be followed for staff to be trained work effectively in the new environment. It is necessary to formulate a change management plan with appropriate interventions for capacity building, training and stakeholder communications. Detailed Change Management Plan is set out in this report.

Finally, the Strategy report details out the Implementation Roadmap for the rollout of IGFMS. The prioritization of development / implementation is done considering the following parameters – criticality, dependency, user-base, availability of COTS and tentative timeline for development / customization. The proposed IGFMS broadly consists of four core

applications - budget application, payment management application, revenue management application, loan and debt management application and few other applications such as rule engine, business intelligence and asset tracking tools. A high level implementation plan is



set out below:

1.1 Key Action Points / Recommendation for O/o CGA

- Inclusion of Budget section & IFD of each ministry into the core accounting application.
- Opening of accounting codes through a work-flow between Ministry and CGA.
- Cash / Debt management to be part of the core accounting application.
- Commitment capturing to be undertaken through the proposed IT System.
- Building an employee master for payroll processing so that centralized GPF / NPS etc can be captured.
- Asset tracking to be included in the system so that the transition to accrual / modified cash can be undertaken as desired. Also, the rules for asset valuation need to be formulated by GoI.
- Unique ID for the Government employees needs to be provided.
- Enhancement of PARAS to compute and disburse pension using the GePG. The PPO information may flow from the PAO of the concerned ministry to CPAO.

- Authorizations to be captured through the system wherein, the agencies utilizing the funds can directly book accounts into the agency authorizing funds.
- Usage of data warehouse / business intelligence tools to generate custom built reports.
- Capturing accounting information from non-civil ministries either using interfaces with their existing system/ providing standardize format for data exchange.
- Information Security (IS) Policy Manual for the stakeholders and users to govern and guide on IS practices of O/o CGA.
- TIA-942 Data Centre Standard to be adhered to while preparing the LAN connections
- Solution to support SAML (the standard for exchanging authentication and authorization information between security management systems) without coding, including both SAML Consumer & SAML Producer modes of operation.
- There should be a single sign on into the entire IGFMS wherein one identity would be used to login into a PC and the same identity can be used for working within the application, database and other software and hardware part of the system.
- There should not be any mechanism to delete data or information. All activities of deletion should lead to data being moved from the main place to a secondary place earmarked for storing deleted data. Under no circumstances data should be expunged.
- The system should support Role-based Administration and Role Based & Rule Based User Provisioning.
- The entire IT system should be governed by a single user management policy which should be defined & deployed centrally using a centralized administration panel.
- The proposed solution must provide the ability to designate specific users as Administrators, Auditors, and Password Managers etc with appropriate rights. The proposed solution must also provide the ability to designate specific users as Subordinate or Group Administrators, to manage users and file permissions for their Group.
- Access to any terminal in the network using any kind of storage devices such as USB, CD, DVD, Floppy and Network terminals should be strictly prohibited and blocked. However it may be essential to allow some copying of data into the IGFMS or out of the Treasury system without jeopardizing the security of the system. Implementing agency should suggest a mechanism governed by processes as well as technologies which can allow such requirements to be addressed.
- The solution must provide support for IPv6 and FIPS140-2.
- The solution must provide SSL Support for Inter-Component Communication.

- A centralized patch management solution shall be deployed for the desktops and servers. This solution shall ensure that the patches for Operating System, RDBMS, any other type of system software, application software, etc can be administered centrally after performing appropriate testing and taking requisite permissions.
- In case of data upload (e.g. upload of a XML file / Excel file / ASCII file) or data transfer the application shall have controls such as data totalling / control totalling / checksums to ensure that the data transfer is complete and accurate. Each data generated out of the system such as MIS or any other information should be time stamped and digitally signed so as to ensure non-repudiation.
- Event logging is extremely helpful in documenting user activity. It creates an accurate record of user activity such as which users accessed which system, as well as which websites they visited when and for how long. The solution should log all types of events especially those related to security and transactions.
- The application should protect its audit records from unauthorized deletion, modification, or disclosure.
- Any critical log information which requires urgent attention, such as issues which can lead to downtime, should be captured properly and an appropriate alert be generated and sent to department officials as well as the technical team of the implementing agency.
- The solution should implement policy management solutions for access control and network security. The software for policy management will ensure implementation of well – defined policy and monitoring of any deviation from the department's policies, which would be in line with global standards like ISO 27001, BS7799, RBI & IBA guidelines, etc.
- The system shall put a limit on the maximum time length of an idle session, which should ensure that automatic session termination takes place after expiry of the specific time length
- The system should provide capability to modify the maximum time length of idle sessions dynamically.
- Users must not have access to the database prompt of the application. Access to the database prompt must be restricted only to the database administrator and / or a person designated for generating MIS reports
- All unused ports, both software and hardware, should be blocked at client PCs and at Server machines.

- The application server should be protected with appropriate Antivirus software.
- The Implementing agency shall use the known standards of Information Security Governance while dealing with the data.
- All workstation hardware and associated peripheral equipment will be marked with a unique asset identification code. The asset identification code will follow a defined naming convention that would uniquely and appropriately identify the asset.
- Latest version of anti-virus should be installed on all workstations, laptops and servers.
- Business continuity plan should comply with zero data latency i.e. the recovery point objective (RPO) for the database stored at BCP would be 0 minutes. However, it does not mean that application should be running on a no downtime policy. The replication process configured should not cause any effect over the transactions conducted over primary database, i.e., the primary and BCP database should be decoupled.
- The switchover from DC to BCP should not result in any data loss and similarly switchover from BCP to DC, after DC is restored back, should also not result in any data loss. Thus both databases should synch with each other such that at any point of time when switchover to the corresponding site is required the databases at both the places are completely synchronized.
- The backup and restoration policy should be framed and provided to the O/o CGA as a deliverable by the Implementing agency.
- To implement an archival mechanism there is a need to implement and bring in place a digital archival policy. With respect to archiving digital information, the following are important examples of archiving standards that are applicable for digital archiving in a government department:
    - ISO 18938:2008, Imaging materials – Optical discs – Care and handling for extended storage.
    - ISO/TR 18492:2005, Document Management Applications – Long term preservation of electronic document-based information.
    - ISO 19005-1:2005, Document management – Electronic document file format for long term preservation.
    - ISO 15489-1:2001, Information and documentation – Records management. Part 1: General
    - ISO/TR 15489-2:2001, Information and documentation – Records management. Part 2: Guidelines

- The standards to be followed in SDLC (Software development Life Cycle) are mentioned below:
    - Software Requirements Specification IEEE 830
    - Software Design Description IEEE 1016
    - Software Validation & Verification Plan IEEE 1012
    - Software Test Documentation IEEE 829
    - Software Project Management Plan IEEE 1058
    - Software Quality Assurance Plan IEEE 730
    - Software Configuration Management Plan IEEE 828
    - Portal development Guidelines for Indian Government website (GIGW)
    - Information access/transfer protocols: SOAP, HTTP/HTTPS
    - Interoperability: Web Services, Open standards, XML Standards
    - Master Data: Metadata standards
    - Scanned documents: Pdf (ISO 32000)
    - Digital signature: PKCS#7 (As per the IT Act 2000)
    - Document encryptions: PKCS specifications
    - Information Security system to be ISO 27001 certified
    - IT Infrastructure management ITIL / EITM specifications
    - Service Management ISO 20000 specifications
    - Project Documentation IEEE/ISO/CMMi (where applicable)
- A dedicated centralized 24 x 7, IT service desk for providing technical support to the users and respond to all the queries and incidents pertaining to the software systems being employed needs to be established.

1.2 Key Learning from IFMIS implementation around the World

- Electronic payment of pension / benefits through a centralized application in lines of Electronic Transfer Account as used in USA may be evaluated by O/o CGA.
- An ITS (as in the USA) like system can be developed in India especially now that the RBI is developing its CBS. A standardized data exchange format can be developed between RBI and Ministries requiring foreign exchange transactions. Ministries could use this data exchange mechanism to directly place their foreign currency transfer requests with RBI through this system. This shall help in standardization of exchange rates across ministries and thereby result in cost saving to the government in terms of currency conversions.

- As a Transparency measure, possibility of developing a transaction monitoring / bill tracking module can be placed in the public domain in line with the PACER system that exists in the US.
- Cheque issue and clearance status is captured in Forms CAM 10 and CAM 11 COMPACT. The Government can evaluate providing the tracking of cheques in the public domain for the benefit of its vendors (as in the USA).
- For the Civil Ministries, Government may consider issuing a pre-paid card (in line with the Eagle Cash used in US) filled with foreign currency to officers going abroad on official tours / study leaves etc. This shall allow them to draw money in foreign countries using standard ATMs and hence, shall help the Government in limiting cash transaction of foreign currency and subsequent conversion loss.
- Like in the US, there is a need in India to develop a payment / collection gateway that can accept payment from through debit card, credit card and net-banking. This shall help the Government in minimizing the duplication of efforts by each ministry in developing a gateway separately. GePG can be developed into an aggregator which can be used for receiving monies due to Government Department. Also, this gateway can be used by Government Departments to pay / disburse various kinds of payments to implementing agencies / beneficiaries of Government Funds.
- The Government of UK is replacing COINS (equivalent of e-Lekha in India) with OSCAR. One of the draw backs of COINS was that it did not contain transaction level data and the level of data aggregation was the choice of the agency. Hence, this feature should be evaluated while developing future system of O/o CGA.
- The UK system has replaced COINS with COGNOS which is a COTS application and fulfils the need of user defined reports which has been enabled through the use of COGNOS Business Intelligence. Hence, while developing a future system requirement of a Business Intelligence tools should be evaluated.
- SIAFI has a robust bank reconciliation system which allows close monitoring of suspense and advance accounts. This feature of SIAFI may be considered while defining the new IT System for O/o CGA.
- SIAFI provides a central system for monitoring all accounts payable of the Central Government, and regularly reports amounts carried over between fiscal years. Such feature should be evaluated in the future IT System for O/o CGA.

- All accounting transactions are recorded in SIAFI and it has strong inbuilt controls which play an important role in ensuring that expenditure commitments are only undertaken within the limits established by the budget and financial programming decrees. This feature is important for any future IT Systems for the O/o CGA as the current IT systems lack this feature which results in over / under expenditure in some cases.
- Accounting transactions in SIAFI are updated in real time, enabling the reconciliation of government accounting records with its accounts on a daily basis. This feature is critical for a future system for Government of India as this shall allow accurate generation of flash figures.
- The Budget division in Ministry of Finance also uses SIAFI thereby, making it possible to generate budget execution report with desired level of details at any point in time. Hence, the proposed system in India should have Budget division as a stakeholder in the system. This shall facilitate better budget execution and budget control.

2 Background

2.1 Overview from As-IS

KPMG had conducted a current state assessment of the existing IT applications landscape and submitted it to O/o CGA in form of an Assessment Report. The key findings of the Assessment Report are set out below:

1 The current applications have evolved over a period of time to address specific needs of stakeholders and have been developed using various technologies that limit the integration capabilities of these applications.

2 COMPACT, which is the core application for processing and recording financial transactions, shall not be able to adapt to the proposed changes in the CGA's business environment viz. New Accounting Code, seamless integration with budget, modified financial reporting etc as the application is hard-coded and requires substantial re-writing of code to make it flexible for the proposed changes.

3 With the advent of new regulations e.g. RTI, FRBM, Outcome budget etc, new reporting requirements have emerged viz. reporting of transaction level data, customizable MIS reports for various stakeholders for greater transparency which are currently not being fulfilled by any of the applications.

4 The IT applications at CGA's organisation are critical for smooth operations however, as of now there is no Disaster Recovery and/ or Business Continuity Plan in place.

5 The IT Systems are stand-alone and distributed which make them vulnerable and as there are limitations in ensuring the enforcement of various checks and balances e.g. restricting access to server; creation / updation / modification of users; periodic review of user accounts; segregation of development production and test environments; adherence to data back-up policy etc.

6 The result of the FQ-TQ analysis yields that the following applications need to be retired or replaced: (1) COMPACT, (2) COMPDDO, (3) Market Loan package, and (4) State Loan package. The following applications need to be enhanced technically: (1) e-Samarth, (2) e-Lekha, (3) COMPACT (REVACT), (4) COMPACT (RAMS), and (5) PARAS. A detailed FQTQ analysis was submitted as part of the Assessment Report.

Apart from the above the short-comings of each application is set out in detail in the Assessment Report which suggests that a complete revamp of the CGA's IT landscape is required in order to meet the challenges in the future.

2.2 Emerging Business Requirements

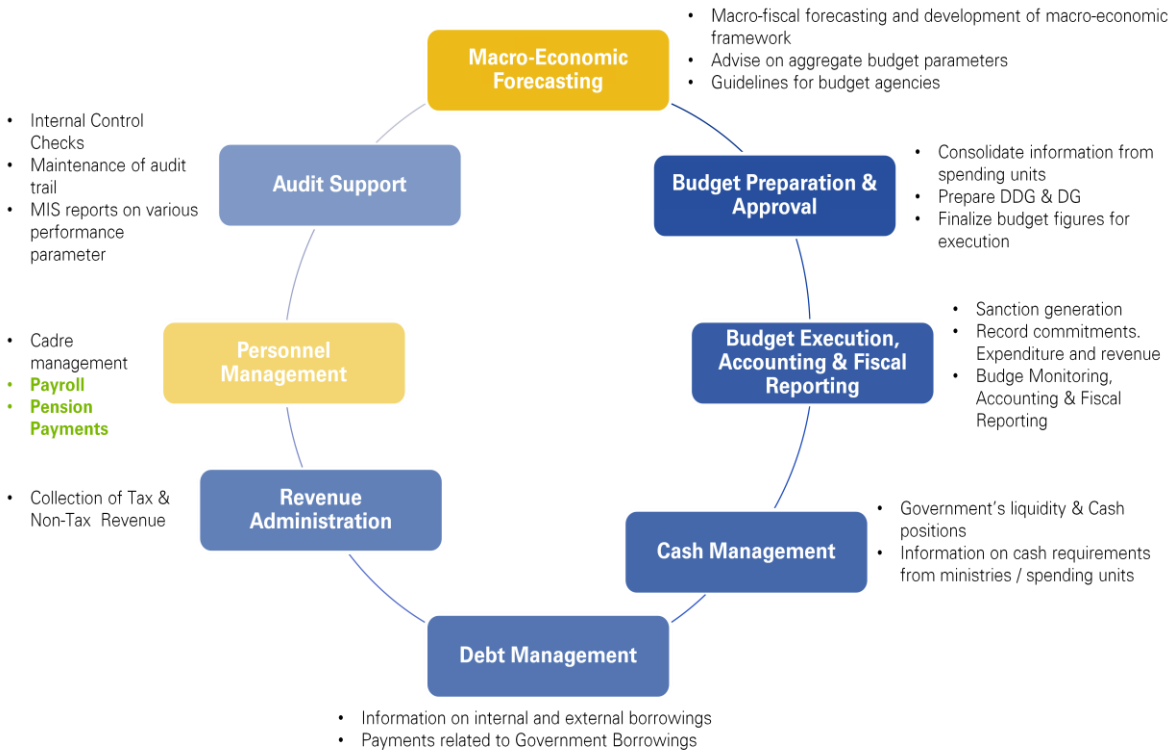
As set out in the Assessment Report, O/o CGA is discharging the duties entrusted upon them through various IT Systems developed over a period of time. However, over a period of time the role of O/o CGA has also evolved due to the changing business requirements from various stakeholders.

The following business requirements, in addition to the existing requirements have emerged which needs to be addressed through the IT systems deployed at O/o CGA:

1 **Integrated system** for budgeting, accounting and payments.
2 Capability to **generate finance accounts, appropriation accounts** from the system.
3 Capturing **accounting information** from both **civil ministries** and **non-civil ministries**.
4 Generating **accurate flash figures**.
5 Availability of **Transaction level data** for analysis and preparation of various reports that are required.
6 **Improving the overall payroll processing** for Government Employees by brining in the concepts like **centralized GPF, capturing NPS contributions, capturing long-terms advance, loans** etc. through IT systems.
7 **Effective fiscal control** through the usage of IT System.
8 Ability to **track government assets** (both financial and non-financial) and **liabilities** (both financial and non-financial).
9 Ability to **conduct slice-n-dice** of data for generating **customized MIS reports**.
10 **Commitment accounting** for better financial management.
11 Ability to **project various government commitments** e.g. payroll commitments, pension commitments, interest commitments, plan fund commitments etc.
12 Ability to conduct **effective cash management** through IT Systems.
13 **Effective performance evaluation** across various parameters for better controls through IT Systems.
14 Ability to incorporate **e-scrolls** from Banks and RBI for **automatic reconciliation** through IT Systems.
15 **Monitoring the effectiveness of IT Controls** on the system so as to effectively monitor government expenditure.
16 **Conducting Internal Audit** using IT Tools.

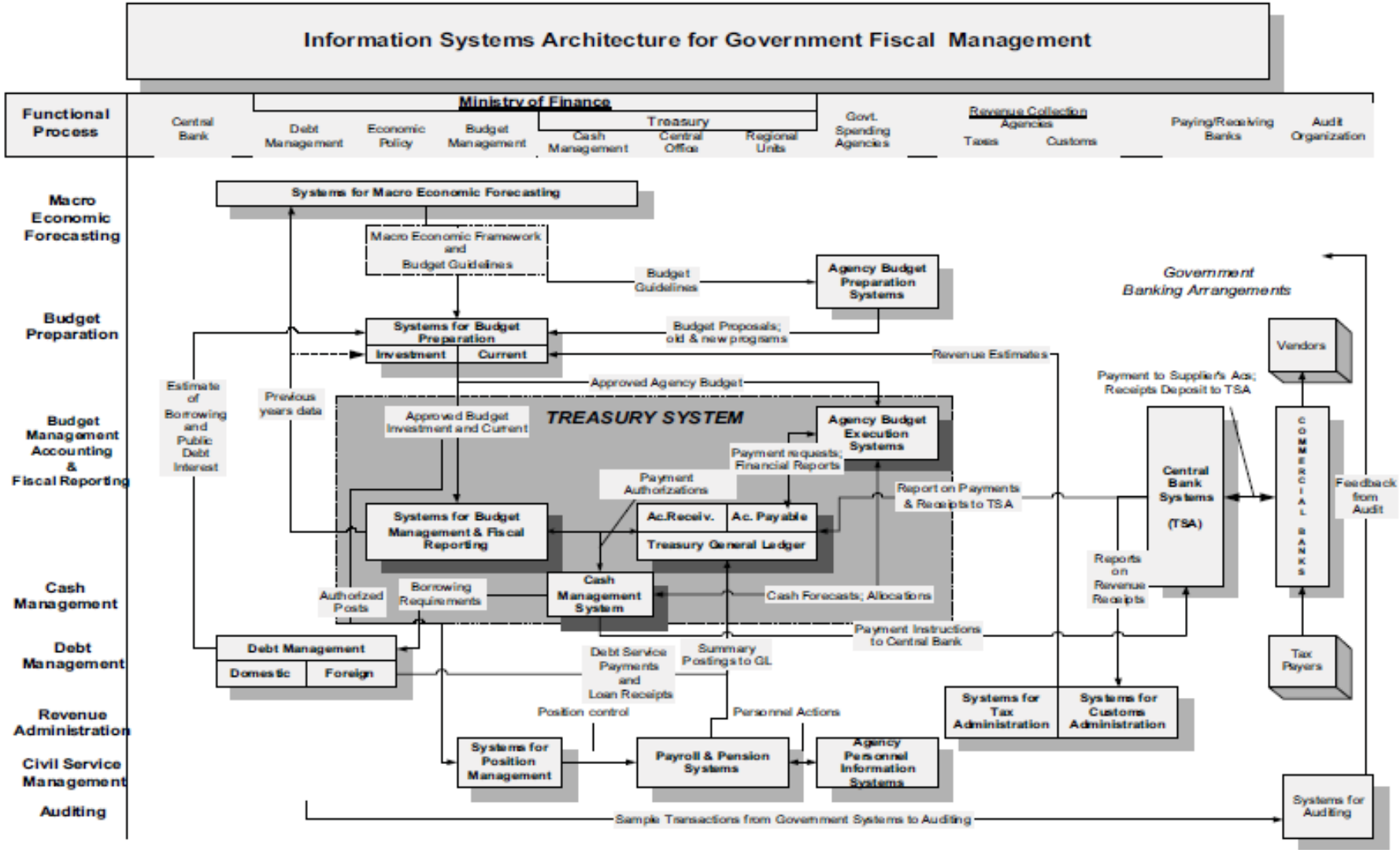
The analysis of business requirements suggests that an **Integrated Government Financial Management System (IGFMS)** is needed to address all the above requirements. The Integrated Government Financial Management System shall include **Budget Preparation and Approval; Budget Execution, Accounting & Fiscal Reporting; Cash Management; Debt Management; Revenue Administration; and Audit Support**. Macro-Economic Forecasting and Personnel Management (except payroll processing and pension payments) shall remain out of scope of the proposed system. The Integrated Government Financial Management shall have suitable interfaces with the other entities and applications e.g. NSDL, RBI, Banks, CPSMS, PARAS etc. for seamless information exchange.

The elements of such a Government Financial Management System is set out in the diagram below:



The scoping of the proposed Government Financial Management System is set out in Chapter 4 "Business IT- Alignment". While designing the Government Financial Management System, the World Bank's Treasury Reference Model has been studied and best practices from the same have been drawn.

The World Bank's Treasury Reference Model is set out in the diagram below:



As set out in the Treasury Reference Model, while designing the proposed Government Financial Management System the boundaries have been limited to Budget Management Accounting & Fiscal Reporting, Cash Management and Debt Management. The Budget preparation has been identified as a bottom-up flow of data from spending units to Budget Section of Ministry and subsequently to Budget Division of Ministry of Finance and then top-down flow of approved Budget data from Budget Division of Ministry of Finance. This information flow from Budget Section of Ministry to Budget Division of Ministry of Finance has been envisaged through an interface with the software being developed at Budget Division of Ministry of Finance. Payroll Management has been kept out of the system as the custodian of this data is the Administration Department of each Ministry however, basic data required for processing of payroll and related benefits like pension, LTA, HBA etc. have been envisaged in the proposed system. The system of revenue administration (receipt management) has been envisaged through ministry specific applications and hence, the transaction level data for same is envisaged to reside at the respective ministry. Only accounting information related to receipt management is expected to flow to the proposed system through suitable interfaces. In light of the above a gap analysis between and current and proposed system is conducted.

2.3 Gap Analysis

Current State	Future State	Gap	How the Gap is addressed
Business Functionality			
Budgeting, Accounting and Payments functions are address by **separate** and **distributed systems**.	**Integrated system** for budgeting, accounting and payments.	**Interfaces** between budgeting, accounting and payments systems needs to be developed.	The proposed system is envisaged to be an integrated system in which the budget division, budget section, IFD and spending units shall be the users.
Manual generation of finance accounts and appropriation accounts.	Capability to **generate finance accounts, appropriation accounts** from the system.	Functionality needs to be built-into e-Lekha to generate finance accounts and appropriation accounts. Timely availability of data in requisite format from Non-Civil Ministries is also needed to ensure preparation of finance and appropriation accounts from future IT Systems.	The system will be able to prepare net position of credit or debit under the appropriate accounting head during the financial year (Statement of Central Transactions) through automatic reconciliation with RBI and banks. The queries on excess / savings and subsequent responses shall be exchanged through the system till it is finally accepted. This shall reduce the time taken preparation of finance and appropriation accounts.
Non-timely receipt of data from non-civil ministries in a non-standardized format.	Capturing **accounting information** from both **civil ministries** and **non-civil ministries**.	An interface between CGA applications and non-civil ministries application is needed so that	The proposed system envisages standardized data exchange formats with the existing applications of the

Current State	Future State	Gap	How the Gap is addressed
		information a standardized format can be used for data exchange.	non-civil ministries. This shall help in pulling out data faster and at the desired accounting head level.
Data from some of the non-civil ministries only at Major head level.	Generating **accurate flash figures**.	Mapping of data from non-civil ministries in a standardized format is desired for generating accurate flash figures.	The proposed system envisages standardized data exchange formats with the existing applications of the non-civil ministries. This shall help in pulling out data faster and at the desired accounting head level.
Daily abstract uploaded on e-Lekha from civil ministries.	Availability **of Transaction level data** for analysis and preparation of various reports that are required.	Daily abstract uploaded on e-Lekha from civil ministries does not contain transaction level data. Data from some of the non-civil ministries is only at Major head level. In order to get transaction level data entire data from COMPACT needs to be uploaded into e-Lekha and standardized formats for non-civil-ministries are needed.	The proposed system will contain entry of each financial transaction and shall verify the same through the integration with GePG. Also, the implementation of new LMMHA will ensure that transaction is captured at the transaction level.
Manual preparation of salary bills. Manual computation of various components of salary. Manual entry of NPS contribution data.	**Improving the overall payroll processing** for Government Employees by brining in the concepts like **centralized GPF,**	Standardized application at DDO level for computation of various components of salary is needed. Also, there is lack of interface	The proposed system is envisaged as integrated application that shall be used by all spending units. The DDOs will maintain salary, GPF, NPS

Current State	Future State	Gap	How the Gap is addressed
	capturing NPS contributions, capturing long-terms advance, loans etc. through IT systems.	between DDO and PAO for processing of data. Data availability from CDDO is another gap which needs to be addressed. The gap exists because of lack of automated data exchange mechanism. Unique IDs for the Government employees needs to be provided for tracking of various details pertinent to an employee.	and all payroll related data in the centralized application wherein, each employee shall be identified by a unique code. The data maintained by administration shall be validated periodically by DDO in order to avoid any discrepancy.
Manual control mechanism.	**Effective fiscal control** through the usage of IT System.	Integrated system is required which allows for expenditure control mechanism at various levels.	The proposed system envisages the use of a Rule engine so that the fiscal controls in the system can be exercised.
Manual tracking through stock registers for non-financial assets.	Ability to **track government assets** (both financial and non-financial) and liabilities (both financial and non-financial).	Adequate interfaces with various divisions of Ministry of Finance are one of the major gaps for tracking financial assets and liabilities of the Government.	Asset purchases are nothing but individual transactions, the transactions that are classified under the head – Asset Purchase in the proposed system shall automatically move to an asset register which will

Current State	Future State	Gap	How the Gap is addressed
		Digitization of records is a gap in tracking of non-financial assets as it is difficult to verify assets from manual records that have been created over a period of time. Also, Policy for valuing and recording fixed assets is one of the major gaps in tracking non-financial assets.	apply business rules (defined by CGA) to value the asset in the books of accounts. Historical data shall be procured from administration department and the same shall be digitized in the system.
MIS reports generated through e-Lekha.	Ability to **conduct slice-n-dice** of data for generating **customized MIS reports**.	Business Intelligence tool for generation of customizable MIS reports is a gap because of which slice-n-dice of data cannot be undertaken to generate customizable reports.	The proposed system shall have a Business Intelligence tool that shall assist the management to generate MIS reports that suit their requirement.
No mechanisms of capturing government commitments (for funds).	**Commitment accounting** for better financial management. Ability to **project various government commitments** e.g. payroll commitments, pension commitments, interest commitments, plan fund commitments etc.	An integrated system is desired that captures various commitments e.g. interest payments, principal payment, salary payments, pension commitments of the Government.	The proposed system is envisaged to be an integrated system in which the budget division, budget section, IFD and spending units shall be the users. Hence, the commit of salary / pensions can be captured from the data available at spending units. The commitments for plan funds can be captured through the sanctions as

Current State	Future State	Gap	How the Gap is addressed
			soon as they are approved at IFD. The commitment against vendor payments can be captured at IFD as soon as the contract with vendor is finalized and approved by IFD. The other commitments like interest payments / principal repayments can be captured through the debt management module proposed in the system.
Manual cash management through reports available from RBI.	Ability to conduct **effective cash management** through IT Systems.	An integrated system (with an interface with the RBI) that processes various government payments is desired so that better cash management can be undertaken.	The various government commitments shall be captured in the system as described above. The same information shall be used to predict the cash requirement of the government on a daily basis. Additionally an interface with the RBI shall be developed that shall exchange data relating to the availability of cash (which shall draw inputs from the daily receipt of the government) at RBI and government liquidity requirement. Hence, this

Current State	Future State	Gap	How the Gap is addressed
			shall result in better cash management.
Manual reports from e-Lekha for performance evaluation of Pay and Accounts offices.	**Effective performance evaluation** across various parameters for better controls through IT Systems.	No mechanism for performance evaluation of Drawing and Disbursing Officers is in place that monitors the days in which a bill is prepared and passed. Also, various controls cannot be monitored as the preparation of bills and disbursement of payments happen in distributed systems.	The proposed system shall affix a data and time stamp to each transaction hence, enabling the management to custom generate performance reports of each DDO / PAO on their adherence to rules as specified in CAM.
Manual scrolls and put-through statement used for reconciliation.	Ability to incorporate all statement in desired format/ **e-scrolls** / **put-through and clearance memo** from Banks and RBI for **automatic reconciliation** through IT Systems.	No standardized mechanism of data exchange with Banks and RBI is devised because the processing happens in distributed system (only REVACT and RAMS can incorporate e-scrolls). No system for automatic reconciliation (due to distributed and disconnected systems) is in place.	The proposed system envisages incorporating scrolls from the banks and RBI into the system thereby facilitating automatic reconciliation.
Manual expenditure control mechanisms.	**Monitoring the effectiveness of IT Controls** on the system so as to effectively monitor government expenditure.	No mechanism to evaluate various IT controls is in place as the systems are distributed.	The proposed system envisages monitoring effectiveness of IT Controls through building in business logics in the system and then evaluating controls through internal

Current State	Future State	Gap	How the Gap is addressed
			audit tools.
IT Infrastructure			
Decentralized distributed Solution	**Centralized** Solution.	The automatic data transfer mechanism to central server is missing. Also, the current systems lack in maintenance of standardized data.	The proposed system envisages utilizing a centralized architecture through which better application maintenance, effective back-up and restore, BCP, standardization can be ensured.
VPN available only for PAOs.	**Extension** of CGA **VPN** to DDOs / CDDOs.	The COMPDDOs are not connected the CGA VPN and hence, not connected to the PAOs.	It is suggested that the CGA VPN be extended to the DDO by utilizing NICNET / NKN or VPN over broadband to ensure secured access.
Rollout of Government ePayment Gateway to PAOs in progress.	Capturing **all transactions** via **Government ePayment Gateway**.	Policy decision to extend the Government ePayment Gateway to CDDOs is desired in order to capture transaction level data.	It is proposed that the ePayment Gateway be extended to CDDOs however, this requires policy decision.
Export of data abstract from one system to another.	**Seamless flow** of **information** with various applications.	Building of interfaces that pull / push data in standardized formats is desired for seamless flow of information.	It is proposed that standardised data exchange formats be developed to exchange date with RBI, Banks, non-civil ministries for seamless flow of desired information.
Information, Communication and Technology Infrastructure a	Extension of **Information, Communication and Technology**	Policy decision is needed to bring DDOs / CDDOs into CGA's IT	It is suggested that a policy decision be undertaken to bring DDOs /

Current State	Future State	Gap	How the Gap is addressed
challenge for remote DDOs / CDDOs.	**Infrastructure at DDOs / CDDOs**.	application to ensure availability of the requisite infrastructure.	CCDOs under CGA's IT application.
No **Disaster recovery site** and Business continuity planning in place.	DR site with fail safe BCP.	DR site hosting model with a well defined BCP Policy and Procedure is gap for implementing a failsafe BCP.	A centralized architecture is proposed that shall help in implementing BCP and other policies in effective and efficient manner.
Change Management			
Rollout and maintenance of applications handled by the IT Division of CGA.	**Institutional structure** for **rollout and maintenance** of centralised application.	Lack of trained manpower to support the roll out and maintenance.	The training requirement is set out in the report in order to up-skill the existing manpower.
IT Division within CGA to support e-Lekha application.	Helpdesk for **issue resolution**.	The helpdesk support is inadequate to provide resolution to all users. Also, there is no mechanism to track issue resolution.	An adequate support mechanism is suggested in the report to support the proposed application.
Awareness being developed through training on e-Payment.	Awareness of **Internet Banking** concept.	Standardized training and refresher courses are needed.	External training support is suggested in order to standardize the training.
Awareness being developed through training on e-Payment.	Awareness of **e-Commerce & e-Payments** systems concept.	Standardized training and refresher courses are needed.	External training support is suggested in order to standardize the training.
Awareness being developed through training on e-Payment.	Awareness of **Digital signature** & encryption concepts.	Standardized training and refresher courses are needed.	External training support is suggested in order to standardize the training.

Current State	Future State	Gap	How the Gap is addressed
		Manuals containing standard operating procedures needs to be developed.	
Low awareness of security and hacking concepts.	Awareness of Computer **security & hacking** concepts.	Standardized training and refresher courses are needed.	External training support is suggested in order to standardize the training.
Low awareness of the computer virus concept and protection.	Awareness of **Computer Virus concepts** and protection.	Standardized training and refresher courses are needed.	External training support is suggested in order to standardize the training.
Low awareness of the data access policy. Multiple administrative users created on the system because of lack of controls.	Awareness of **Data access** policy.	Standardized training and refresher courses are needed.	External training support is suggested in order to standardize the training.
Low awareness of backup & disaster recovery concepts leading to frequent loss of data.	Awareness of **Backup** & **Disaster recovery** concept.	Standardized training and refresher courses are needed.	External training support is suggested in order to standardize the training.
Low awareness of day-to-day trouble shooting.	Readiness for **Day-to- day trouble shooting**.	Standardized training and refresher courses are needed. Manuals containing standard operating procedures needs to be developed.	External training support is suggested in order to standardize the training.

3 Financial Management System – International Examples

Government Financial Management is being carried out through various IT Systems in many developed / developing countries. KPMG has conducted a secondary research on the various countries and have also interacted with various service providers like IBM, Oracle and SAP who have been involved in implementing Financial Management Systems in various countries. A snapshot of various IT Systems deployed in various countries is set out in this section.

3.1 Overview of IT Systems Deployed at USA[1]

The Financial Management Service (FMS), a bureau of the United States Department of the Treasury, provides central payment services to Federal Program Agencies, operates the federal government's collections and deposit systems. FMS provides government-wide accounting and reporting services, and manages the collection of delinquent debt owed to the government. FMS also supports federal agencies' financial management improvement efforts in the areas of education, consulting, and accounting operations. Currently the US has separate systems for payments, collections, debt management and accounting.

Payments	Collection	Debt	Government Accounting
•ASAP: Used for paying Implemenation Agencies that is pre authorised by Fedral Agencies •ETA: Is a type of account designed for individuals who receive Fedral Agencies •IPP: Resembles an e-Procurement Portal •ITS.Gov: Application for payment / receipt of foreign payments •PACER: Application to check status of claims •SPS: Application to create payment schedule •TCIS: Records / Reconcilies worldwide issuance of payment •Vendor Experess: Is an application for the commercial vendor of Fedral Agencies •Eagle Cash: Is an application for US military for making payments to its personnel	•CAS: Through this government collects obligations via credit or debit card transactions •CashLink II: Receives deposit information, initiates fund transfer and concentrates daily deposits •EFTPS: Free Service to pay all federal taxes •Pay.Gov: To process collections electronically using Intenet Technologies	•Debt Check: To confirm whether applicants for federal financial assistance owe delinquent non-tax debt to the federal government or owe delinquent child support •Fed Debt: FedDebt is a comprehensive system that integrates FMS' Cross-Servicing and Treasury Offset Programs	•FACTS I: Collects agency pre-closing adjusted trial balances •FACTS II: Allows agencies to submit one set of accounting data •FMS Registry: Information about government-wide financial data elements •GFRS: Application designed to collect the Federal Program Agencies closing package information •IFCS: IFCS is the official confirmation system for FPAs that engage in fiduciary intragovernmental transactions •GOALS II: Report and view agency financial information provided to Treasury •GWA: Addresses the central accounting and reporting functions •IPAC: Provide a standardized interagency fund transfer mechanism •SAM: Assist GWA in classifying financial transactions •TCIS: reconciles the worldwide issuance and payment of U.S. Treasury cheques

[1] Source: Financial Management Service, A Bureau of the United States Department of the Treasury

3.1.1 Systems for Payments

Name of System / Application	Description
Automated Standard Application for Payments (ASAP)	• ASAP allows grantee organizations receiving federal funds to draw from accounts pre-authorized by federal agencies. • It makes payments to financial agents that are performing financial services for FMS and other federal agencies.

Electronic Transfer Account (ETA)	• ETA is a low-cost account for recipients of Federal payments. The U.S. Department of the Treasury designed the ETA for individuals to receive their Federal payments electronically. Generally anyone who receives (or represents someone who receives) one of following Federal Government payments is eligible to receive his / her monthly payments electronically through ETA.
	  ◦ Social Security
	  ◦ Supplemental Security Income (SSI)
	  ◦ Veterans Benefits
	  ◦ Civil Service Wage Salary or Retirement Payments
	  ◦ Military Wage Salary or Retirement Payments
	  ◦ Railroad Retirement Board Payments
	  ◦ DOL / Black Lung

Internet Payment Platform	• The IPP provides a centralized location to view all transactions in the purchase-to-pay process. It transforms paper-based processes into an electronic process for both federal agencies and their suppliers. The IPP's modular design allows agencies to implement functionality in phases, according to their business need.
	• IPP Functions and Modules include:
	  ◦ Digital Orders
	  ◦ Digital Invoices
	  ◦ Workflow
	  ◦ Invoice Self-service
	  ◦ Early Payment Opportunity
	  ◦ Payment Reporting
	  ◦ Central Supplier Directory
	  ◦ E-mail Notification

International Treasury Services (ITS.Gov)	• ITS.gov enables federal agencies to issue foreign currency payments using the Automated Clearing House (ACH) network, Wire, SWIFT

Name of System / Application	Description
	(Society for Worldwide Interbank Financial Telecommunication), Check, Western Union or Pay upon Proper Identification (PUPID) transactions. Additionally, ITS.gov enables agencies to issue international US Dollar wire transfer payments without a corresponding US financial institution. FMS processes monthly recurring benefit payments, foreign payroll, vendor, and miscellaneous payments. • There is no cost to federal agencies to use ITS.gov. The U.S. Treasury pays all transaction fees associated with processing international payments and collections, including any in-country lifting fees.
Payments, Claims and Enhanced Reconciliation (PACER)	• PACER provides on-line access to payment status, capability to initiate claims, and the ability to view the initial on-line disposition for Electronic Fund Transfer and cheque payments.
Secure Payment System (SPS)	• SPS is an application that provides a mechanism by which government agencies can create payment schedules in a secure fashion, and with a strictly enforced separation of duties. This application allows personnel at Federal Program Agency (FPA) locations to submit schedules to FMS over a browser/web interface. • Two different user-types are required and responsible for an FPA to submit schedules to SPS. First, a Data Entry Operator (DEO) creates a schedule and submits the schedule for certification. Next a Certifying Officer (CO) examines the schedule and upon verification, certifies the schedule which results in the schedule being submitted to FMS.
The Treasury Check (cheque) Information System	• TCIS records and reconciles the worldwide issuance and payment of U.S. Treasury cheque. This system also allows end users to query the Payments, Claims & Enhanced Reconciliation (PACER) system for claim status on Automated Clearing House (ACH) payments.
Vendor Express (Service)	• Vendor Express electronically transfers money and remittance information through the ACH network to commercial payees of federal agencies. • FMS has recently enhanced the Vendor Express Program with additional electronic data interchange (EDI) capabilities to provide improved payment services that benefit both federal agencies and

Name of System / Application	Description
	the commercial payees. • EDI is the computer-to-computer transmission of business information in a standardized format.
Eagle Cash (Service)	• EagleCash is a cash management tool designed to support U.S. military personnel deployed in combat zones and on peace-keeping missions. • The program, which improves convenience for Soldiers and other authorized personnel, was developed and is managed jointly by the U.S. Army, U.S. Air Force and U.S. Department of the Treasury. • The program uses smart-card technology and off-line batch processing to reduce the amount of U.S. currency in circulation overseas, and to take workload out of the base Finance Office. • EagleCash cards can interface with automated kiosk devices located at convenient locations on the camp/base, which allow enrolled cardholders self-service access to funds in their U.S.-based checking or savings accounts.

3.1.2 Systems for Collections/ Receipts

Name of System / Application	Description
Card Acquiring Services	• Through the Card Acquiring Service, the government collects obligations via credit or debit card transactions. The objective of the service is to increase electronic collections received by the government, and process these transactions in an efficient, timely and cost-effective manner. • Payments include assessed fees, fines, and other monies due the federal government. Card acquiring services are provided at both domestic and international locations. • Most federal agencies that accept credit or debit cards for payment, including Visa and MasterCard branded products must do so through the Card Acquiring Service. The U.S. Postal Service, Army/Air Force Exchange Service, Navy Exchange, the Smithsonian, and certain other non-appropriated funds instrumentalities are authorized to obtain credit and debit card acquiring services on their own and thus do not participate in this program.

Name of System / Application	Description
Pay.gov	• Pay.gov has been developed to meet the FMS commitment to process collections electronically using Internet technologies. Pay.gov satisfies agencies and consumers demands for electronic alternatives by providing the ability to complete forms, make payments and submit queries 24 hours a day electronically. • Launched in October 2000, Pay.gov is a secure government-wide collection portal. The application is web based allowing customers to access their accounts from any computer with Internet access. It provides a suite of services allowing agencies to obtain and process collections in an efficient and timely manner. The Pay.gov application is comprised of 4 services: Collections (ACH and Credit Card), Forms, Billing/Notification, and Reporting.
Electronic Federal Tax Payment System (EFTPS)	• It is a free service from the U.S. Department of the Treasury to pay all federal taxes.
CASHLINK II	• Receives deposit information, initiates fund transfers, and concentrates daily deposits made through multiple collection mechanisms into the Treasury's account at the Federal Reserve Bank, • Provides federal agencies with information, via the Internet, to verify deposits, ACH and Fedwire transfers, as well as adjustment information used to reconcile their accounts, and • Assists the Treasury in managing depositary services provided by financial institutions and monitoring the cash position of the U.S. government.

3.1.3 Systems for Debt Collection

Name of System / Application	Description
Debt Check	• This program allows agencies and outside lenders to obtain information regarding whether applicants for federal loans, loan insurance or loan guarantees owe delinquent child support or delinquent non-tax debt to the federal government.
Fed Debt	• FedDebt is a comprehensive system that integrates FMS' Cross-Servicing and Treasury Offset Programs; FMS ensures that its customers receive efficient and secure service. FedDebt provides

Name of System / Application	Description
	Federal agency users with a Web based interface to FMS' debt collection system. • This system has the capacity to separate and protect sensitive data (Personally identifiable Information) and employs stringent user authentication procedures, protecting the financial interests of the American taxpayer.

3.1.4 Systems for Government Accounting

Name of System / Application	Description
Federal Agencies' Centralized Trial-Balance System (FACTS I)	• FACTS I is a system that collects agency pre-closing adjusted trial balances at the fund group level using the U. S. Standard General Ledger (USSGL) accounts in a numerical order with the required attributes. • The attributes are modifiers that further describe a USSGL account in order to meet a specific reporting requirement in the preparation of the Financial Reports.
FACTS II	• The Federal Agencies' Centralized Trial-Balance System (FACTS II) allows agencies to submit one set of accounting data. • This data includes mostly budgetary information that is required for the Report on Budget Execution and Budgetary Resources, the Year-End Closing Statement (FMS 2108), and much of the initial data that will appear in the prior year column of the Program and Financing (P&F) Schedule of the President's Budget.
FMS Data Registry	• FMS Data Registry is an authoritative reference for information about government-wide financial data elements; specifically those data elements commonly used across multiple agencies. • It is developed to promote the common identification, use and appropriate sharing of financial data/information across the federal government. It contains information about the definition, authoritative source, data type, format and uses of common financial data.
Government wide Financial Report System (GFRS)	• GFRS is an Oracle based internet application designed to collect the Federal Program Agencies closing package information. • The closing package is a set of special purpose financial statements that represents the FPAs' comparative, audited consolidated,

Name of System / Application	Description
	department-level financial statements and is used to prepare the Financial Report of the United States. • The primary purpose of this process is to present a comprehensive report on the Government's financial position as well as defining a mechanism that assist with resolving material deficiencies identified by the Government Accountability Office.
Intra-governmental Fiduciary Confirmation System (IFCS)	• IFCS is the official confirmation system for FPAs that engage in fiduciary intra-governmental transactions. • FPAs are required to confirm and reconcile the following fiduciary transactions: Investment with the Bureau of the Public Debt (BPD), Borrowings from BPD or the Federal Financing Bank, Federal Employees' Compensation Act transactions with the Department of Labour, and Employee Benefit Program transactions with the Office of Personnel Management.

Government On-line Accounting Link System II (GOALS II)	• Allows agencies to report and view their financial information provided to Treasury.
	• GOALS II applications include:
	  • FMS 1219/1220 System: The FMS-1219/1220 uses a state-of-the-art Windows-based environment and enables real-time transmission of monthly transactions to the Central Accounting System (STAR).
	  • IPAC System (described separately)
	  • GFRS/FACTS I/IFCS (described separately)

Government-wide Accounting and Reporting Program (GWA)	• It addresses the central accounting and reporting functions and processes associated with budget execution, accountability, and cash/other asset management. This includes the collection and dissemination of financial management and accounting information from and to federal program agencies. • It also includes the business processes in FMS that are related to ledger accounting for each appropriation, fund, and receipt account's Fund Balance with Treasury, General Ledger accounting for the cash and monetary assets of the government, and the preparation of the Monthly Treasury Statement and the U.S. Government Combined Statement and Appendix.
Intra-Governmental	• The Intra-Governmental Payment and Collection (IPAC) Systems

Name of System / Application	Description
Payment and Collection System (IPAC)	primary purpose is to provide a standardized interagency fund transfer mechanism for Federal Program Agencies (FPAs). IPAC facilitates the intra-governmental transfer of funds, with descriptive data from one FPA to another. • It is software to process intra government payment and collection which facilitate the accounting process.
Shared Accounting Module	• The Shared Accounting Module (SAM) is an application that facilitates the process of validating or deriving Treasury Account Symbol (TAS) and Business Event Type Code (BETC) combinations to assist GWA in classifying financial transactions as they occur. SAM is becoming the single source for Enterprise Reference Data to government agencies and Treasury applications.

3.1.5 Key Developments in the US Treasury Management Systems

Payment Application Modernization (PAM)

The vision for the PAM initiative involves replacing **30+ COBOL and Assembler applications** that have evolved over the last several decades, **with a single standardized application**. Because the basic functionality within all of the current applications is similar, a standardized system that is highly extensible and configurable is the desired end state. In addition to standardization, FMS is looking to modernize the technologies employed in the development of the system, using commercial off-the-shelf (COTS) products where feasible. Additionally, the Project will incorporate new and enhanced functionality to support improvements in the payment process.

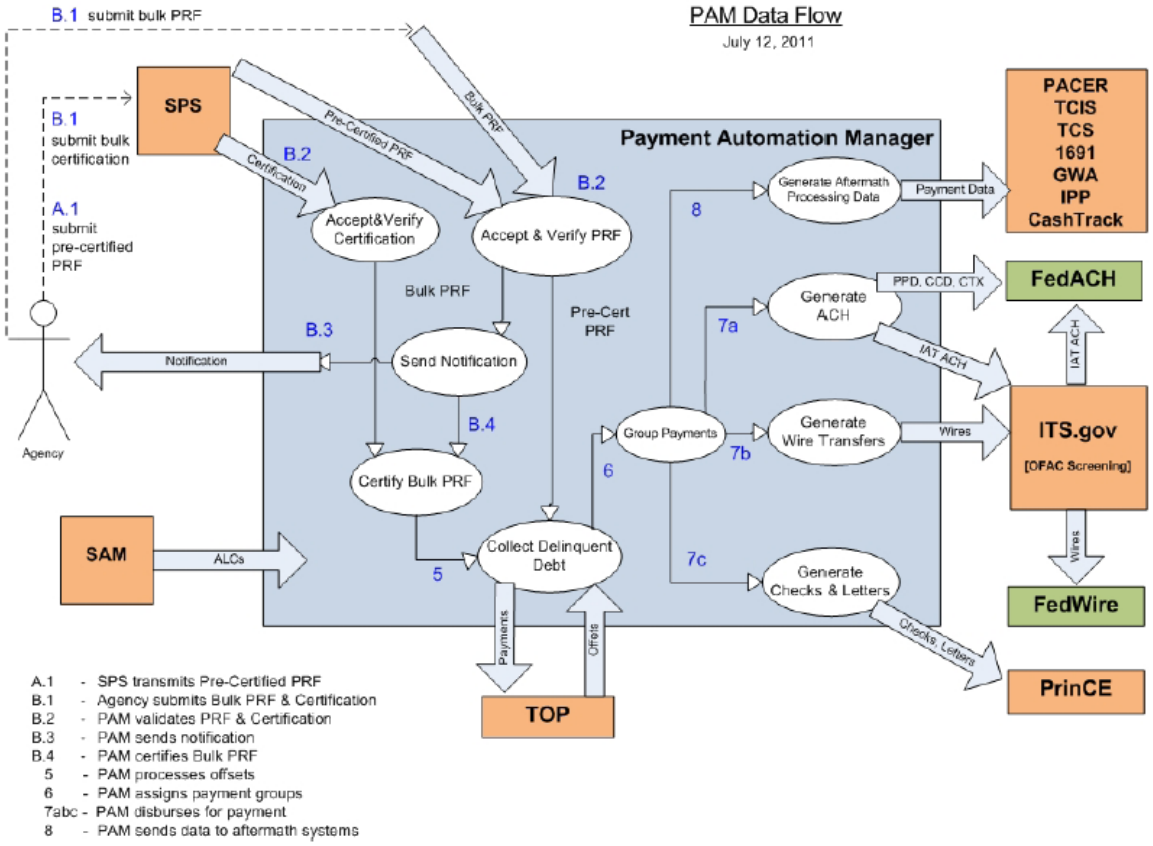
Effective October 1, 2014, all Federal agencies using Treasury disbursing services will be required to submit payment data in a newly developed standard input format. Using the new PAM standard format, agencies shall provide Treasury Account Symbol/Business Event Type Code (TAS/BETC) information along with your payment files, satisfying new Government wide Accounting (GWA) reporting requirements.

PAM is an effort to standardize and modernize the legacy software applications that are used by the three FMS Regional Financial Centres (RFC's) to distribute approximately 1 billion federal payments annually.FMS plans to achieve the following:

- Centralized support roles
- Standard Payment Request (SPR)

- Standard Notification Report
- Standard check face

Key Features of PAM



- 1 standardized application will replace 30+ payment processing applications, many of which have redundant functionality.
- Use of current technology to replace legacy applications that are decades old and use COBOL and Assembler.
- Automated workflow will eliminate numerous manual processes.
- 14 interfacing applications.
- Application to operate within FMS computing environment.
- There will be changes in the way payments are processed as all 100 percent of the validations will be conducted upfront. Once a payment from an agency is certified, it will be processed immediately. In legacy, payment processing takes 2-3 hours to validate, batch, and process a payment file. In PAM, if validations are passed, the payment file and the matching certification process automatically, within seconds.

Collections and Cash Management Modernization (CCMM)

The Collections and Cash Management Modernization (CCMM) initiative is a multi-year effort to simplify and modernize the collections and cash management programs of FMS and the Department of the Treasury. CCMM involves a re-architecting of processes that have built up over decades. It impacts over two dozen programs that process collections for hundreds of agency cash flows (taxes, customs duties, coin sales, etc.), conduct over 400 million transactions a year, and collect over $3.1 trillion a year.

Credit Gateway:

- The Credit Gateway is a deposit program that the U.S. Treasury's Financial Management Service (FMS) uses for the receipt of federal agency Fedwire and Automated Clearing House (ACH) credit transactions. The Credit Gateway is a component of FMS's Collections and Cash Management Modernization (CCMM) initiative.
- The Credit Gateway is a service operated by a commercial bank that has been designated as a financial agent of the government. The bank processes FMS transactions using its own infrastructure and commercial software. However, the transactions settle at Federal Reserve Banks, rather than at the commercial bank. The Gateway interfaces directly with Federal Reserve Bank systems to process transactions. As collections are processed by the Gateway, detail transaction information is sent in real time to FMS reporting systems, namely the Transaction Reporting System (TRS).
- The Gateway consolidates several legacy programs and helps in the decommissioning of CA$HLINK II.
- The Credit Gateway is being implemented in multiple phases over the course of two years. Current legacy collection systems are being migrated one at a time to the new Gateway. Migrations so far have included the Fedwire Deposit System (FDS) and the Remittance Express (REX) applications. The Federal Reserve Electronic Tax Application (FR-ETA) has also migrated, under specially branded Credit Gateway functionality called the Federal Tax Application.
- Future migrations will include FMS's electronic lockboxes and ACH credit collections associated with the Electronic Federal Tax Payment System EFTPS. FMS will make every attempt to minimize impacts to agencies and external customers during these migrations.

OTCnet

- OTCnet is the Treasury/FMS solution to one stop shopping for all the Over the Counter (OTC) deposits. OTCnet combines the functionality of TGAnet and PCC OTC providing one system for making check and cash deposits.
- The CASHLINK II system will be phased out as part of the Collections and Cash Management Modernization initiative that will transform the government's infrastructure for revenue collection. With the phasing out of CASHLINK II, all agencies with OTC deposits to commercial banks and Federal Reserve Banks must report them electronically in OTCnet.

Transaction Reporting System

- TRS is a collections reporting tool, supplying the latest information on deposits and detail of collections transactions to federal agencies. The system will allow financial transaction information from all collections systems and settlement mechanisms to be exchanged in a single system.
- TRS is a key component of the Collections and Cash Management Modernization (CCMM) initiative, a multi-year effort to simplify and modernize FMS's and the U.S. Treasury's collections and cash management programs.
- TRS is an FMS-wide transaction broker, data repository, and reporting solution. TRS will:
    - Provide a single touch-point for the exchange of all financial transactions across all collections systems
    - Offer a centralized repository containing detailed and summarized records of all revenue collections transactions processed by FMS systems
    - Facilitate Collections and Cash Management Modernization (CCMM)
    - Support reporting of classification information for the Government wide Accounting (GWA) Modernization initiative
    - Normalize financial transaction reporting and standardize the availability of financial information across all settlement mechanisms and collections systems.

3.1.6 Key Takeaways from the US Treasury Management Systems

- US is undertaking modernization of US Treasury Management Systems by developing single integrated application.
- Electronic payment of pension / benefits through a centralized application in lines of Electronic Transfer Account may be evaluated by O/o CGA.
- An ITS like system can be developed in India especially now that the RBI is developing its CBS. A standardized data exchange format can be developed between RBI and

Ministries requiring foreign exchange transactions. Ministries could this data exchange mechanism to directly place their foreign currency transfer requests with RBI through this system. This shall help in standardization of exchange rates across ministries and thereby result in cost saving to the government in terms of currency conversions.

- As a Transparency measure, possibility of developing a transaction monitoring / bill tracking module can be placed in the public domain in line with the PACER system that exists in the US.
- Cheque issue and clearance status is captured in Forms CAM 10 and CAM 11 COMPACT. The Government can evaluate providing the tracking of cheques in the public domain for the benefit of its vendors.
- For the Civil Ministries, Government may consider issuing a pre-paid card (in line with the Eagle Cash used in US) filled with foreign currency to officers going abroad on official tours / study leaves etc. This shall allow them to draw money in foreign countries using standard ATMs and hence, shall help the Government in limiting cash transaction of foreign currency and subsequent conversion loss.
- Like in the US, there is a need in India to develop a payment / collection gateway that can accept payment from through debit card, credit card and net-banking. This shall help the Government in minimizing the duplication of efforts by each ministry in developing a gateway separately. GePG can be developed into an aggregator which can be used for receiving monies due to Government Department. Also, this gateway can be used by Government Departments to pay / disburse various kinds of payments to implementing agencies / beneficiaries of Government Funds.

3.2 Overview of IT Systems Deployed at UK[2]

HM Treasury in the UK is using Combined Online Information System (COINS) which was introduced in 2005. The COINS data is used for:

- Fiscal management (e.g. Budget and Pre-Budget reports);
- Operational publications (e.g. Supply Estimates);
- Statistical publications (e.g. Public Expenditure Statistical Analyses, ONS/Treasury Public Sector Finances statistical bulletin, the National Accounts, etc); and
- Whole of Government Accounts.

Data are input into COINS by each central government department. Where an entity does not have on-line access to the system, the data provided by these entities are loaded centrally by the Treasury. In addition, the Treasury loads onto COINS the local government spending data provided by certain Whitehall departments and the Devolved Administrations. The Treasury also loads data relating to central funds (such as the Reserve) and other aggregates (e.g. central government debt interest) that are required for publications. Each entity is responsible for its own data and retains the ownership of the data in the system. The Treasury performs quality assurance at the level at which the data are included within publications.

Transaction level data or other specific items of expenditure are not available in COINS. Departments aggregate their transactions and map these to a list of accounts maintained by the Treasury. Departments can largely choose the level at which they aggregate their data, as long as at predefined levels the aggregates are correct. Departments' resource accounts are produced from departmental systems that record their individual transactions. The data in COINS are updated continuously. Departments have on-line access to the system and can make adjustments to the open parts of the system as required.

COINS is coming to the end of its expected life, demands on it are likely to increase, maintenance costs. Also, the level of manual reconciliation is increasing. In the light of this a new system - Online System for Central Accounting and Reporting (OSCAR) is being developed.

[2] Source:

- HM Treasury website, http://www.hm-treasury.gov.uk/
- Business Link, http://www.contractsfinder.businesslink.gov.uk/Common/View%20Notice.aspx?site=1000&lang=en&NoticeId=254713

OSCAR is expected to provide a reliable and efficient management information system holding consistent, accurate and timely public spending data that enables the Treasury to perform its key functions, while minimising reporting burdens on departments.

The key HM Treasury functions that OSCAR shall support are:

- Plan and control public spending – OSCAR shall hold departmental spending plans up to 5 years ahead, including an audit trail of changes to these plans from the spending review onwards. It shall then capture monthly in-year spending forecasts that can be used to control spending against the agreed plans, and also outturns/actual to understand the impact of spending against key fiscal aggregates and for Whole of Government Accounts purposes;
- Analyse and report on public spending – OSCAR shall support the analysis of public spending against multiple frameworks (currently resource accounting, budgeting and National Accounts) in order to seek parliamentary approval for spending and to report public expenditure statistics over a period of up to 11 years (5 outturn years, current year, and up to 5 plans years). For certain outputs, data for all years shall be maintained against current definitions and against the current structure of government departments. OSCAR shall also be capable of producing print ready outputs for key publications;
- Challenge and support departmental spending decisions in a way that adds value – OSCAR shall provide HM Treasury with access to accurate, timely and meaningful data that can be interrogated to understand and question departmental spending decisions; and
- Drive greater transparency in public spending data – OSCAR shall hold data that is reported on a consistent basis by all departments, and which is meaningful and user-friendly for internal and public scrutiny.

The data on OSCAR shall largely be non-transactional aggregate public spending data, which shall not necessarily be subject to standard double entry. This shall generally be based on transactional accounting data held on departments internal accounting systems, which shall be captured using standard double entry. The OSCAR solution shall allow the completion of core business processes, which are expected to include the following:

- Budgeting Plans – to record annual spending plans agreed at a Spending Review.
- Budgeting Outturn – to record final annual outturn (actual) at the end of the financial year.
- Budgeting Adjustment – to amend agreed plans or update prior year budgeting outturn.
- (Budgeting) Forecast Outturn – to capture actual/expected monthly in-year spending.

- (Budgeting) Publications – to present budgeting data in the format required for various publications.
- Whole of Government Accounts – to produce a set of consolidated accounts for the public sector.

3.2.1 Solution Overview

The core Project OSCAR solution shall be delivered using a single, integrated, intuitive and easy to use COGNOS toolset. The OSCAR system shall provide three main capabilities:

1 Data gathering – the ability to accept user data (budgets, forecasts and actual) in the form of files or manual inputs, allow aggregation, allocation and versioning as well as workflow and data validation as stipulated in the requirements. This shall be enabled by the use of IBM COGNOS Enterprise Planning, IBM COGNOS TM1 and IBM QualityStage.

2 Consolidation – the ability to merge and aggregate financial data using consolidation functionality such as intercompany eliminations. This shall be enabled by IBM COGNOS Controller.

3 Reporting – the ability to aggregate the data supplied by Authorised Users and present it in the form of formatted reports, ad-hoc analysis, what if scenarios, dashboards and other reporting needs. This shall be enabled by the use of IBM COGNOS BI (including, IBM COGNOS BI Statistics, IBM COGNOS Analytics Server and using the flexible analysis feature of IBM COGNOS TM1.Apart from these core functions, the solution shall also adhere to best practices such as:

    1 Data Warehouse – to store and present a single version of the data which has the flexibility to present views as per slowly changing dimensions. This shall be enabled by IBM DB2.

    2 Reference Data Management – to provide consistency between dimensions across the products in the solution. This shall be enabled by IBM COGNOS Business Viewpoint.

    3 Data extraction, Cleaning and Loading – to be able to extract data from source systems and feed it into the solution in an integral fashion with the ability to clean source data. This shall be enabled by IBM InfoSphere QualityStage.

    4 Testing software – to automate testing processes around systems test, performance test and enable its use for subsequent testing purposes such as regression test. This shall be enabled by IBM Rational Functional Tester, IBM Rational Performance Tester, IBM Rational Quality Manager and IBM Rational Performance Test Pack.

5 System Administration tools – to enable the system to be maintained in a manner that allows ease of user maintenance, system security and automation of scheduled tasks, including data loading and housekeeping. This shall be enabled using IBM Lotus Domino Utility Server and IBM Cognos 10 BI.

3.2.2 Key Takeaways from OSCAR

- The Government of UK is replacing COINS (equivalent of e-Lekha in India) with OSCAR. One of the draw backs of COINS was that it did not contain transaction level data and the level of data aggregation was the choice of the agency. Hence, this feature should be evaluated while developing future system of O/o CGA.
- The application that aggregates such data should also have the capability to generate various statements of accounts.
- There is a need to develop the aggregator of data as a single integrated application for efficient capture and analysis of a public expenditure data.
- The UK system has replaced COINS with COGNOS which is a COTS application and fulfils the need of user defined reports which has been enabled through the use of COGNOS Business Intelligence. Hence, while developing a future system requirement of a Business Intelligence tools should be evaluated.

3.3 Overview of System Deployed at Brazil[3]

The Integrated System of Federal Government Financial Administration (SIAFI) is the primary tool used by the government for budget and financial management. It is a transactional system that automates budget execution, financial planning and accounting processes of the Brazilian Federal Government.

SIAFI has gained international recognitions as a system for public financial management and served as the model for construction of similar systems.

The key characteristic of the SIAFI system is the automation of the accounting process based in the structuring of the information in the budget execution process.

This approach used by the SIAFI system guarantees that the budget and accounting information are permanently matched, The financial statement is automatically generated, and all financial transactions are accessible by the executive, legislature, internal audit, external audit, and the society via internet/website.

The primary functionalities of SIAFI are as under:

- Recording, monitoring and control of budget execution
- Management of receipts and payments through Treasury Single Account (TSA)
- Financial control and accounting of Federal budget
- Preparation of financial statements

Over a period of time, the system has been augmented with functions for planning and budgeting, managerial control and is linked to other centralized government systems (personnel, etc.). Some of these modules compete with systems from other ministries such as budgeting system from the Ministry of Planning.

The SIAFI System is used by or has interfaces with the following government bodies:

- Federal Revenue Secretariat
- Central Bank
- Federal Budget Secretariat
- All federal government units (Executive, Legislative and Judiciary branches), including all Dependent State-owned Companies, must use SIAFI.

[3] Source http://www.tesouro.fazenda.gov.br/english/siafi/index.asp
http://www.wiley.com/college/turban2e/icase4.html

- Independent State-owned Companies and by entities not pertaining to the Public
- Administration that have celebrated a Technical Cooperation Agreement (TCT, in Portuguese) with the Treasury
- SIAFI is also used by Brazilian units from Ministry of Defense, located at Washington and London

3.3.1 Functional description of SIAFI

Function	Description
Budgetary Allocation – Approval of the budget and allocation to the specific government unit	• SIAFI facilitates the double entry bookkeeping for approved budgetary credit and allocated budgetary credit for the specific government unit
Budget Commitment - When contracting, the unit must commit some of its budgetary credit, making it unavailable for a new use	• SIAFI facilitates the double entry bookkeeping for available budgetary credit committed for expenditure
Expenditure Acceptance- When activities, transactions, or other events occur that create the unconditional obligation of general government units to make payments or otherwise give up resources.	• SIAFI facilitates the double entry bookkeeping for expenditure acceptance
Payment - delivery of money **to a u**nion **creditor**	• SIAFI facilitates the double entry bookkeeping for payments

3.3.2 Technical Details

SIAFI presently runs on an IBM 9021/962 mainframe machines based on client server architecture. The network uses around 2,000 leased data lines. There are around 33 subsystems and 130 modules.

3.3.3 Key Takeaways from SIAFI

- SIAFI has a robust bank reconciliation system which allows close monitoring of suspense and advance accounts. This feature of SIAFI may be considered while defining the new IT System for O/o CGA.

- SIAFI provides a central system for monitoring all accounts payable of the Central Government, and regularly reports amounts carried over between fiscal years. Such feature should be evaluated in the future IT System for O/o CGA.
- All accounting transactions are recorded in SIAFI and have strong inbuilt controls which play an important role in ensuring that expenditure commitments are only undertaken within the limits established by the budget and financial programming decrees. This feature is important for any future IT Systems for the O/o CGA as the current IT systems lack this feature which results in over / under expenditure in some cases.
- Accounting transactions in SIAFI are updated in real time, enabling the reconciliation of government accounting records with its accounts on a daily basis. This feature is critical for a future system for Government of India as this shall allow accurate generation of flash figures.
- The Budget division in Ministry of Finance also uses SIAFI thereby, making it possible to generate budget execution report with desired level of details at any point in time. Hence, the proposed system in India should have Budget division as a stakeholder in the system. This shall facilitate better budget execution and budget control.

3.4 Overview of IT Systems at the Ministry of Finance, United Arab Emirates[4]

The UAE Ministry of Finance needed to replace its legacy system to provide efficient reporting that would enable the government to make more accurate fiscal decisions for the country. In addition, the Ministry wished to standardize financial reporting for its 20 federal ministries and more than 25 autonomous agencies. Some of the key challenges that the ministry faced are given below:

- Replacing the ministry's system to accommodate new developments and provide the speed, accuracy and efficiency required by the ministry.
- Standardizing the federal government's financial database and generate financial reports – such as balance sheet and final accounts – from a single source.
- Automating the federal government's budgeting processes – from preparation to approval- across all ministries and agencies, as well as exercise budgetary control over expenditures.
- Providing timely and accurate financial information for statutory reporting requirements and decision making.
- ligning and improving financial processes to achieve the ministry's vision and objectives.

The ministry established an integrated financial management system (IFMS) using Oracle E-Business Suite. With the implementation, the ministry enabled financial data extraction from a single source and enhanced its reporting capabilities for internal ministry stakeholders and international agencies. The specific Oracle solutions implemented by the minsitry are given below:

Oracle E-Business Suite: To establish and IFMS that standardizes the federal governement's financial management in line with international procedures, extracts all financial data from a single source, and substantially enhances its reporting capabilities.

Oracle Hyperion Planning: To apply zero based budgeting methodology – calculating budgets from scratch and covering areas, such as expenditure and revenue planning, budgeting for employees, and capital asset planning – and improve forecast accuracy.

[4] Source: KPMG's interaction with Oracle

Oracle Cash Management: To decentralize account management in the federal ministries for recurring processes, such as cheque remittance and cashing.

With automated budgetary reporting capabilities, the ministry can now exercise greater control over expenditures and provide timely and accurate financial information to senior leadership to enhance fiscal and budgetary decision-making.

3.5 Overview of IT Systems - Department of Works and Pensions (DWP), London, United Kingdom[5]

In 2007, the Department of Works and Pensions was bestowed with the responsibility to operate shared services for its own divisions and other government departments. DWP chose to work with Oracle to streamline its financial, HR, and procurement services and to offer those services to other government departments. DWP Shared Services, the product implemented at DWP, was the first internal government supplier, in the UK, to provide a consolidated and integrated service to other government departments. This radical change provided better value for money, increased quality of service, improved effectiveness, integrated services, and forged collaborative working partnerships.

DWP Shared Services is underpinned by the Oracle E-Business Suite. The integrated system provides staff and line managers with greater access to and control over activities, such as staff pay, budget reports on spend against cost centers, and checking whether invoice payments have been made against purchase orders.

Implementing Oracle has helped the department in implementing the following:

1) **Integrated HR:** This drives consistency, streamlines services, and reduces costs. A single operation serving multiple customers helps to drive economies of scale. Employees are encouraged to use self-service options, such as Self Service HR, as much as possible, further reducing costs. Other queries are managed through contact centers, which handle all correspondence for DWP.

2) **Comprehensive Accounting:** DWP Shared Services offers a comprehensive accounting service, producing financial and management accounts. In 2009 and 2010, DWP commenced reporting under International Financial Reporting Standards (IFRS) and achieved all HM Treasury "trigger points", designed to help government departments make the transition to IFRS. Now, all accounts are filed on time. In addition to this, a key service also operated through the DWP Shared Service center is debt management.

3) **Centralized Procurement:** The Purchase-to-Pay (P2P) department processes and pays approximately one million invoices per annum for goods and services purchased

[5] Source: KPMG's interaction with Oracle

by DWP and other customers, such as the Cabinet Office and DfE. It now pays 95% of all invoices within 10 days. It also provides low- risk purchase order processing and administers the Government Procurement Card—a purchasing card used by the U.K. public sector to buy high volume, low value products in a cost-effective and process-efficient way. As part of the shared service offering for procurement, DWP and its customers are connected to the Zanzibar collaborative e-Marketplace. Zanzibar provides access to electronic supplier catalogs and collaborative procurement opportunities across the public sector and is an integral part of the Shared Services.procurement function. Zanzibar links seamlessly with Oracle EBusiness Suite P2P processes. The full solution enables DWP to act as a procurement hub that can potentially be rolled out to other government bodies not currently in DWP Shared Services.

3.6 Overview of IT Systems – Ministry of Finance, State of Israel

The Ministry of Finance at the State of Israel has implemented the IT solution provided by SAP to meet its financial management needs. The ministry has implemented the SAP for Public Sector Solution Portfolio, including the SAP ERP application; the SAP NetWeaver technology platform and the SAP Supplier Relationship Management application.
Initially the ministry was facing certain fundamental issues. These have been given below:

Challenges

- Disparate set of systems for each ministry,
- Lack of information transparency across organizations
- Redundant administrative efforts
- Financial accounting not accrual based
- No existing infrastructure for e-government

The Ministry of Finance, took up the exercise to install a comprehensive business platform across 25 ministries and 100 agencies to improve efficiency and lay the foundation for e-government services. One of the major assets of using the SAP development kit was that the software developers, who were proficient at Microsoft .NET technologies, could easily develop programs using the SAP Portal Development Kit (PDK) for Microsoft.NET. The SAP system provided a comprehensive business platform to cater to the public sector needs.

Key Highlights

- Comprehensive business platform for public sector
- Support for collaborative outcomes
- Superior functionality
- Best practices
- Vendor stability
- Proven ability to perform
- Lowest total cost of ownership
- Effective collaboration agencies
- Improved service responsiveness to public
- Elimination of 143 legacy systems
- 45% reduction in IT expenditures

Major Benefits of the SAP system

- Ability to capitalize on existing .NET assets
- Ability to quickly and easily create portal content, which can then be easily integrated into portal pages
- No need for recruitment or retraining resources
- Single unified view of data and applications
- Personalized portal for each individual executive or user
- Improved decision making within the capital markets department and other units in the Ministry of Finance

3.7 Overview of IT Systems – Ministry of Finance, Government of Catalonia, Spain[6]

The introduction of the Euro in 1999 and the inability of the government's software to handle the change provided the opportunity to evaluate new applications for supporting financial processes. The government chose the SAP ERP application as the common management software across all departments and public companies.

The government was facing the following challenges:

- Requirement to convert to new currency, the euro
- Need to integrate multiple, disparate accounting systems
- Inability to evolve financial management processes
- Need to improve under automated budgeting processes
- Difficulty in carrying out cross departmental initiatives

Key Benefits

- Comprehensive, integrated end-to end process support
- Robust, scalable functionality
- Strong support for financial and human resource management
- Well planned, carefully executed change management
- Gained deep visibility across entire organization
- Enabled dissemination of reports to diverse constituencies
- Integrated financial processes across departments
- Improved financial controls
- Eliminated manual processes
- Eliminated duplicate data entry
- Successfully integrated 15 departments and 50 public entities with comprehensive financial and accounting software.

[6] Source: KPMG's interaction with SAP

3.8 Overview of IT Systems – Ministry of Finance, Government of Singapore[7]

In 2005, several government agencies, in Singapore, announced plans to upgrade or replace their existing enterprise resource planning (ERP) systems independently. It became apparent to the Singapore Government that the existing model of "one system per agency" was not ideal. Information was often duplicated across systems and tasks were carried out inconsistently, resulting in waste and inefficiency. Hence, the Singapore Ministry of Finance launched its **Alliance for Corporate Excellence (ACE) program.** Under this initiative, the Ministry of Finance would consolidate the IT systems and operating environments 11 agencies used to manage their human resources, payroll, finance and procurement functions. These agencies were the Agri-Food and Veterinarian Authority of Singapore, the Economic Development Board, International Enterprise Singapore, the Inland Revenue Authority of Singapore, the Intellectual Property Office of Singapore, the National Heritage Board, the National Parks Board, the People's Association, the Public Utilities Board, the Singapore Land Authority and the Science Centre Board. This move made sense given the similarities in administrative procedures across these agencies. In addition, the Government would drive efficiency gains and cut costs by sharing IT services and best practices, and improving reporting.

The Ministry of Finance engaged **Accenture to deploy** a standard ERP system for the 11 agencies. Following Accenture's assessment, the Ministry of Finance selected the highly scalable and reliable **SAP ECC 6.0 integrated application suite**, running on Microsoft Windows Server and a Microsoft SQL Server database. ACE supports key human resources, finance and procurement functions across 11 agencies, so the reliability and availability of the system have a direct impact on operational efficiency.

During the project, Accenture was the primary system integrator and was responsible for the overall program management. The application suite was rolled out to around 12,000 users across the 11 agencies between October 2009 and April 2010. Accenture provided transition support, especially for users migrating to the new system from a non-SAP environment. Accenture will manage the system until 2016, providing helpdesk support, application maintenance and conducting annual reviews to ensure the system continues to run smoothly and meets key performance indicators.

[7] Source: KPMG's interaction with SAP

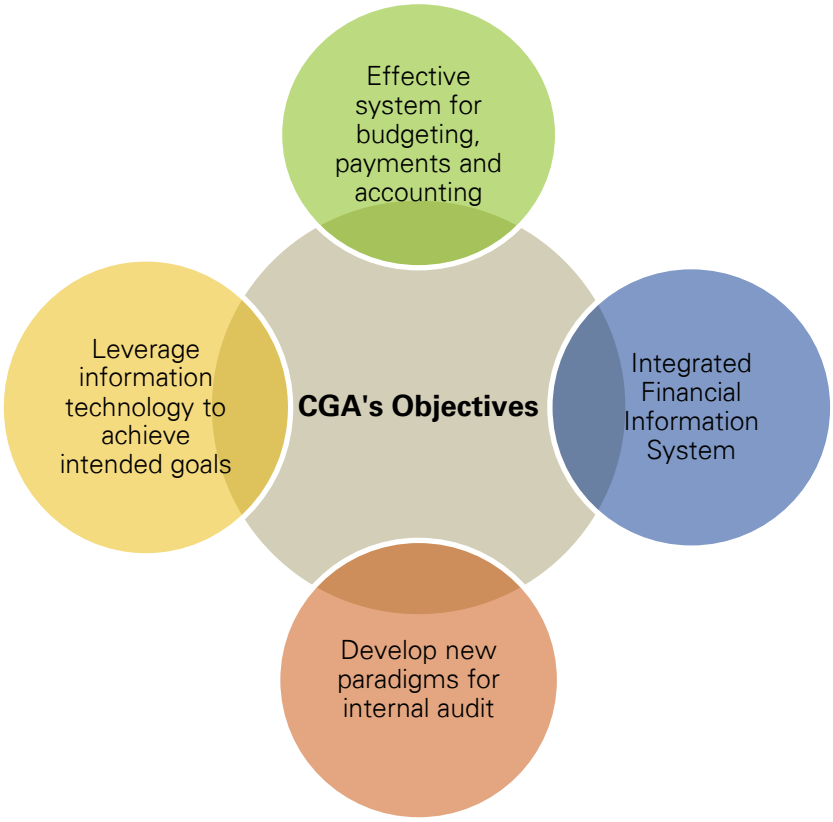
The Ministry of Finance and the participating agencies are achieving true high performance by using this integrated SAP system to drive operational efficiencies, reduce redundancy and waste, and improve the speed and quality of reporting. The success of the initiative has demonstrated how a shared ERP system can drive efficiencies in government. In August 2010, the project received the prestigious MIS Asia IT Excellence Award in recognition of its achievements. From August 2011 to January 2012, the shared system serving 11 agencies was further extended to another 4 agencies. They are Info-communications Development Authority of Singapore, National Environment Agency, National Council of Social Service and Singapore Sports Council. There are currently 15 agencies on the shared system with more than 17,000 users.

4 Business – IT Alignment

4.1 IT Strategy Aligned with Organizational Goals and Mandate

The CGA's vision is to strengthen governance by excelling in public financial management. Further to this, one of the mission statements of the CGA clearly mentions the leveraging of information technology to achieve CGA's mandate. This strategy has been developed following a widespread consultation and individual interviews with various stakeholders of the CGA.

The aims and objectives of the CGA which have been discussed in detail in the Assessment Report have been summarized in the diagram below:



Further to the CGA's Vision and Mission, the recommendations of the Technology Advisory Group for Unique Projects (TAGUP) and the 14th Report of the Second Administrative Reforms Commission (ARC) were also studied for developing the IT strategy.

The TAGUP report specifically mentions the salient features of an Expenditure Information Network. The table below summarizes these features and also depicts how the IT strategy takes into account these features by implemening a centralized system that provides interfaces with banks and external entities, has an expenditure control mechanism, uses

business intelligence tools for reporting purposes, and provides a web-based information portal for greater transparency to the citizens.

Salient Features of EIN	Corresponding Features of the proposed IT system
▪EIN should handle the information flow through the Central Expenditure Repository (CER)	Centralized System
▪Banks should report the details of disbursals to EIN for reconciliation purposes	Interface with Banks
▪EIN should track all authorizations and forward electronic instructions to banks	
▪ PAOs should be able to view the payment authorizations marked in EIN and release funds to spending agencies	Expenditure Control
▪Program Divisions at various ministries should be able to set first leg of fund flow transaction (allocation of funds to parent agency).	
▪Ministries, departments, state agencies, planning commission etc. should have access to EIN with appropriate access controls	Connectivity to External Entities
▪For greater transparency, citizens should also have access to a transparency portal	Information Portal
▪EIN should have a proper reporting mechanism with near real time availability of information.	BI Tool

The 14th Report of the Second Administrative Reforms Commission (ARC) mentions Development of a Financial Information System that helps in[8]:

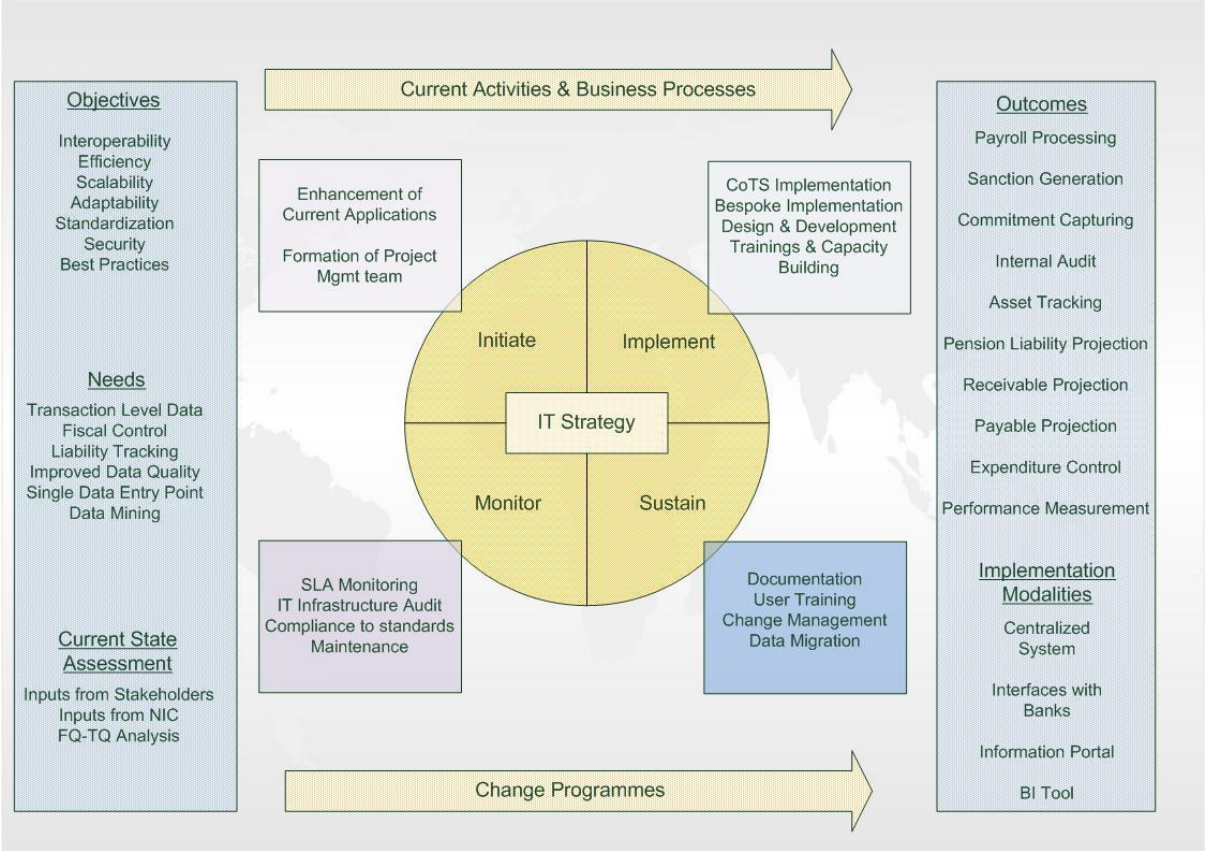
- Providing timely and reliable information to the decision makers
- Providing inputs to control systems
- Monitoring financial and physical progress
- Ensuring proper utilization of resources

Further, the report recommends that "A robust financial information system, on the lines of SIAFI of Brazil,needs to be created in the government in a time bound manner. This system should also make accessible to the public, real time data on government expenditure at all levels".

A diagrammatic representation of the IT strategy that emerged after the current state assesment has been shown in the figure below. The inputs from the various stakeholders

[8] Source: Strengthening Financial Management Systems, 2009, Second Administrative Reforms Commission, Fourteenth Report

and KPMG's analysis gave a clear understanding of the needs and objectives of the future IT system for the CGA. Considering the requirements of interoperability, efficiency, scalability etc., and the ability of the IT system to provide transaction level data, fiscal control, improved data quality, single data entry point, data mining etc., the IT strategy was devised. The IT strategy, once implemented, aims to yield several outcomes from the IT system. Some of these are: (1)Payroll Processing (2) Sanction Generation (3) Commitment Capturing (4) Internal Audit (5) Asset Tracking (6) Pension Liability Projection (7) Receivable Projection (8) Payable Projection (9) Expenditure Control (10) Performance Management etc.



4.2 Critical Factors for Architecture Design

The technical architecture for the proposed IT system should be designed based on the understanding of the business model and envisaged requirements. The following are the factors that need to be considered in order to develop a robust and technically efficient system:

Scalability – The conceptual application architecture should be scalable to meet the future demands of the business. However, careful consideration should be taken to create a balance between a conceptual application architecture that meets the current business

requirements in a cost effective manner and also scales to meet the longer term business requirements in a cost effective manner. In many situations, what is cost effective in the short term may not be in the long term and vice versa. The organization of the CGA is widespread; there are some PAOs, such as those at the CRPF and the BSF where the workload on the IT system is much greater than certain other PAOs. Thus, the scalability of the IT system should be a major consideration during the design phase.

Availability – The system availability requirements will impact the conceptual application architecture. For example, the current systems are not required to run 24 x 7 as of today, since the IMAS system that is implemented at the Indian Missions abroad is not part of the integrated system; however, there should be scope of the availability of the proposed future system to be available 24 x 7.

Security – The security requirements of the conceptual application architecture are essential and must be considered from the initial development phases of the conceptual application architecture. There are several standards that are followed as part of best practices in implementing the security layer in the IT framework. Implementation of the security structure is discussed in detail in the following sections.

Maintainability – The maintainability and more importantly, the cost of maintaining the environment defined by the conceptual application architecture, is a key consideration. Thus, deploying applications that follow a consistent conceptual application architecture design, that allows for easy to deployment, monitoring and troubleshooting, becomes important.

Interoperability – The conceptual application architecture should work across various business scenarios and deployment situations. The application should able to work (accept, share and forward data) with other applications or systems or products without any special effort on the part of the end user.

Responsiveness – Keeping in the mind the widespread expanse of the organization of the CGA, and the excessive load on the servers at certain PAOs, such as BSF and CRPF, the response times of the application and/or the turnaround time of the output becomes an important aspect to consider before implementing any IT system.

Efficiency – The proposed system should utilize limited computing resources but at the same time have a high throughput (rate of processing of work).

Adaptability - Adaptability refers to the ability of the system be customised through tailoring activities by the users. It is extremely essential that any new system that is developed caters to the requirements of the users at the CGA and is also flexible during usage. For instance, there is a need to be able to generate customisable reports from the financial and accounting data.

Standardization – While developing any new system, standard best practices should be followed in order to achieve an efficient system.

4.3 Business Architecture

Business Architecture articulates the functional structure of an enterprise in terms of its

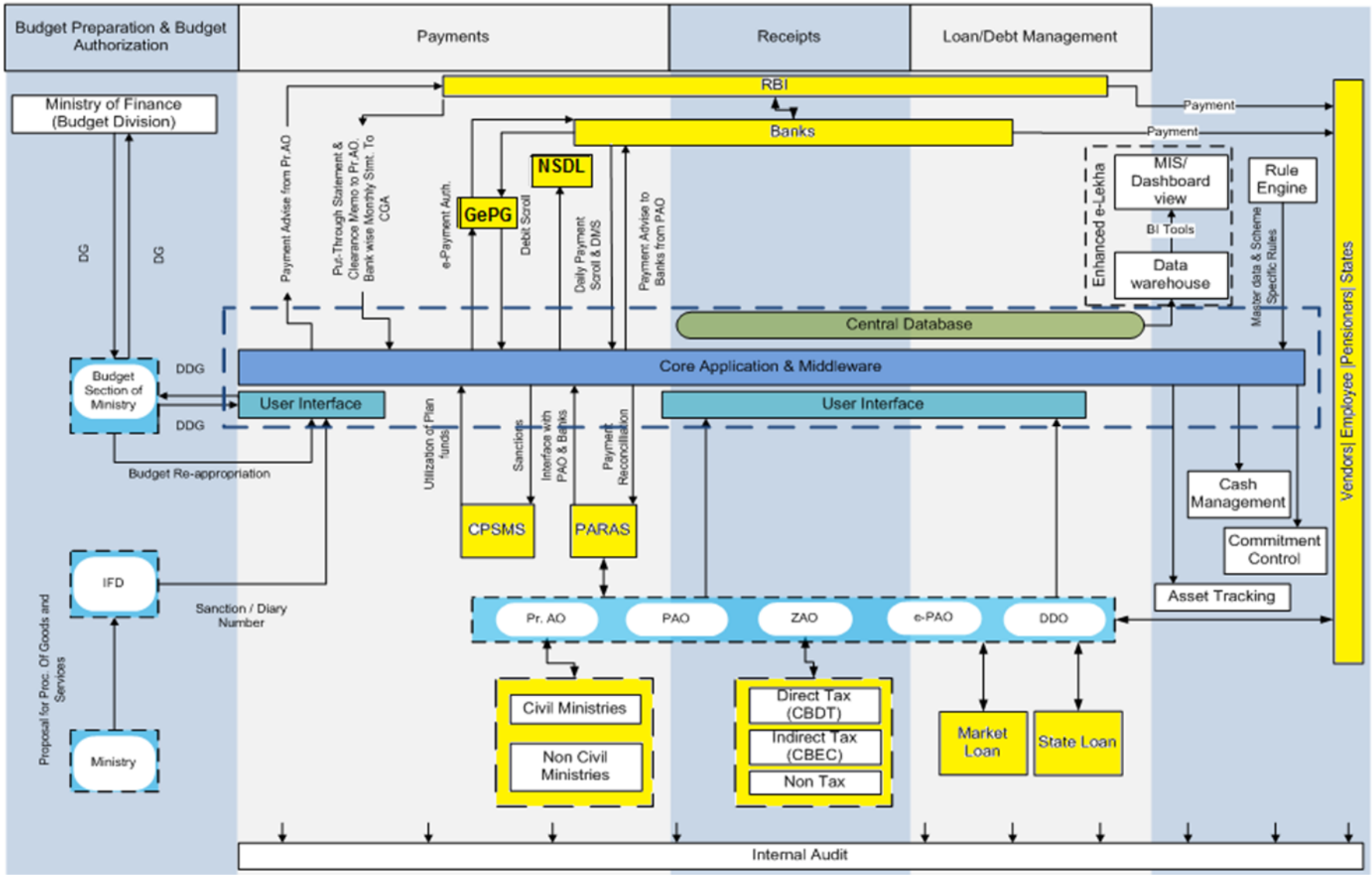
- Area of operation;
- Core business functions; and
- Services performed.

It depicts all stakeholders and is a precursor to subsequent architectures. The proposed business architecture view for CGA is derived from the existing functions performed by the organization both manually and with the help of IT systems.

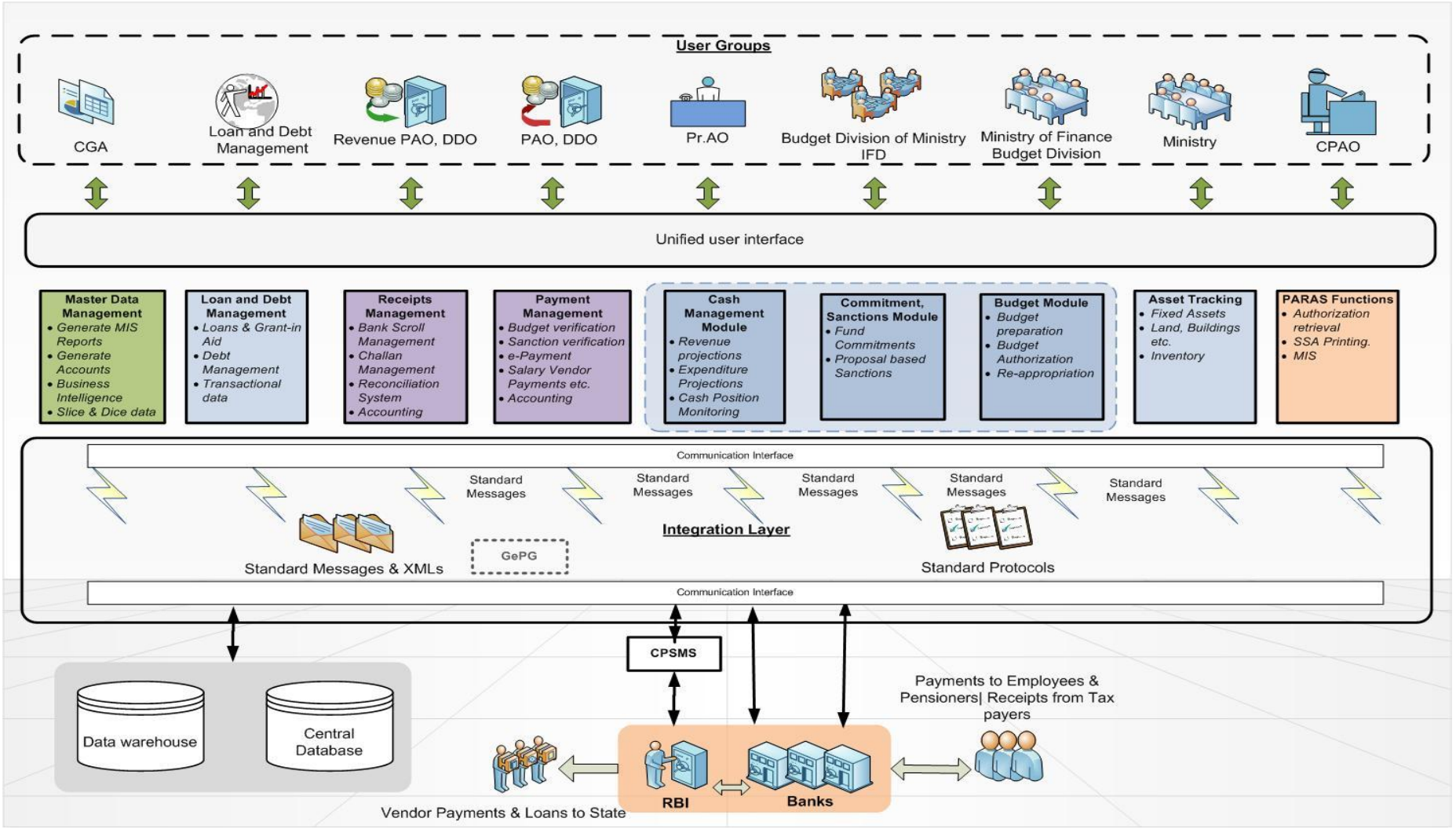
The proposed business architecture depicts broad business functions of CGA. These business functions further shows various stakeholders, existing IT systems and interlinkages between them.

In order to enhance the overall business functionality, it is proposed that the future system be a centralized solution, accessible to all stakeholders. This centralized solution shall cover the functionality of budget preparation and authorization, payment process, receipt process and loan and debt management. These functionalities shall be provided by applications/modules which will be part of the overall centralized solution.

The detailed functions of each of the application/modules, interfaces with other systems/stakeholders and data exchange requirements are covered as part of the proposed business architecture. The schematic below describes the proposed business architecture for CGA.


Budget Preparation & Budget Authorization
Payments
Receipts
Loan/Debt Management
RBI
Banks
Ministry of Finance (Budget Division)
Payment
Payment
NSDL
GePG
Payment Advise from Pr.AO
Put-Through Statement & Clearance Memo to Pr.AO. Bank wise Monthly Stmt. To CGA
e-Payment Auth.
Debit Scroll
Daily Payment Scroll & DMS
Payment Advise to Banks from PAO
Enhanced e-Lekha
MIS/ Dashboard view
BI Tools
Data warehouse
Rule Engine
Master data & Scheme Specific Rules
DG
DG
Central Database
Core Application & Middleware
Budget Section of Ministry
DDG
DDG
User Interface
User Interface
Budget Re-appropriation
Utilization of Plan funds
Sanctions
Interface with PAO & Banks
Payment Reconciliation
CPSMS
PARAS
Cash Management
Commitment Control
Asset Tracking
Vendors| Employee |Pensioners| States
IFD
Sanction / Diary Number
Pr. AO
PAO
ZAO
e-PAO
DDO
Proposal for Proc. Of Goods and Services
Ministry
Civil Ministries
Non Civil Ministries
Direct Tax (CBDT)
Indirect Tax (CBEC)
Non Tax
Market Loan
State Loan
Internal Audit

The figure below describes various applications of the centralized solution. These applications broadly cover following functionalities; detailed functionalities of the application are mentioned at section 4.7 scoping of IT systems:



Budget Preparation, Authorization, Commitment Control and Cash Management: It will facilitate the budget preparation process including preparation and submission of budget estimate, revised estimate, final estimate, supplementary grant, budget surrender, budget re-appropriation, budget authorization. Commitment control and cash management functionality will be derived by linking this application with other applications and entities such as CPSMS, rule engine/master module, RBI etc.

Payments Management: Budget data will be input to the payment management application. After incorporation of the budget data this application will facilitate processing and accounting of bills such as salary, vendor payments, loans and grant-in-aids etc.

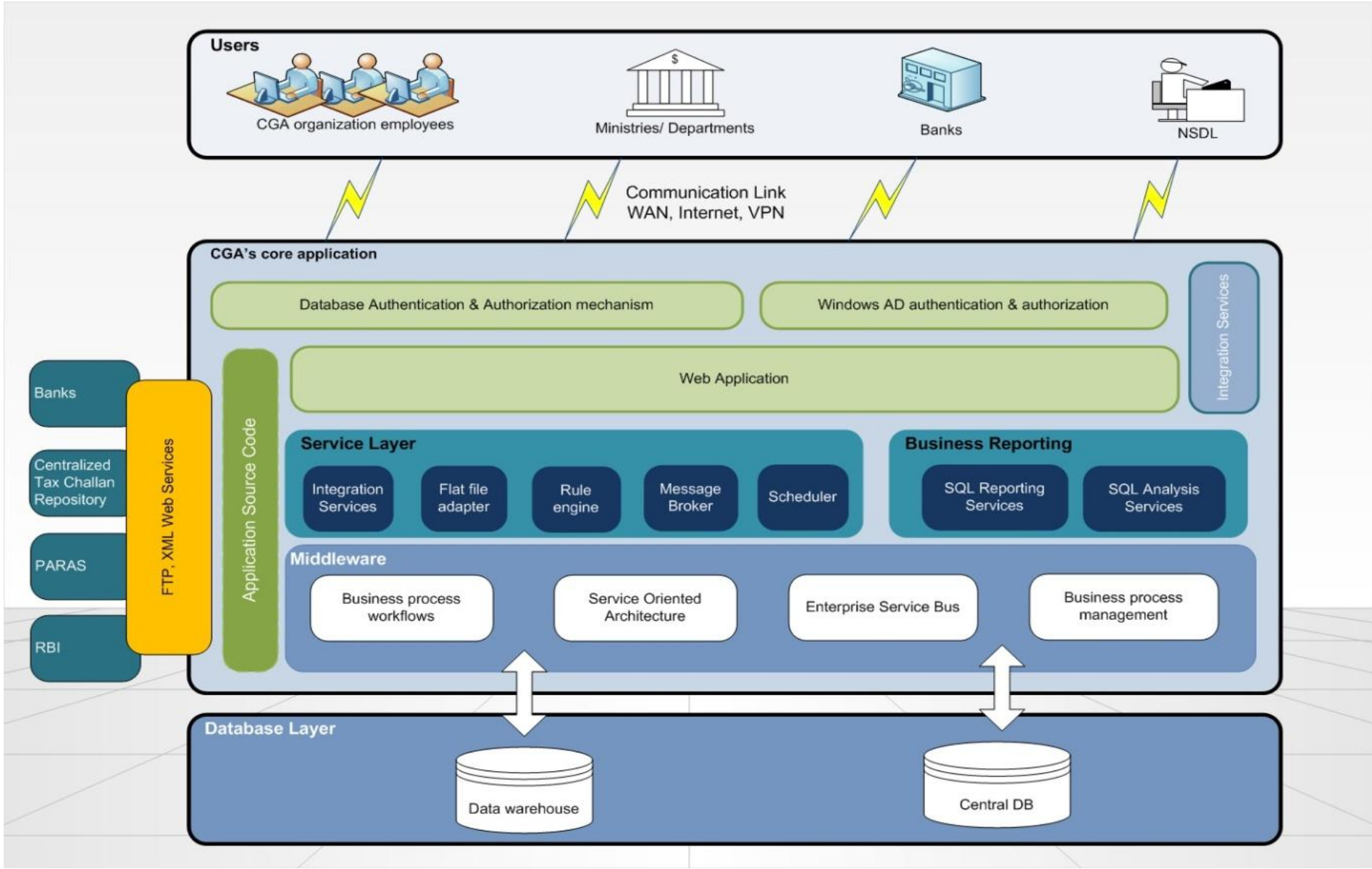
Receipts Management: This application will facilitate processing and accounting money received by the government from direct taxes, indirect taxes and non tax revenues.

Loan and Debt Management: It will facilitate disbursal of loans and grant-in-aids to state governments via various Ministries and state loan division of Ministry of Finance (MoF). It will also facilitate recording transactions related to market borrowing of the government.

Apart from these the proposed solution will also have **business intelligence tools**, **rule engine and** also covers the functionality of **internal audit**.

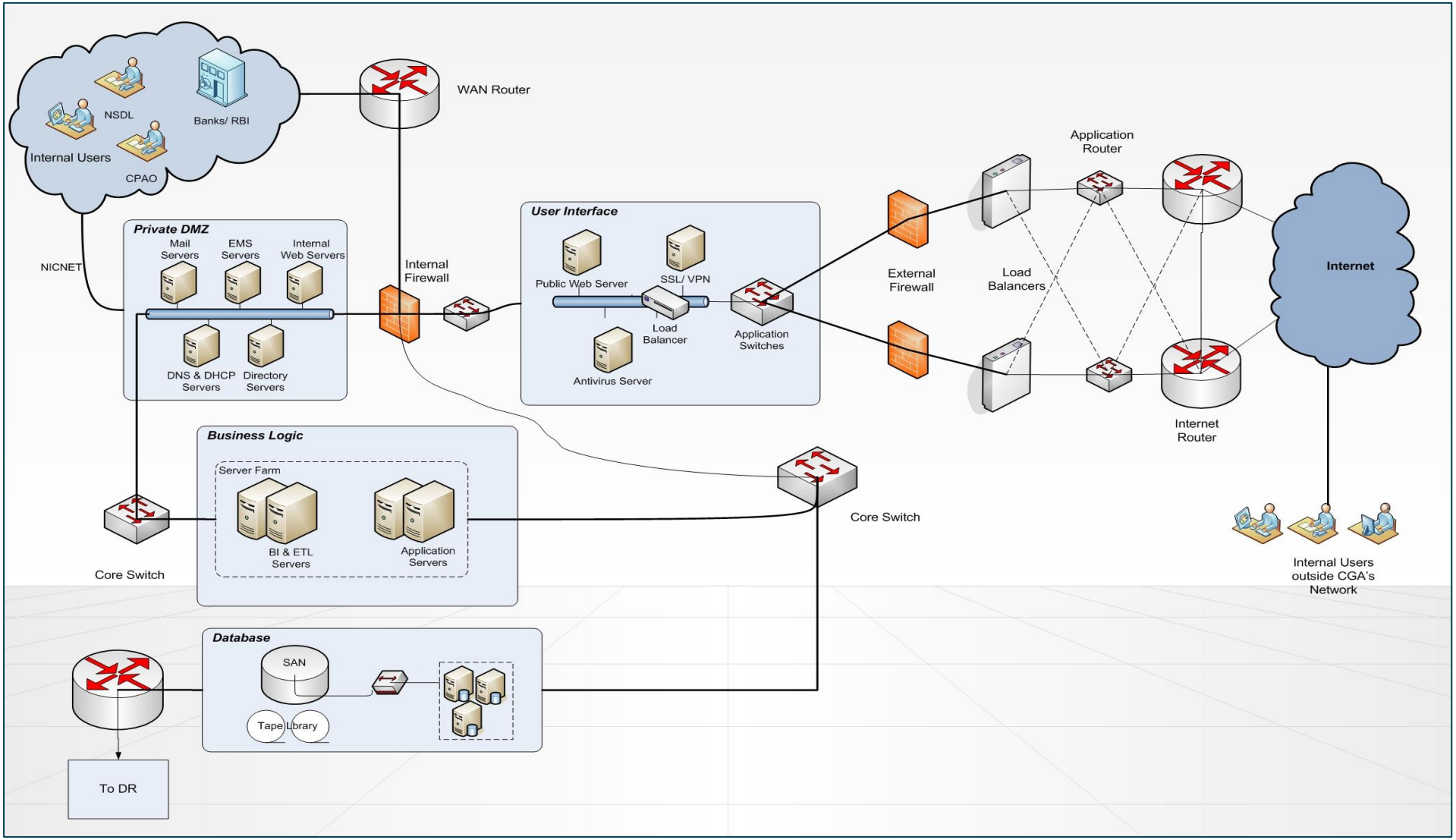
4.4 Technical Architecture

The application model below represents the conceptual view of the architecture for the proposed CGA IGFMS. The architecture shows a set of levels that provide enterprise-based services for a CGA IGFMS. These levels contain the elements that would be required by web based service application or system.


Users
CGA organization employees
Ministries/ Departments
Banks
NSDL
Communication Link
WAN, Internet, VPN
CGA's core application
Database Authentication & Authorization mechanism
Windows AD authentication & authorization
Integration Services
Web Application
Service Layer
Integration Services
Flat file adapter
Rule engine
Message Broker
Scheduler
Business Reporting
SQL Reporting Services
SQL Analysis Services
Middleware
Business process workflows
Service Oriented Architecture
Enterprise Service Bus
Business process management
Application Source Code
FTP, XML Web Services
Banks
Centralized Tax Challan Repository
PARAS
RBI
Database Layer
Data warehouse
Central DB

4.5 Deployment Architecture

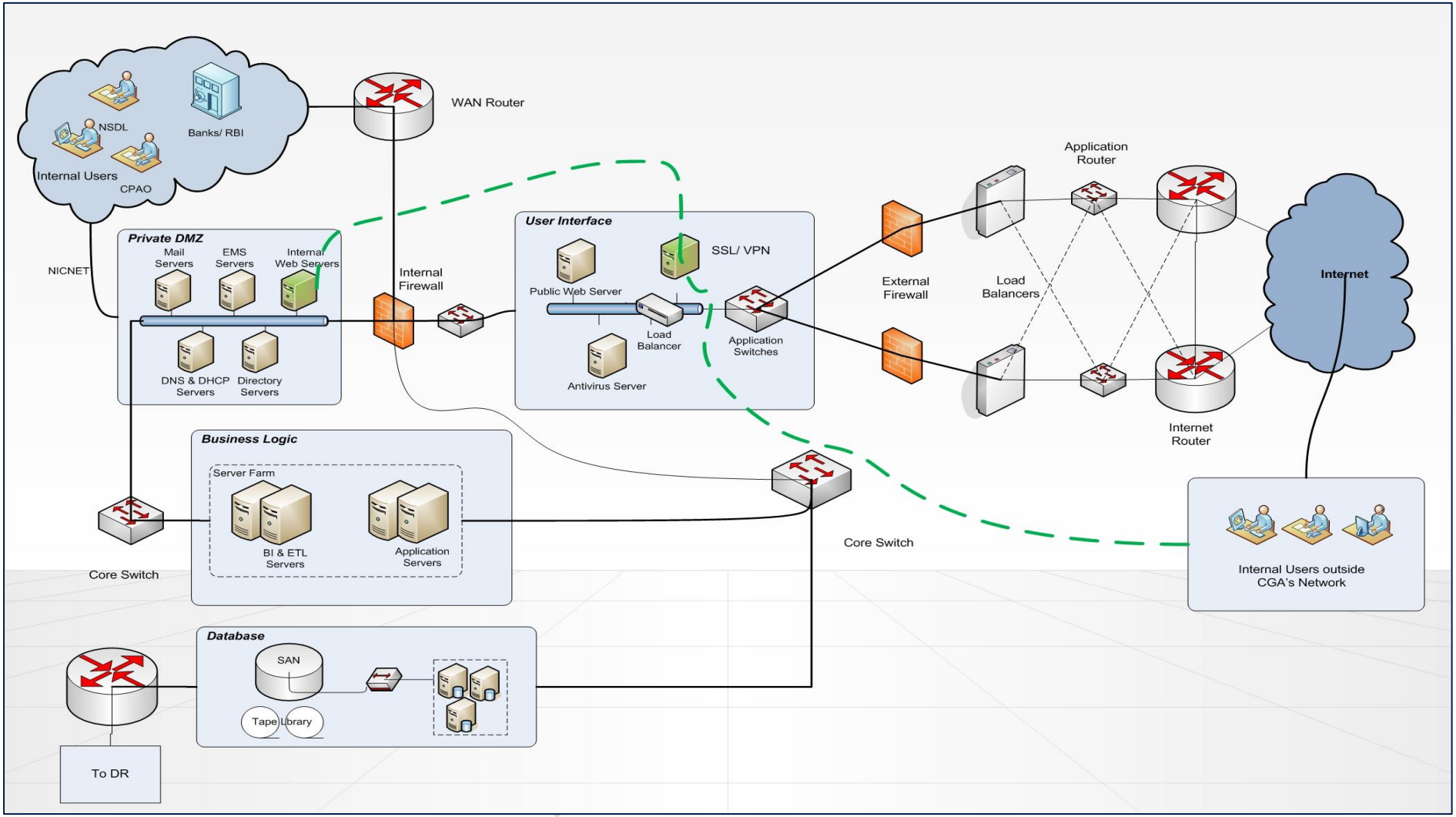
A centralized architecture" has been proposed for the CGA IGFMS application to ensure better manageability of the computer resources. Additionally, the Centralized Architecture offers an ease of technology upgrades as the patches released can be applied uniformly. The integration challenge between the various application and infrastructure components in a Centralized Architecture are much easier to deal with as the various components of the application are under single ownership. Also, in accordance with Business continuity Planning (BCP) best practises, A DR site has been proposed for the CGSA IGFMS application keeping in mind the criticality of the application to ensure an automatic failover and continuous operation of the system. This architecture envisages keeping a disaster recovery site, and carrying out regular disaster recovery drills to ensure DR preparedness.


NSDL
Banks/ RBI
Internal Users
CPAO
WAN Router
NICNET
Private DMZ
Mail Servers
EMS Servers
Internal Web Servers
DNS & DHCP Servers
Directory Servers
Internal Firewall
User Interface
Public Web Server
SSL/ VPN
Load Balancer
Antivirus Server
Application Switches
External Firewall
Application Router
Load Balancers
Internet
Internet Router
Internal Users outside CGA's Network
Business Logic
Server Farm
BI & ETL Servers
Application Servers
Core Switch
Core Switch
Database
SAN
Tape Library
To DR

User Interface / Presentation Layer

The user interface shall receive requests from CGA IGFMS users and send desired output by communicating with other modules. The various infrastructure components of this layer shall be hosted in the Demilitarized Zone (DMZ). The firewalls and intrusion prevention systems shall protect the application from malicious attacks or theft of data from hackers. Virus and worm attacks shall be defended with the anti-virus system. It is proposed that Load balancers be deployed to minimize response time and maximize throughput.

Users outside CGA's network shall be able to access the application through Internet. The public web server and the internal firewall (which is a part of the public DMZ) shall be configured to render only those application modules that are relevant to the user.


NSDL
Banks/ RBI
Internal Users
CPAO
WAN Router
NICNET
Private DMZ
Mail Servers
EMS Servers
Internal Web Servers
DNS & DHCP Servers
Directory Servers
Internal Firewall
User Interface
SSL/ VPN
Public Web Server
Load Balancer
Application Switches
Antivirus Server
External Firewall
Application Router
Load Balancers
Internet
Internet Router
Business Logic
Server Farm
BI & ETL Servers
Application Servers
Core Switch
Core Switch
Internal Users outside CGA's Network
Database
SAN
Tape Library
To DR

Business Logic Layer

The business logic layer in the proposed architecture shall control the application functionality by performing detailed processing as per defined rules and logic. It shall only be accessible through the User Interface layer. It is suggested that the server load balancers be deployed to minimize response time. It is recommended that a central information repository of all the data about schemes and agencies such as Banks, CPAO, NSDL etc. be formed. The central data repository shall consist of following components:

a) Data Staging

Staging area shall contain the data files from different source systems. This shall also act as a backup for the source system data. Data from the storage area shall then be loaded to appropriate data marts using ETL tool.

b) Data Warehouse and Data Marts

The data marts shall be appropriately designed keeping in mind the business requirement of various users groups and subject areas. The data shall then get loaded in data marts from source system after Extraction, Transformation and Loading (ETL). This shall ensure cleanse, consistent and consolidated data. Creation of data marts shall provide the basic foundation layer for creating a reporting and analysis framework consisting of standard, parameterized and ad-hoc reports as well as statistical analysis and data mining.

c) Data Integration Layer

An Extraction, Transformation and Load (ETL) tool shall be used to cleanse, transform and load data from various source systems to the central data warehouse. This is important because the data from various sources shall be required to be consolidated and matched to actually be able to track each financial transaction of the agency vis–a-vis bank transaction. Appropriate alerts shall be implemented for source data inconsistency.

The tool shall have the provision for native connectivity to extract data from all possible data sources like RDBMS, flat files and MS Excel (legacy data) keeping in mind the current and future data integration needs in mind.

Data Quality shall enable the users to seamlessly manage the quality of source information, as well as integrate information from complex, disparate data sources into one single, unified view. It shall address every phase of the data quality and data integration lifecycle including data profiling, cleansing, consolidation, enrichment, and monitoring.

d) Portals and Dashboards

As part of the project there shall be a secured, role-based portal that provides personalized interaction with information. Business users can access aggregated information via an easy-to-use Web-based dashboard. The portal shall provide seamless integration with data mining results in order to disseminate these across the enterprise.

e) Web Reporting

The web reporting shall provide users to quickly create basic queries and reports about the funding of schemes or agencies. Users shall view reports in a self-service manner while IT maintains control of the underlying data and security

f) Multi-Dimensional Analysis (OLAP)

The CGA IGFMS users shall be able to view and explore Online Analytical Processing (OLAP) data via the Web. This shall allow business users to look at data from multiple angles, view increasing levels of detail and add linked graphs and maps to gain greater insights into trends, exceptions and opportunities. The multidimensional reporting shall help analyze the allocation, release, expenditure of budget data across multiple dimensions.

Database Layer

The database layer shall manage and provide access to the CGA IGFMS data. A relational database management system shall be used to store data. To meet the increased demand of users a relational Database system has been proposed for scaling up the CGA IGFMS application. Some of the envisaged benefits of a Relational Database management system are extensibility, inheritance polymorphism, and encapsulation and database management systems.

4.6 Network Architecture

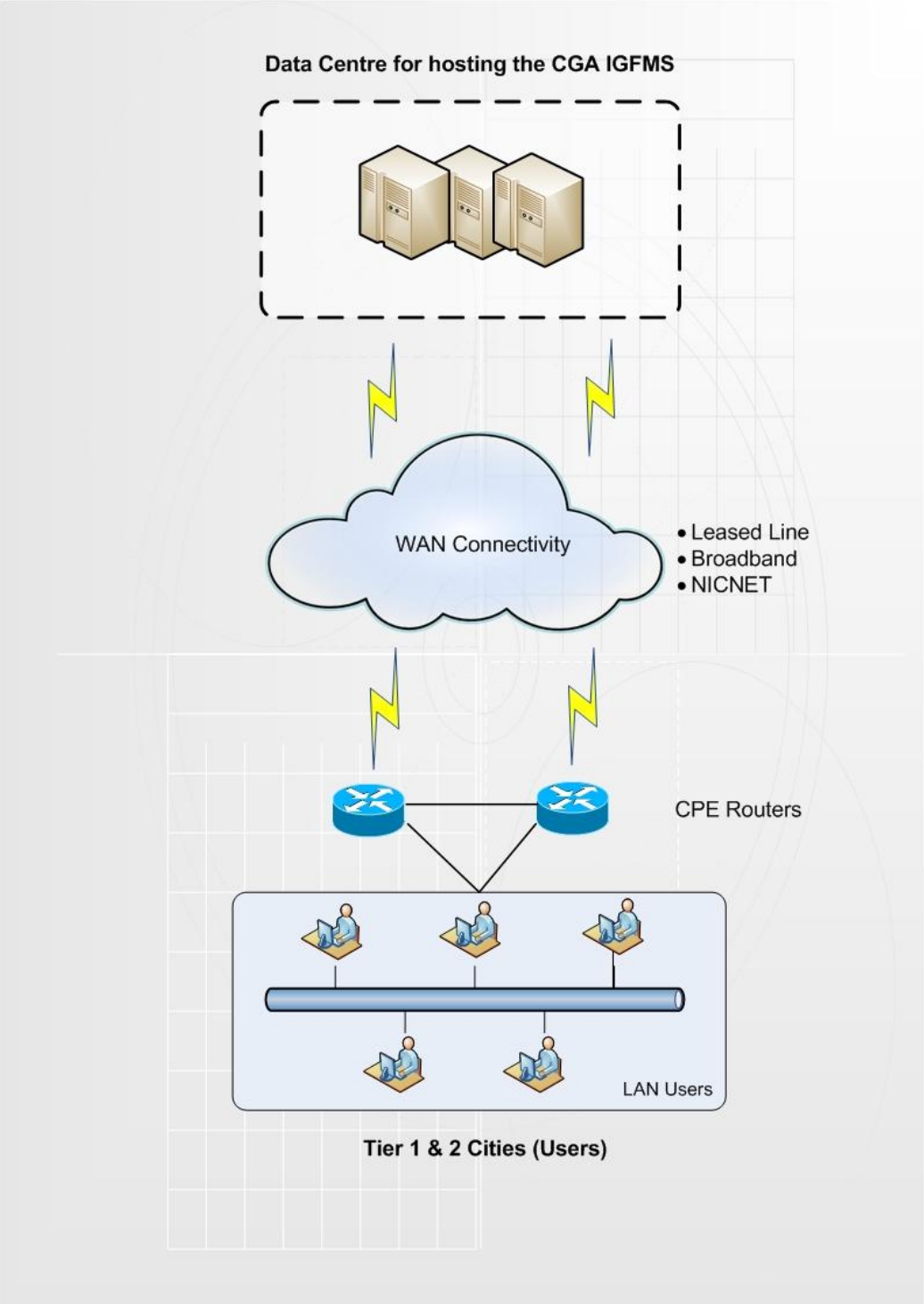
Network architecture, is the logical layout of the network that may be used for connecting the DDOs and PAOs for accessing the CGA IGFMS Application hosted at the Data Centre. The DDOs and PAOs office are located across India and abroad. These locations have been classified into the four categories based upon the network connectivity infrastructure that may be employed at these locations.

Connectivity Options for DDOs & PAOs

	Area Classification (List enclosed at Annexure 13.2.2)	No of DDOs	Percentage of Users	Connectivity Options				
				NICNET	Leased Line	Broadband	VSAT	BSNL WiMax
1	**Tier 1 Cities** *Metro cities, state capitals (excluding Jammu & Kashmir, North Eastern states and Islands)*	4487	53.01	✔	✔	✔		
2	**Tier 2 Cities** *Major cities which have fair connectivity options like presence of major Internet Service Providers and NICNET have been categorised as Tier 2 Cities*	1143	13.50	✔	✔	✔		
3	**Tier 3 Cities** *Cities and Towns which have limited connectivity options and are located at smaller district headquarters have been classified as Tier 3 Cities*	1337	15.79	✔	✔		✔	
4	**Remote locations** *Cities/towns in North Easters States (Assam, Manipur, Meghalaya, Tripura, Nagaland, Arunachal Pradesh, Mizoram, Sikkim), Jammu & Kashmir, Lakshadweep and Andaman & Nicobar Islands have been classified as remote locations.*	1120	13.23	✔			✔	✔
5	Outside India DDOs *DDOs in Mission Offices abroad*	213	2.52	Internet				
6	Un identified DDOs *Location not given in the master list*	165	1.95					
	Total DDOs	8465						

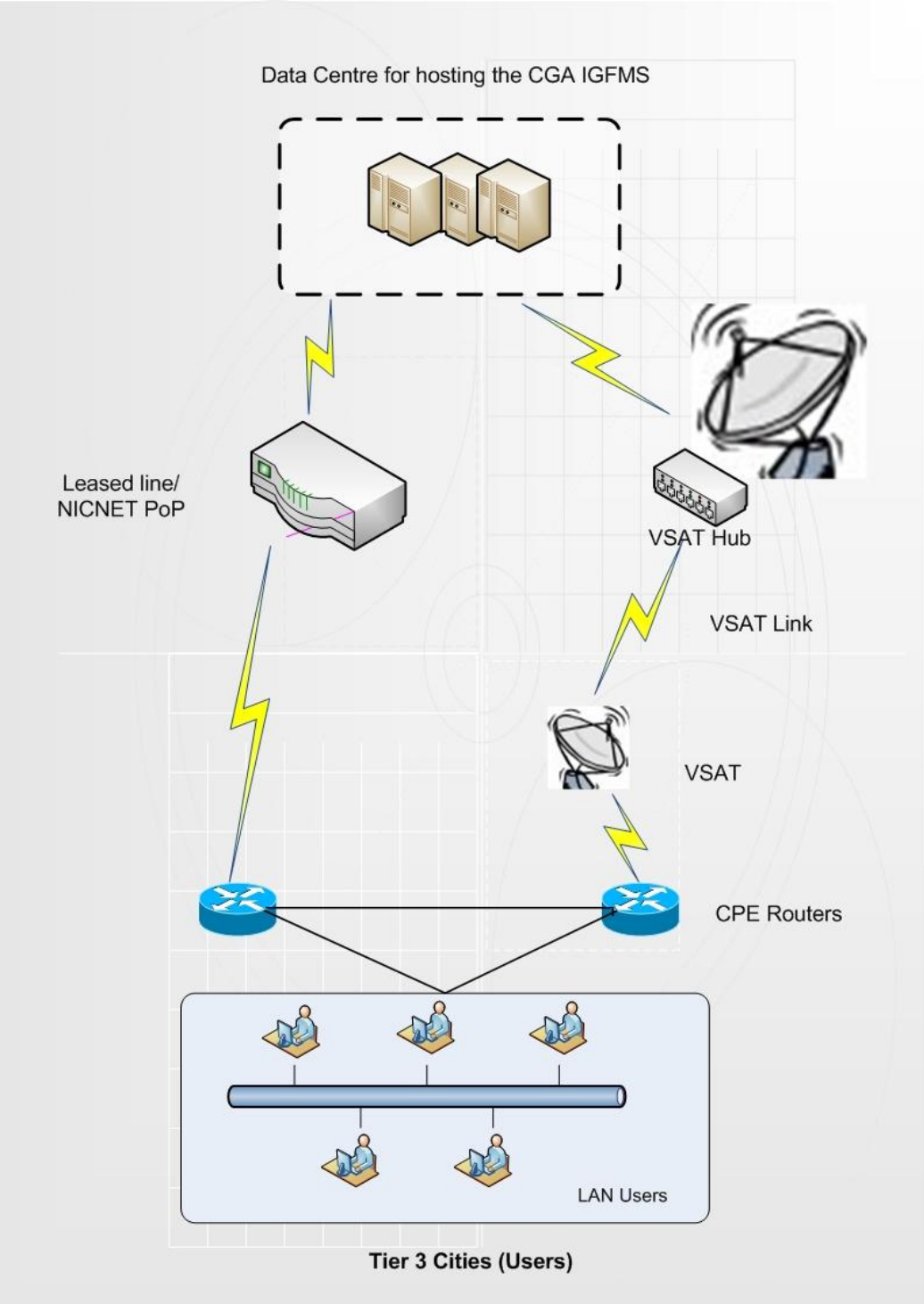
Network Architecture for Tier 1 & 2 Cities:

The network connectivity may be provided through Broadband, leased line or NICNET in these locations, which consists of Metro cities, state capitals (excluding Jammu & Kashmir, North Eastern states and Islands). Cities which have fair connectivity options like presence of major Internet Service Providers and NICNET have been categorised as Tier 2 Cities.



Network Architecture for Tier 3 city users:

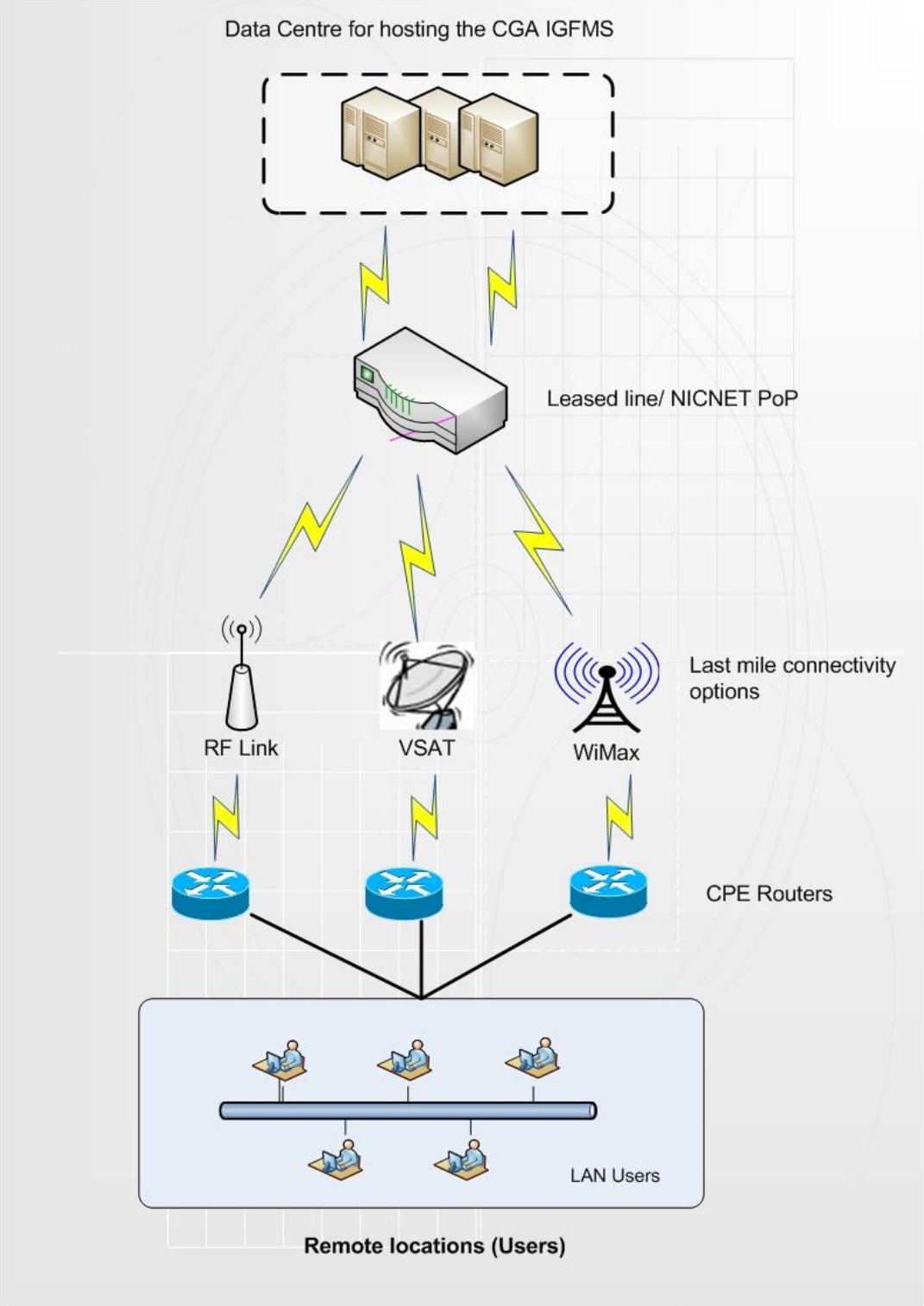
Cities and Towns which have limited connectivity options and are located at smaller district headquarters have been classified as Tier 3 Cities. Leased line of VSAT link may be used to provide connectivity in Tier 3 cities where the NICNET PoP is not present



Tier 3 Cities (Users)

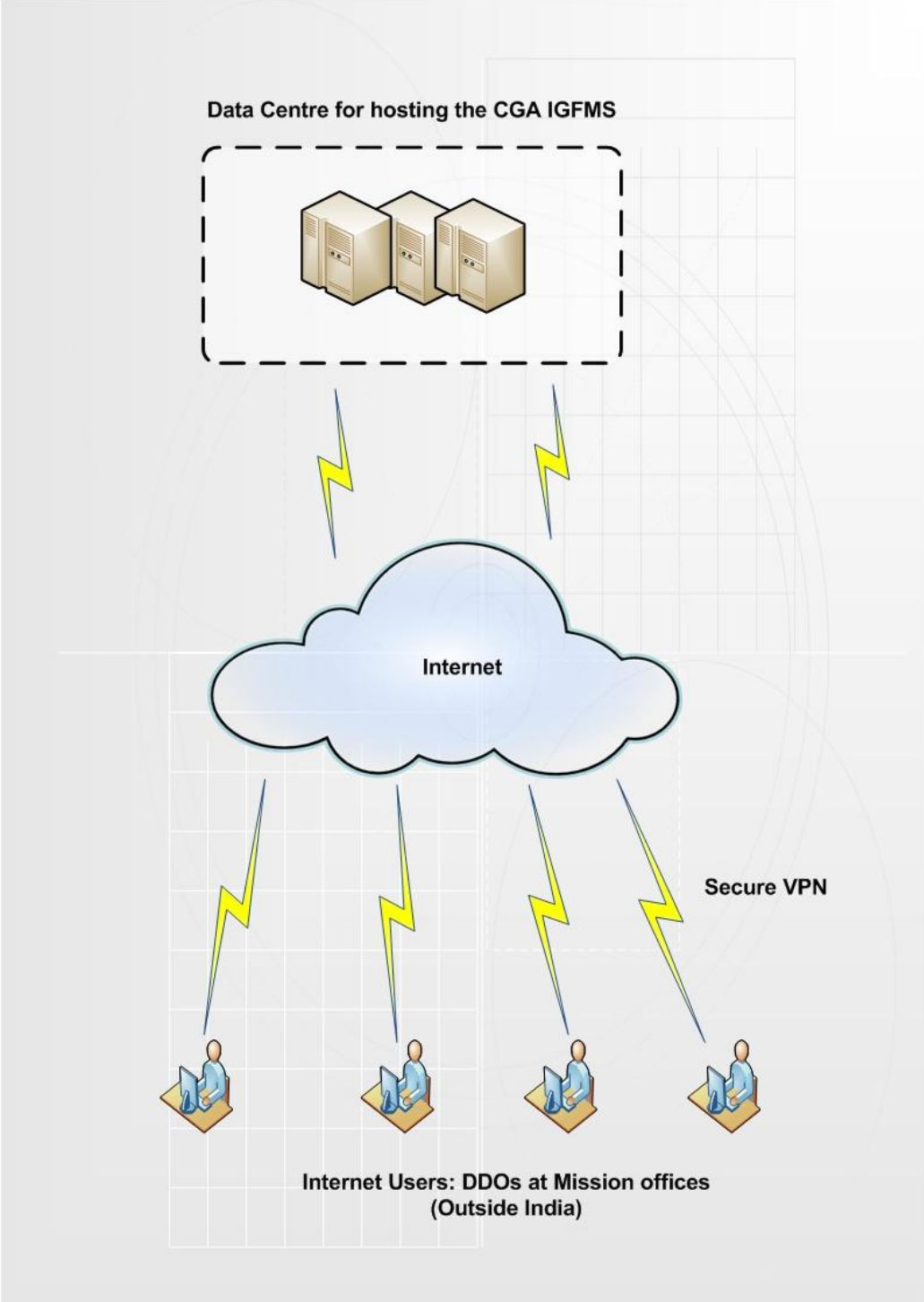
Network Architecture for Remote location users:

Cities in North Easters States (Assam, Manipur, Meghalaya, Tripura, Nagaland, Arunachal Pradesh, Mizoram, Sikkim), Jammu & Kashmir, Lakshadweep and Andaman & Nicobar Islands have been classified as remote locations. Connectivity options like RF link, VSAT or WiMax may be used to connect remotely located DDOs



Network Architecture for DDO outside India

DDOs at Mission offices outside India shall connect through internet via secure VPN Channel



4.7 Scoping of IT systems

The business architecture provides an overview of the overall system. It consists of four core applications for capturing the functionality of budget, payments, receipts and loan & debt management. In continuation to this, scoping of IT systems further elaborates the functions of the core applications, sub applications and modules, along with the interfaces and actors involved. Also, the information/data flow between different applications / entities is captured as part of the scoping of IT systems.

4.7.1 Master Application

It will contain Ministry specific master data pertaining to PAO/DDO master, employee master, vendor master. It will be a central repository/database accessible by different applications and modules.

S. No.	Application Function / Modules	Interface (if any)	Actors
1	**DDO Master** - Contain list of DDO codes	Budget, Payment, Receipts, loan and debt management Applications	Pr.AO, HoD of the Ministry / Department
2	**PAO Master** – Contain list of PAO codes	Budget, Payment, Receipts, loan and debt management Applications	Pr.AO, HoD of the Ministry / Department
3	**Budget Master/Code Master** – List of codes as defined by CGA, Ministries can open account heads after the 3rd tier, but as per the codes defined by CGA. After the implementation of new chart of accounts the budget master will be suitably augmented such that the changes are reflected in all linked applications/modules. This module can either be part of master application or it can be part of payment/revenue application, but in both the cases the budget master/code master but it has to be flexible to incorporate new chart of accounts as and when it is implemented	Budget, Payment, Receipts, loan and debt management Applications	Budget Section, Pr.AO
4	**Employee Master** - Employee details required	Payment - Salary	DDO and Pr.AO

S. No.	Application Function / Modules	Interface (if any)	Actors
	for payroll processing such as date of birth, date of joining, leave details, loan details etc. to be entered by DDO. Some of the entries such as Leave details, loan details etc. to be validated monthly b y DDO	Processing	(reporting/consolidate view)
5	**Vendor Master** – List of vendors to be entered by DDO, and vendor account validation (Vendor Name, Account Number, IFSC Code etc.) by bank	Payment, Banks	PAO, Pr.AO, DDO, Banks

4.7.2 Rule Engine

It will contain rules which will govern or override functionalities of all applications/modules in exceptional cases. The business rules in the rule engine can be defined at Pr.AO, HoD of the Ministry/Department level. Some on these rules (not limited to) are mentioned in the table below:

S. No.	Application Function / Modules	Interface (if any)	Actors
1	**Budget Control rules** – Rules related to controlling the utilization of budget, such as in the last quarter not more than 10-15% of the overall budget can be spend etc.	Budget, Payment, Receipts, loan and debt management Applications	Pr.AO, HoD of the Ministry / Department
2	**Expenditure control rules –** These will be rule related to specific type of payments, such as in case of Grant-in-Aids no TDS is deducted, such exceptions will be defined in the rule engine and it will be adhered by the payment management application.	Budget, Payment, Receipts, loan and debt management Applications	Pr.AO, HoD of the Ministry / Department

The rule engine can be a centralized application accessible by all other applications/modules if homogeneity in terms of technology platform is maintained during implementation of overall proposed solution, but if the proposed solution is a mix of bespoke and COTS applications then the rule engine functionality will be part of the specific application.

4.7.3 Application - Budget Preparation, Authorization, Commitment Control & Cash Management

This application will facilitate the automation of budget preparation process as required or in preview of the CGA. It contains three modules – Budget Preparation, Budget Authorization and commitment control and cash management.

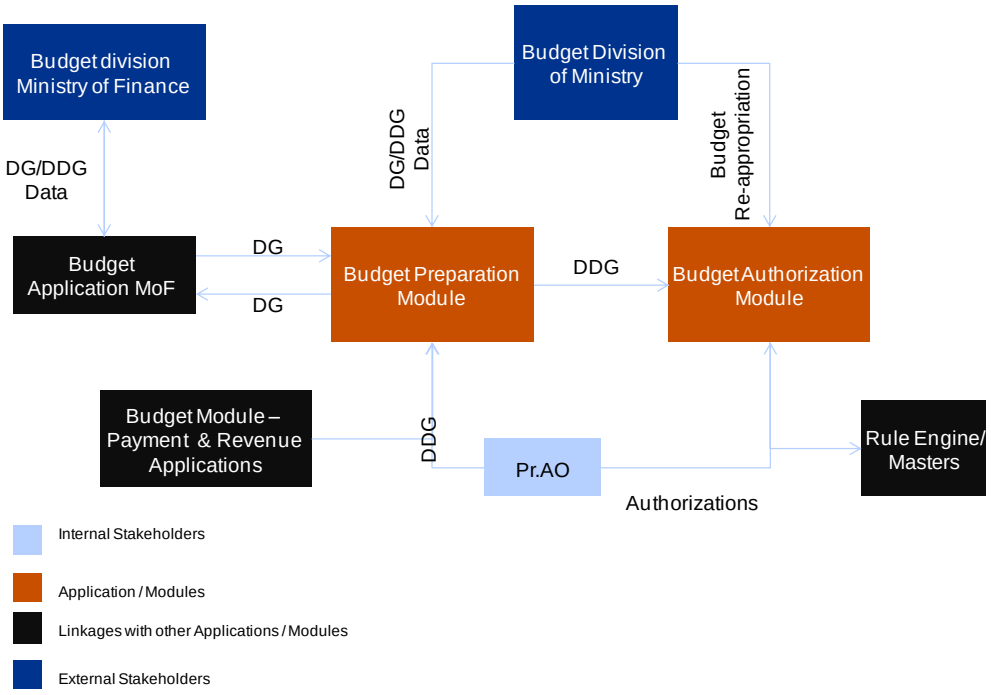
S. No.	Functions	Interface (if any)	Actors
1	Pr.AO consolidate expenditure (Statement of Budget Expenditure) and Receipt Budget and send to Budget Section of the Ministry	Budget preparation module of Payment and Revenue Accounting Application	Pr.AO
2	Budget Section of the Ministry sends Demand for Grant (DG) to the Ministry of Finance (MoF) in standard format as required by MoF	Budget Preparation application at MoF	Budget Section of the Ministry, and budget division of the Ministry of Finance(MoF)
3	Budget Section of the Ministry receives Demand for Grant (DG) from Ministry of Finance(MoF) after approval in standard format	Budget Preparation application at MoF	Budget Section of the Ministry, Ministry of Finance(MoF)
4	Budget Section of the Ministry prepares the Detailed Demand for Grant (DDG) from Demand from Grant (DG). DDG gets automatically mapped with the respective spending unit because of DDO & PAO masters	Rule Engine, Master – DDO & PAO Master	Budget Section of the Ministry
5	For preparation of revised budget estimate and final budget estimate and appropriate process shall be followed.	Budget Preparation application at MoF, Rule Engine, Master – DDO & PAO Master	DDO/CDDO, PAO, Pr.AO, Budget Section of the Ministry, Ministry of Finance(MoF),

S. No.	Functions	Interface (if any)	Actors
6	Function- Budget Re-appropriation & Supplementary Grant The module shall have provision for Budget Re-appropriation and Supplementary Grant as required by various ministries. The supplementary grant requirements of each spending unit needs to be captured via this module	-	Budget Section of the Ministry, DDO/CDDO, PAO.
7	Function – Budget Surrender Provision of budget surrender by the cut-off date as specified in rule engine	Rule Engine	Budget Section of the Ministry

a) Module – Budget Preparation (B.E., R.E., F.E.)

Currently the budget preparation process is done manually and it is not fully integrated with budget execution process. This module will facilitate automation of budget preparation process to the extent required by the O/o CGA.

This module will include bottom-up compilation of expenditure and receipt budget of each ministry and it will have interface with the budget module of payment and revenue management. Whereby, finalization of budget subsequent to approval of parliament is taken as top-down execution through the system hence, ensuring integration of budget v/s expenditure.



b) Module – Budget Authorization

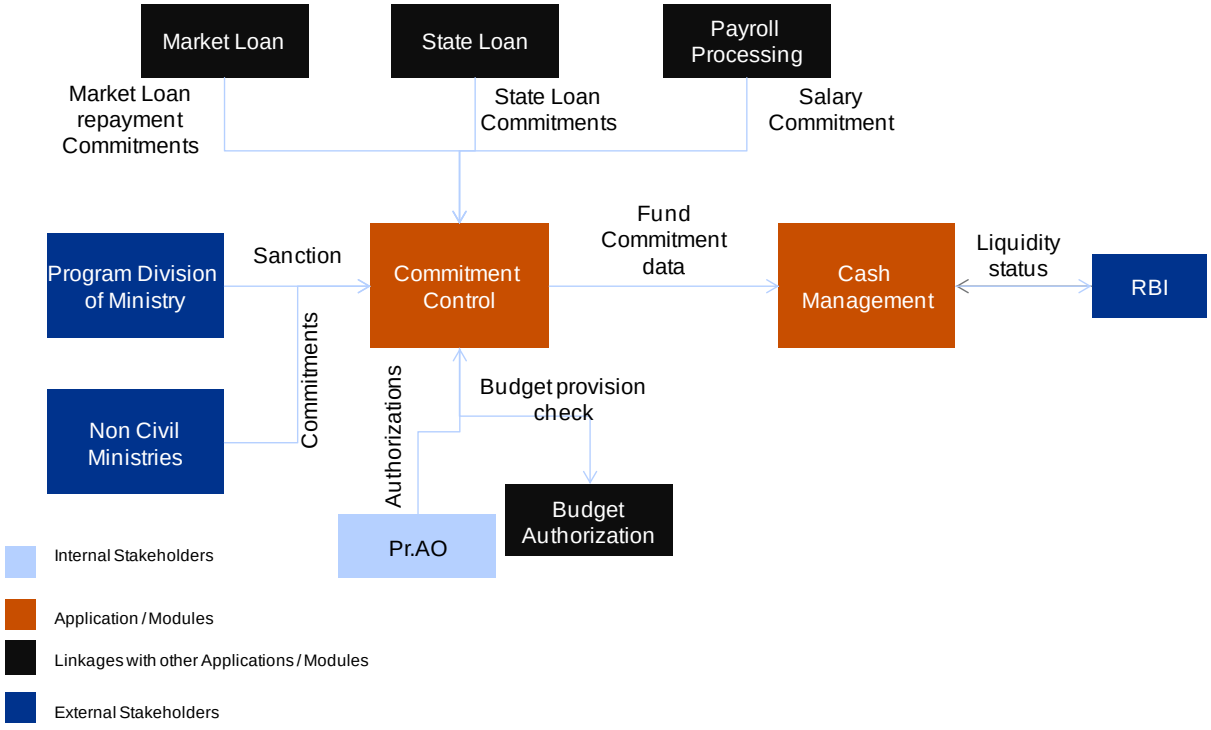
Budget Authorization module will facilitate authorization of funds form one ministry to another ministry. In the present system authorization of funds is not centralized which leads to inefficiencies and creation of suspense. This module will help in centralization of budget authorization process and reduction in creation of suspense account. At present CDDOs in MoUD uses Nirman-Jyoti for creation and maintenance of accounts. In order achieve complete automation of budget authorization process it is desired that either there is seamless integration with the Ministry specific applications such as Nirman –Jyoti etc. or the CDDOs are mandated to use e-payment.

S. No.	Functions	Interface (if any)	Actors
1	DDG mapped with the respective spending unit is an input to the module	Budget preparation Module	-
2	Capturing Advance given by ministries in terms of Letter of Authorization (LoA), Letter of Credit (LoC) etc.	-	Pr.AO
3	Pr.AO of a particular grant controller shall authorize particular account heads to Pr.AO of the spending ministry	-	Pr.AO of Authorizing Ministry

S. No.	Functions	Interface (if any)	Actors
4	Notification on the dashboard of Pr.AO of the spending ministry	BI tool/Dash board	Pr.AO of Spending Ministry
5	Pr.AO of the spending ministry will accept the request and authorize a particular PAO/DDO to spend the amount	-	Pr.AO of Spending Ministry
6	It will link grant controller of the authoring ministry to spending units (DDOs) in other ministries. It will facilitate/improve the process of intergovernmental fund transfer, accounting and audit.	-	Pr.AO of Spending Ministry
7	It will also capture the Foreign Letter of Credit (FLC) issues to banks by MEA and also the scrolls received for reconciliation	Banks(CBS)	Pr.AO of Authorizing Ministry

c) Module- Commitment Control and Cash Management

Absence of commitment controls, data mining and business intelligence tools are some problematic areas in the current system. Apart from these, risk management and tracking sanctions related to Financial Concurrence are other issues. The Commitment Control and Cash Management Modules will provide functionality to cater to these requirements.



S. No.	Functions	Interface (if any)	Actors
1	Capturing Sanction for planned funds from program division of ministry to implementation agency at state level	CPSMS	
2	Salary commitments from employee master/payroll processing	Rule Engine / Master Application, Payroll Processing Module	PAO
3	Integration with state loan application for capturing state loan commitments for funds transferred to state treasuries as Grant-in-Aids/loans	Loan and debt application	PAO
4	Integration with market loan application for capturing commitments related to principal repayment and interest payments	Loan and debt application	PAO
5	Commitment of funds for procurement of goods and services on signing of contract with the vendor. It will be entered into the system by the IFD, for contracts which will come for approval from IFD. For any other contract commitment will be entered by Pr.AO.	-	IFD, Pr.AO
6	Interface with RBI and budget division MoF for cash management – Budget division MoF shall monitor the payments commitments of GoI with the cash reserves at RBI and issue necessary instructions for managing the liquidity through issues of bonds, T-bills etc.	RBI CBS application, budget division MoF	Budget Division MoF
7	Interface with BI/Data warehouse for dashboard view to various users and projection of commitments	Data warehouse and BI tool	Pr.AO
8	Capturing principal repayment and interest payment details against foreign loans.	CAAA	

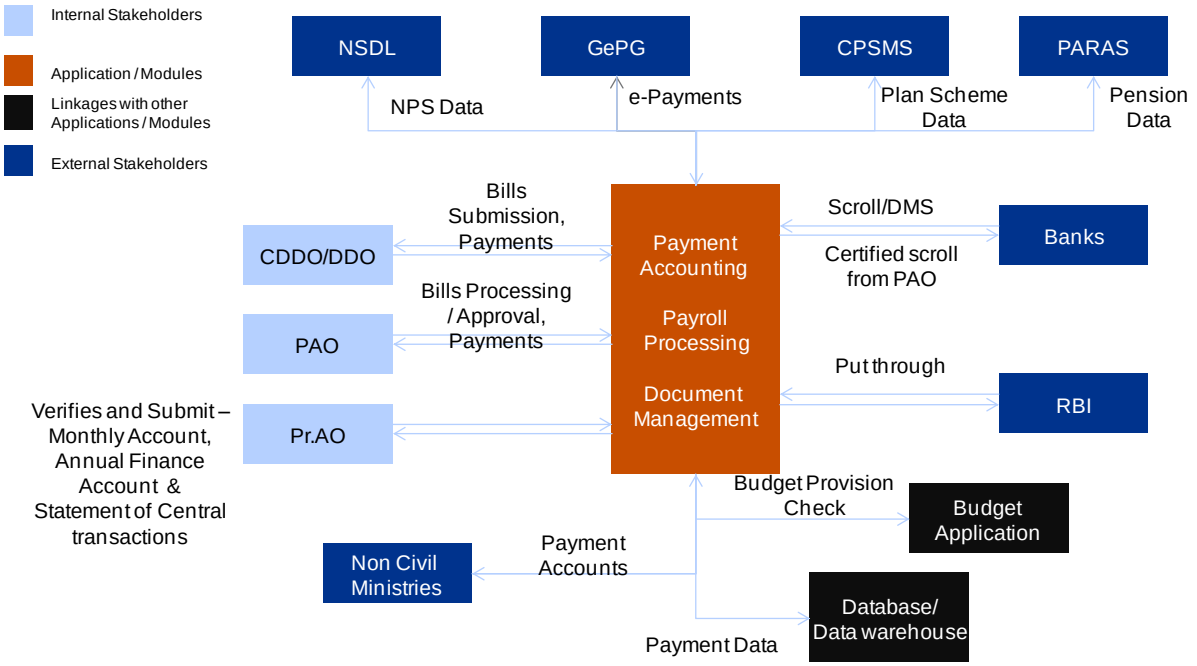
4.7.4 Application- Payments

a) Module- Payment

The Payment Management Application will facilitate (not limited to) the following:

- The business process right from preparation of bills to processing to be automated and have built-in work flows.
- Transaction level data to be captured from the point of preparation of bill.

- The application should allow work-allocation and should have the capability to track the ageing of bills.
- Management of scanned copies of bills/other digital records through a document management system.
- It will reduce the gap in accounting and actual incurring of expenditure; by recording the expenditure in the system at an early stage.
- The Payment Management Application being a centralized application will facilitate information flow from PAO level to DDO level.
- Offline functionality will be provided via an offline client application or a spreadsheet based solution, data can be loaded to the central application as and when connectivity is available or by transferring data to a CD/pen drive and uploading from a different location where connectivity is available.
- Complete automation of payment and reporting process will also reduce the problem of un-cleared suspense at PAO level.
- The payment application will be able to monitor the status of utilization certificate (UC) if details of UC are either electronically fetch from some other system/portal or are manually entered. UC monitoring needs to be handled on case to case basis, as the methodology/systems/applications varies based on the scheme/department.



S. No.	Functions	Interface (if any)	Actors
1	Bill entry at DDO level for all kind of bills viz. salary bill, vendor payment, bills against sanctions for planed funds etc.	Linkage with budget preparation module	DDO
2	Bill entry and processing for all kind of bills by CDDO	Linkage with budget preparation module	CDDO
3	Processing of bill at PAO – pre-check, post check (for bills prepared by CCDOs) and consolidation etc.	Linkage with budget preparation module	PAO
4	Interface with GePG for payment by PAO/CDDO.	GePG	PAO/CDDO
5	Capture employee details required for payroll processing such as date of birth, date of joining, leave details, loan details etc. to be entered by DDO. Some of the entries such as Leave details, loan details etc. to be validated monthly by DDO. Employee master in the master application to be populated via this interface.	Rule engine/master application	DDO/CDDO
6	Centralization of GPF process (advances, withdrawal, final payment etc.)	-	DDO
7	Sub-module for salary processing. The salary module should capture loans, advances, arrears etc. data of employees.	-	DDO, PAO
8	The payroll processing module will require creation of employee master with a unique number assigned to each number. For creation of employee master a system generated unique ID to be provided to each employee or UID issued by UIDAI can be utilized.	-	
9	Interface with banks for receiving scroll/DMS and reconciliation	Banks (CBS)	PAO
10	Interface with RBI for receiving put-through statements at PAO, Pr.AO and CGA level	RBI (CBS)	PAO, Pr.AO, CGA (RBD Section)
11	Accounts of non civil ministries such as flash figures, monthly accounts and annual accounts to be incorporated. It can be facilitated if the accounts are send in a predefined/standard format	Non civil ministries	PAO, CGA (Monthly account section)
12	Interface of payment management application with	PARAS application,	CPAO, PAOs

S. No.	Functions	Interface (if any)	Actors
	PARAS for pensions for electronically sending Pension Payment Order (PPO) to CPAO. It will also facilitate the following: - Disbursal of Payment - Minimization/elimination of Manual data entry - Incorporation of changed information of pensioners - Reconciliation with bank	Bank (CBS)	
13	The application shall take into account the various cases of pensions such as disability pension, freedom fighter pension etc. for generation of pre-pension	-	-
14	Interface with NSDL for uploading data of new pension scheme.	NSDL	PAOs
15	Accounts of non civil ministries to be incorporated	Non Civil Ministries via browser based access or a client application or through a spreadsheet	Non Civil Ministries, CGA (Monthly Accounts division)
16	Dashboard view for monitoring of bills, generation of accounts from transaction data	Data warehouse and BI tool	PAO, Pr.AO, CGA
17	Generation of statement of central transaction (SCT)	-	Pr.AO, CGA
18	Facilitate generation of Journal Entry (JE) and Transfer Entry (TE)	-	Pr.AO, CGA
19	Preparation of Finance Accounts & Appropriation Accounts with facility to exchange queries / information on excess / savings	-	Pr.AO, CGA

PARAS has been mentioned as an external stakeholder in line with the best practice study of the various systems across the world. It is suggested that PARAS be technically enhanced and integrated with GePG so that the pensioners can receive pension / revised pension directly through the CPAO's office. Additionally, it is recommended that an interface between PARAS and IGFMS be developed for exchange of PPO data, pension liability projections and accounting information. The validation of pensioner's data can be conducted by the bank which flow into PARAS through bank integration that shall be achieved in the IGFMS.

CPSMS is also recommended to be retained as a separate application for tracking of the central government funds right upto the beneficiary level. Further, the sanction generation module of the CPSMS be discontinued, and a similar module should be developed in the proposed IGFMS for both plan and non-plan funds. CPSMS should have an interface with the IGFMS so that the various program division and Pr. AO is able to view the details of expenditure incurred which can be used for informed decision making.

b) Module – Expenditure Budget

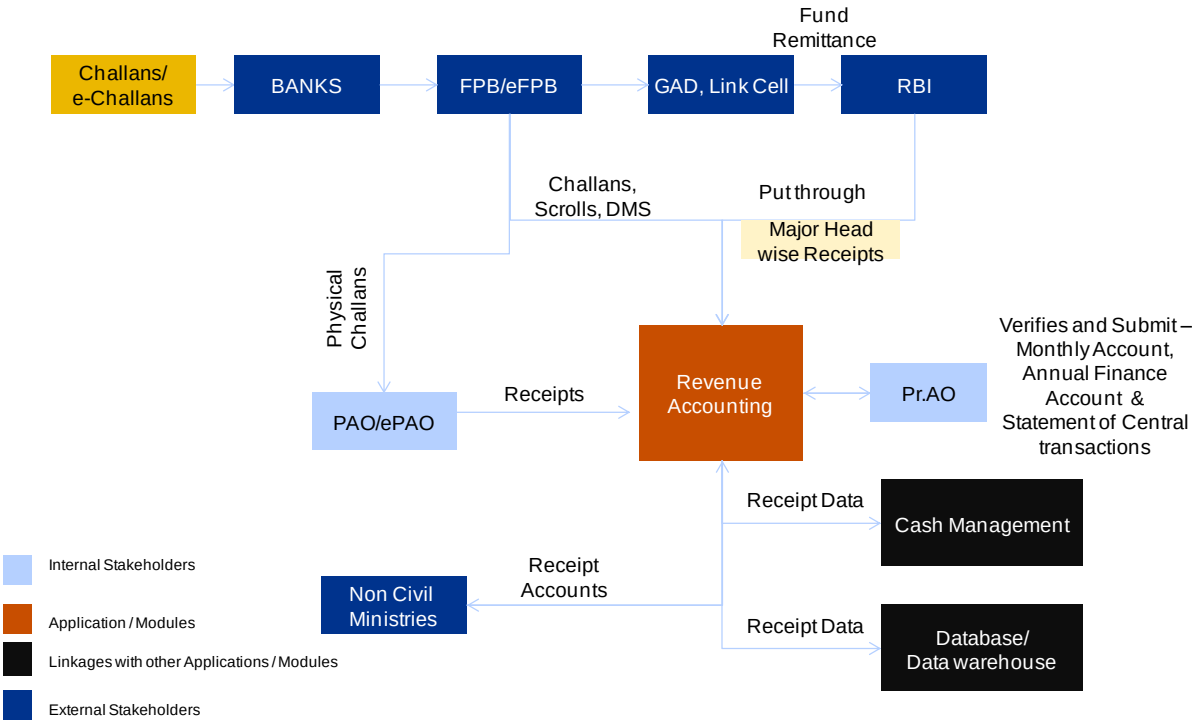
Expenditure budget module will facilitate the compilation of spending unit wise expenditure budget which will further be linked the budget preparation module of Budget Preparation, Authorization, Commitment Control and Cash Management Application.

S. No.	Functions	Interface (if any)	Actors
1	DDO/CDDO sends budget data for expenditure receipts to PAO	-	DDO/CDDO
2	PAO compile budget data for expenditure received from DDO/CDDOs and submit to Pr.AO.	-	PAO
3	Expenditure budget module shall have interface with budget preparation module of Budget Preparation, Authorization, Commitment Control & Cash Management Application	Budget Preparation, Authorization, Commitment Control & Cash Management Application	-
4	Pr.AO will get consolidated view of expenditure and receipt budget from budget preparation module of Budget Preparation, Authorization, Commitment Control & Cash Management application	-	Pr.AO
5	Budget data will be an input to this module for checking budget provisions	Budget Preparation, Authorization, Commitment Control & Cash Management Application	-

4.7.5 Application -Revenue Accounting

c) Module – Indirect Tax (CBEC)

Indirect tax module of revenue accounting application will facilitate in recording transactions and accounting of central excise and customs. It will also have an electronic interface with banks and RBI.

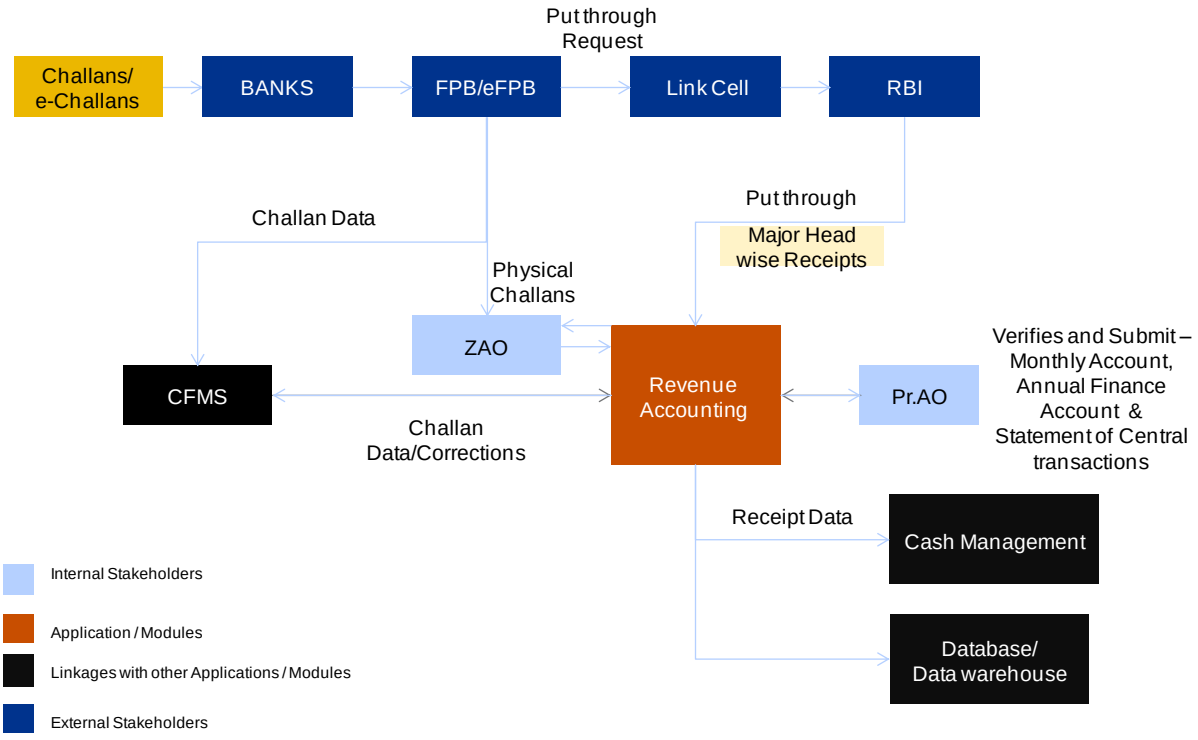


S. No.	Functions	Interface (if any)	Actors
1	The module shall accept challan in electronic format, scrolls (Major Head wise and PAO wise), DMS from focal point branch of banks	Banks (CBS)	Banks and PAO
2	PAO will verify challans received in electronic format from FPB and will do the accounting in appropriate account heads	-	PAO/ePAO
3	PAO will submit daily abstract and monthly account	Data warehouse	PAO
4	Pr.AO consolidate and submits monthly accounts to the data ware house	Data ware house	Pr.AO
5	Pr. AO submits annual finance accounts and Statement of Central Transactions (SCT)	Data warehouse	Pr.AO
6	Interface with RBI-CAS for receiving Put-Through statement at PAO and Pr.AO level. Also for receiving Major Head wise receipts from RBI-CAS to CGA.	RBI-CAS	PAO, Pr.AO, CGA
7	The integrated system should be flexible	-	-

S. No.	Functions	Interface (if any)	Actors
	enough to cater to the changes in the business environment e.g. GST		
8	Receipt accounts of non civil ministries to be incorporated	Non Civil Ministries via browser based access or a client application or through a spreadsheet	Non Civil Ministries, CGA (Monthly Accounts division)

d) Module – Direct Tax (CBDT)

Direct tax module of revenue accounting application will facilitate in recording transactions, and accounting of Direct Taxes. It will also have an electronic interface with banks and RBI.

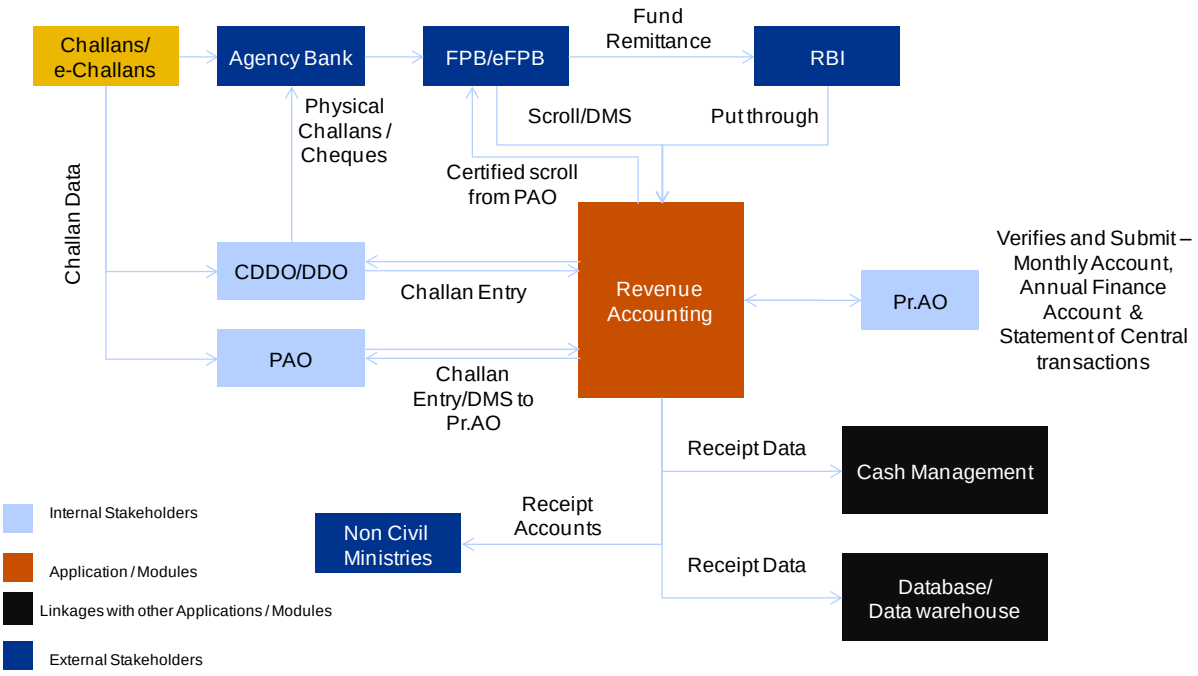


S. No.	Functions	Interface (if any)	Actors
1	The module shall accept challan data in electronic format from CFMS application	CFMS	ZAO
2	ZAO will verify challans received in electronic format from CFMS and will do the accounting in appropriate account heads	-	ZAO
3	ZAO will submit daily abstract and monthly account	Data warehouse	PAO

S. No.	Functions	Interface (if any)	Actors
4	Pr.AO consolidate and submits monthly accounts	Data warehouse	Pr.AO
5	Pr. AO submits annual finance accounts and Statement of Central Transactions (SCT)	Data warehouse	Pr.AO
6	Interface with RBI-CAS for receiving Put-Through statement at PAO and Pr.AO level. Also for receiving Major Head wise receipts from RBI-CAS to CGA.	RBI-CAS	PAO, Pr.AO, CGA

e) Module – Non Tax

Non tax module of revenue accounting application will facilitate in recording transactions, and accounting of non tax revenue of the government. It will also have an electronic interface with banks and RBI.



S. No.	Functions	Interface (if any)	Actors
1	The module shall accept challan in electronic format, scrolls (Major Head wise and PAO wise), DMS from focal point branch of banks	Banks (CBS)	Banks and PAO
2	DDO/CDDO enters challans in the application	-	DDO/CDDO
3	PAO will verify challans received in electronic format from FPB and DDO/CDDO, do the accounting in appropriate account heads	-	PAO
4	PAO will submit daily abstract and monthly account (DMS) to Pr.AO	Data warehouse	PAO
5	Pr.AO consolidate and submits monthly accounts	Data ware house	Pr.AO
6	Pr. AO submits annual finance accounts and Statement of Central Transactions	Data warehouse	Pr.AO

S. No.	Functions	Interface (if any)	Actors
	(SCT)		
7	Interface with RBI-CAS for receiving Put-Through statement at PAO and Pr.AO level. Also for receiving Major Head wise receipts from RBI-CAS to CGA.	RBI-CAS	PAO, Pr.AO, CGA
8	Receipt accounts of non civil ministries to be incorporated	Non Civil Ministries via browser based access or a client application or through a spreadsheet	Non Civil Ministries, CGA (Monthly Accounts division)

d) Module – Receipt Budget

Receipt Budget module will facilitate the compilation receipt budget which will further be linked the budget preparation module of Budget Preparation, Authorization, Commitment Control and Cash Management Application.

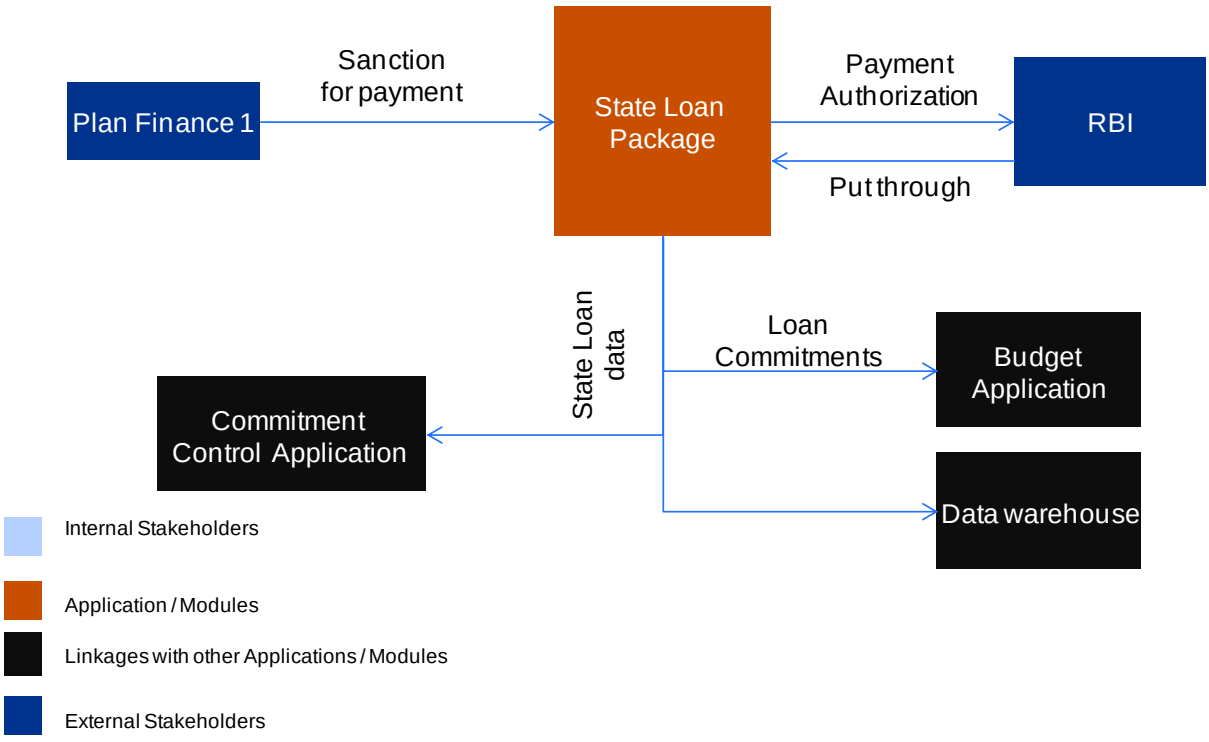
S. No.	Functions	Interface (if any)	Actors
1	DDO/CDDO sends budget data for revenue receipts to PAO	-	DDO/CDDO
2	PAO to compile budget data for revenue receipts received for DDO/CDDOs and submit to Pr.AO for non tax revenue. ZAO/PAO/e-PAO will compile the budget data via Receipt Budget module of the revenue accounting application for direct and indirect tax.	-	PAO, ZAO, ePAOs
3	Receipt Budget module shall have interface with budget preparation module of Budget Preparation, Authorization, Commitment Control & Cash Management Application	Budget Preparation, Authorization, Commitment Control & Cash Management Application	-
4	Pr.AO will get consolidated view of	-	Pr.AO

S. No.	Functions	Interface (if any)	Actors
	expenditure and Receipt Budget from budget preparation module of Budget Preparation, Authorization, Commitment Control & Cash Management application		

4.7.6 Application – Loan and Debt Management

a) Module – Loan

This module shall capture the all Grant-in-Aid & Loans given by Ministries to state governments, UTs, NGOs, Societies, Private Organizations etc. This module shall also facilitate State loan division, Ministry of Finance disbursal Grant-in-Aid & Loans to state governments.



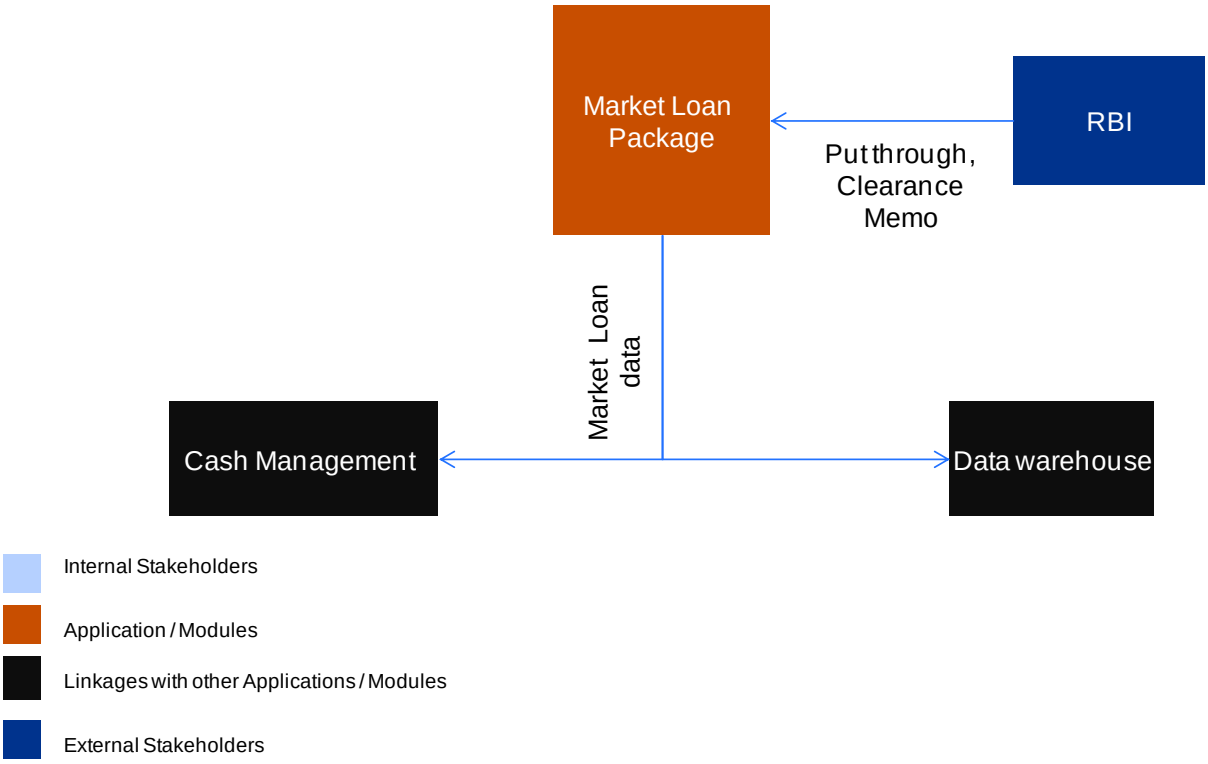
S. No.	Functions	Interface (if any)	Actor (s)
1	PAO receives sanction for program division of the Ministry for payment of Grant-in-Aids and loans	Program division of Ministry	PAO
2	Pr.AO will issue electronic advise to RBI for transfer of Grant-in-Aids and loans to state government/UTs	RBI-CAS	Pr.AO

S. No.	Functions	Interface (if any)	Actor (s)
3	Pr.AO will issue payment instruction via GePG for providing Grant-in-Aid & Loans to NGOs, Societies, Private organizations etc.	GePG	Pr.AO
4	Pr.AO will maintain repayment details of loans via this module	-	Pr.AO
5	Concerned PAO will do the accounting of the Grant-in-Aids and Loans via payment management application	Budget Preparation, Authorization, Commitment Control & Cash Management Payment application- for doing accounting of loan and grants	-
6	PAO at state loan division of MoF receives sanction for Plan Finance 1 of the Ministry of Finance for payment of Grant-in-Aids and loans to State Government /UTs	Program division of Ministry	Pr.AO
7	PAO at state loan section of MoF shall issue authorization RBI for transfer of funds to state governments	RBI-CAS	PAO state loan section MoF
8	PAO at state loan division of MoF will maintain repayment details of loans via this module		PAO state loan division
9	PAO at state loan division of MoF will do the accounting of the Grant-in-Aids and Loans via payment management application	Budget Preparation, Authorization, Commitment Control & Cash Management Payment application- for doing accounting of loan and grants	PAO state loan division
10	Receive Put-Through statement in electronic format form RBI for automatic reconciliation	RBI-CAS	-
11	Receive debit scroll from bank via GePG for automatic reconciliation	GePG	-
12	The module shall have interface with budget preparation module for validating the authorization	Budget Preparation, Authorization,	-

S. No.	Functions	Interface (if any)	Actor (s)
	of Grant-in-Aid and loans	Commitment Control & Cash Management and Payment application	

b) Module – Market Loan

This module shall facilitate Market Loan division, Economic Affair Division, Ministry of Finance capturing details of loan taken from Market and its repayment.



S. No.	Functions	Interface (if any)	Actor (s)
1	Receive Put-Through statement and clearance memo in electronic format form RBI	RBI-CAS	
2	PAO at Market loan division of MoF will do the accounting of the Loans via payment/receipt management application	Payment/receipt management application	PAO Market loan division
3	PAO at Market loan division of MoF will maintain repayment details of loans via this module		PAO Market loan division

4.7.7 Data warehouse/Business Intelligence

Data warehouse will have data from all the applications, and with the help of business intelligence tools it will provide dash board view to key stakeholders at CGA and Ministry level.

Data warehouse and business intelligence tools will provide the following functionalities (not limited to):

- The data warehouse will have all type of data such as transaction level data of payments/receipts, budget processing, re-appropriation, sanctions etc.
- It will provide functionality of slice and dice of data which will be over and above the standard reports provided by the individual applications.
- The dashboard view provided to key stakeholders at CGA and Ministry level will be customizable based on the requirements.
- The Business Intelligence tools will also facilitate functionality of internal audit by providing access to customizable reports and data.
- A flexible parameter based reporting mechanism should be made part of the system. It will facilitate extraction of information related to expenditure against budget, State-wise details, receipt-wise details etc
- Data migration of existing applications such as PARAS will be carried out for preparation of customizable reports via BI tools. It will also help in grievance redressal.
- It will facilitate multi-year perspective in expenditure planning and budgeting.
- Record keeping, migration of historical data and maintenance of audit trails will be part of the data ware house / Business intelligence tool.
- The head of the accounting unit will have view of the day-to-day workings of the PAO & DDO.

4.7.8 Asset Tracking

Asset tracking is a challenging task for the government. Asset tracking is a pre-requisite in case the government decides to move to accrual based accounting. Asset tracking is primarily the responsibility of the respective ministry/department. There can be different approaches for asset tracking; first one can be development/deployment of an asset tracking application which will be proactively used by all ministries/departments. It will not only record the asset at the time of procurement/development/purchase along with appropriate asset classification, but yearly valuations and verification can also be done. But it will be a difficult task to enforce implementation of such government-wide asset tracking application and it will involve carrying widespread reforms.

Another approach can be by keeping record of the accounting transaction made during the time of procurement/development/purchase of the asset. Accounting organization of various ministries can record these transactions for any new procurement/development/purchase of the asset, and do data entry for all previous such transactions in an asset tracking application. It will not be a complete asset tracking solution and shall not facilitate annual asset verification and valuation, but it will provide record of assets of government which will be accessible to various stakeholders.

On the similar lines an asset tracking application can be used to keep record of stock/inventory such a stationary and other consumable by either recording the accounting transaction or by digitizing the stock/inventory register. The accounting unit of the ministry/department, office of Pr.AO, PAO, DDO can be made responsible for keeping record of stock/inventory at the ministry/department. This stock/inventory tracking application can be implemented on a pilot basis for the O/o CGA on a pilot basis, if the initiative is successful, it can be replicated in other ministries/departments and later on can be implemented as a government-wide asset tracking solution which can be linked to the overall IT solution of CGA.

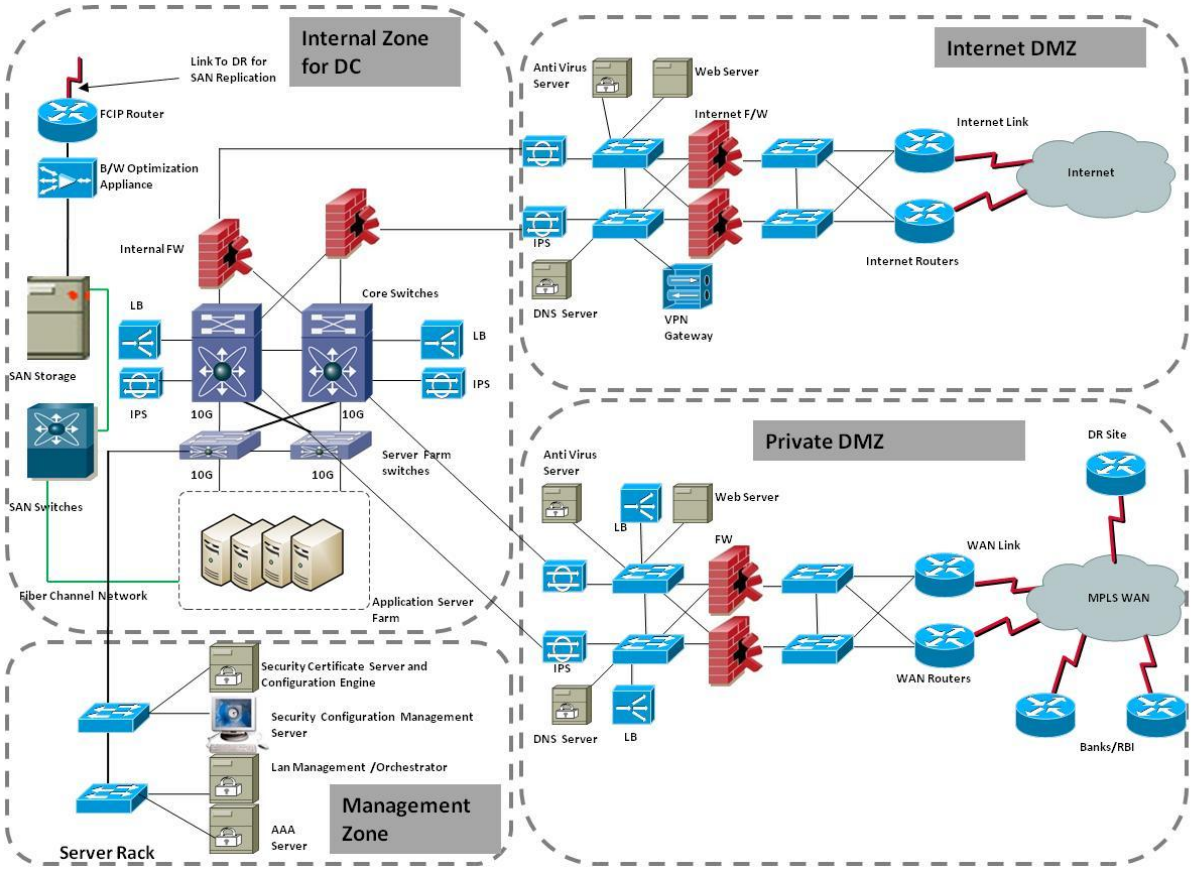
4.8 Network and Security Architecture

In order to implement a highly secure integrated system, a strategy for the information technology infrastructure needs to be developed. This would include servers, software and storage. Servers form the backbone of the infrastructure and ensure that sudden data surges in traffic can be handled efficiently. Ultimately, a single network may connect the entire system comprising of the various devices involved. A major portion of the work is

performed behind the scenes, in the network, by larger computers running powerful and complicated software to provide collaborative solutions that securely bring the information together. To most efficiently provide for a network infrastructure, the architecture should provide for storage devices that group storage systems on their own high-speed networks.

To implement an integrated solution, the focus for the CGA should be to implement real time, online applications with intranet and internet networking (through a Wide Area Network). This requires that a highly secure data centre is either established or employed with access limited to authorized individuals. The data centre should have a built-in recovery plan (in case of power outages or other disasters) that will permit the system to degrade gracefully. This would include back-up generators and back-up storage devices. The indicative SLA's are set out in Annexure 13.2

A highly secured architecture has been proposed for the organization of the CGA. Multi data centre architecture, consisting of two data centres, has been provisioned; considering the redundancy and fail safe aspects for the data centre. The subsequent diagram depicts the architecture of each of the data centres.



The IGFMS should have an Integrated Security Management System, which would integrate the information security infrastructure and implement standardized processes across various user levels. Given below is the set of requirements, which the proposed system should possess so as to mitigate all forms of threats to the IGFMS.

4.8.1 Information Security

Government's financial transactions and its accounting are sensitive in nature. It is therefore essential that security, consistency and integrity of data and transactions be maintained at all levels. CGA needs to have an Information Security (IS) Policy Manual for the stakeholders and users which will govern and guide them in IS practices.

4.8.2 Physical Security

The physical security of the proposed system should cover both:

- The Data Centre/ Disaster Recovery site
- The end offices

4.8.3 Network Security

- LAN cabling at all the locations, would be the responsibility of the Implementing agency and it should adhere to the TIA-942 Data Centre Standard while preparing the LAN connections
- The maintenance of the Data Centre LAN would be the responsibility of the Implementing agency.
- NICNET has certain sets of security and infrastructure maintenance policies, these policies may be followed.
- A de-militarized zone will be created to segregate the extent of access external / web users can have of the system for security reasons. The DMZ would consist of a primary and a secondary firewall
- Intrusion Prevention Systems coupled with a weekly review of the system logs/audit trails should be adopted.
- It must be ensured that all the services and associated ports, which are not required for IGFMS operation, are disabled / uninstalled in the IT Infrastructure including operating systems, database, application server, network and security infrastructure.
- The firewall should be able to but not limited to: provide state-full inspection, perform Prevention of Denial-of-Service Attacks, filter packets based on protocol / source & destination address / source & destination ports / interface of the firewall that the packet entered, support for protection of common internet applications like mail, DNS, AAA, etc.

and shall prevent IP Spoofing & Denial of Service Attacks, be able to filter malicious viz. Java Applets, ActiveX and perform Network Address Translation

- Implementation of Gateway Anti-virus, anti-spyware, anti-spam, anti-phishing, URL blocking & filtering and content filtering for scanning all incoming and outgoing traffic to and from the IGFMS for patterns of virus, spyware and spam.
- Firewall should support Dual-ISP connectivity.
- Capability to block compressed or very large files that exceed specified parameters.
- Use of Host based Intrusion Prevention System should be looked into while considering performance related issues.

4.8.4 System Security

- The entire IGFMS should be looked as a whole and should not be looked as a combination of different software, hardware and network resources. While framing access control procedures it should be kept in mind the requirement to secure the entire IT system physically and logically.
- The access control procedures will cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention will be given, where appropriate, for the need to control the allocation of privileged access rights, which allow users to override system controls.
- External users (users outside the department) should be given access to the system via the DMZ only.
- Access for internal users should be secure through LDAP and appropriate authentication services.
- Every component of the IGFMS, including the computers, printers, users, application and any other peripheral equipment should have an identity within the directory server and access to which, would be governed by the policies defined in the server itself.
- Database server access shall be provided through appropriate access control mechanism. User groups would be created at database server for allowing access to various data repository.
- Users should be granted access to information, data, devices, processes/daemons, audit files and software on a "need to know" basis. Access will be restricted according to the user's requirement to read, write or execute data or software on the basis of least privilege to achieve the desired function. The proposed solution must allow controlling

actions and access to resources of all users including privileged accounts such as root / administrator.

- There should not be any mechanism to delete data or information. All activities of deletion should lead to data being moved from the main place to a secondary place earmarked for storing deleted data. Under no circumstances data should be expunged.
- The system should support Role-based Administration and Role Based & Rule Based User Provisioning.
- There should be a single sign on into the entire IGFMS wherein one identity would be used to login into a PC and the same identity can be used for working within the application, database and other software and hardware part of the system.
- The entire IT system should be governed by a single user management policy which should be defined & deployed centrally using a centralized administration panel. System administrator must have the ability to define the user policies which would enable the following activities - perform password management functions including controlled password expirations, forced password change with optional grace logins, minimum password lengths (eight characters), alphanumeric password standards, password history logging, and user lockout from failed login attempts. The list is indicative and not exhaustive.
- The proposed solution must provide the ability to designate specific users as Administrators, Auditors, and Password Managers etc with appropriate rights. The proposed solution must also provide the ability to designate specific users as Subordinate or Group Administrators, to manage users and file permissions for their Group.
- All desktops / laptops, which will be used for accessing information, should have protected with a combination of user Id / password.
- All systems used must have the ability to perform password management functions including controlled password expirations, forced password change with optional grace logins, minimum password lengths (eight characters), alphanumeric password standards, password history logging, and user lockout from failed login attempts.
- Solution should support SAML (the standard for exchanging authentication and authorization information between security management systems) without coding, including both SAML Consumer & SAML Producer modes of operation. SAML Consumer capability should support both one-to-one user mapping as well as many to- one user mapping.

- All active user ID's will be reconciled on quarterly basis to ensure removal of redundant / unauthorized user IDs.
- Capability to access the data content of the database from an interface other than the application interface should be prohibited.
- Access to any terminal in the network using any kind of storage devices such as USB, CD, DVD, Floppy and Network terminals should be strictly prohibited and blocked.
- However it may be essential to allow some copying of data into the IGFMS or out of the Treasury system without jeopardizing the security of the system. Implementing agency should suggest a mechanism governed by processes as well as technologies which can allow such requirements to be addressed.
- The solution must provide support for IPv6 and FIPS140-2.
- The solution must provide SSL Support for Inter-Component Communication.
- Access to mailing service should be strictly controlled using an access control policy within the entire Treasury system.
- All attachments made while using Internet based services such as email should be disallowed or filtered to prevent data pilferage.
- Access to Internet content should be controlled using access control & content filtering policies and procedures.
- A centralized patch management solution shall be deployed for the desktops and servers.
- This solution shall ensure that the patches for Operating System, RDBMS, any other type of system software, application software, etc can be administered centrally after performing appropriate testing and taking requisite permissions.
- Each desktop shall be configured for automatic updation of patch from the centralized patch management server. The centralized patch management server at the data centre would be deployed and managed by implementing agency.
- The Implementing agency should be able to perform activities of system configuration management, asset management and operations management centrally from the central hub.

4.8.5 Application Security

- Internal Users (Department Users / Operators) should not be able to login to the application, without providing login credentials, biometric authentication and digital certificate. The application should have capability to enforce required password policy (e.g. minimum password length, complexity requirements, password age etc).

- The application should lock out user Id after performing a configurable number of unsuccessful attempts.
- Application user Authentication & authorization related transactions should be encrypted.
- Application should restrict to authenticate a user whose password has expired until the user changes the expired password.
- In case the system is being accessed by other systems / web services / interfaces, the system should perform due authentication.
- In case of data upload (e.g. upload of a XML file / Excel file / ASCII file) or data transfer the application shall have controls such as data totaling / control totaling / checksums to ensure that the data transfer is complete and accurate.
  Each data generated out of the system such as MIS or any other information should be time stamped and digitally signed so as to ensure non-repudiation.
- In certain cases there may be requirement to upload data into the application system. The application system should provide provision to define the processes where uploading feature has to be provided or has to be withdrawn from. Along with such provisions it should also provide for a mechanism to define the type and size of attachments for each upload.
- Any uploaded file to the application system should be scanned thoroughly before allowing the uploaded file to reach IGFMS application system for storage.
- The application should implement for Maker-Checker concept wherein a user who creates a record or request should not be able to approve or update the record or request.

4.8.6 Audit Trails & Logs

- Event logging is extremely helpful in documenting user activity. It creates an accurate record of user activity such as which users accessed which system, as well as which websites they visited when and for how long. The solution should log all types of events especially those related to security and transactions.
- The Implementing agency and CGA should agree on a timeframe for which old audit logs will be maintained for ready reference in the system. The old records may be archived.
- The application should log all application transaction details including time stamp, operator, approver IDs, update/modification trail etc.
- The application should protect its audit records from unauthorized deletion, modification, or disclosure.

- Any critical log information which requires urgent attention, such as issues which can lead to downtime, should be captured properly and an appropriate alert be generated and sent to department officials as well as the technical team of the implementing agency.
- The system shall have a secure and preferably embedded log repository to store logs that do not require separate database expertise to administer and manage.
- The solution should implement policy management solutions for access control and network security. The software for policy management will ensure implementation of well – defined policy and monitoring of any deviation from the department's policies, which would be in line with global standards like ISO 27001, BS7799, RBI & IBA guidelines, etc.

4.8.7 Data Protection

- The application should store password and other key data content in encrypted form.
- The database/file which stores username and password should be secured and have restricted access.
- The application shall support SSL encryption mechanism for transferring data across network. Provision should be made to ensure that data in any form should not be copied on to any external media without authorization.
- Complete end point data protection should be provided such that any type of data pilferage using unauthorized copying, storing and emailing could be prohibited.

4.8.8 Session Management

- The system shall limit to only one session per user or process ID
- The system shall put a limit on the maximum time length of an idle session, which should ensure that automatic session termination takes place after expiry of the specific time length
- The system should provide capability to modify the maximum time length of idle sessions dynamically.
- The application users should be able to explicitly terminate a session (logout).
- The application should not store authentication credentials on client computers after a session terminates.
- The application shall map the sessions with the client machines and should store the appropriate data.

4.8.9 SMTP Server Security

- Anti-Relay, Anti-SPAM & Anti Virus Service.

- Support for SMTP relay services through Multiple SI s/Gateways.
- Ability to provide proactive e-mail virus protection (scanning prior to delivery at the mail Server)
- Ability to provide proactive e-mail content filtering.
- Ability for the administrator to block or allow e-mail based on multiple message attributes.
- Ability for the user to encrypt outbound e-mail.
- Ability to limit the size of files attached and the type of files attached and sent using the
- SMTP server.

4.8.10 Database Security

- Users must not have access to the database prompt of the application. Access to the database prompt must be restricted only to the database administrator and / or a person designated for generating MIS reports. "Super user" rights for the database must only be given to the database administrator and the activities of these accounts must be properly logged.
- Even the super user should not have access to the data stored within the database.
- Access to the data from any non-application platform should be strictly prohibited.
- The database configuration shall adhere to base line security guidelines released by the product vendor.

4.8.11 Application Deployment

- All unused ports, both software and hardware, should be blocked at client PCs and at Server machines.
- The application server shall be segregated from user zone through firewall or other filtering mechanism.
- The application server should be protected with appropriate Antivirus software.
- Any version upgrade / changes in application software shall not be performed on the production server directly without appropriate methodologies of staging in testing environment.
- Any version upgrade/ changes in application shall be implemented in staging / test server. The application shall be migrated to the production environment only after adequate testing and approval from CGA.
- Access to application server would be restricted to system administrator.
- The Implementing agency shall implement and maintain dedicated staging/test environment even after go-live of the new system.

- Separate development, testing and production environments for data security and unhindered running of the production environment.

4.8.12 Information Security Governance

- The Implementing agency shall ensure that each of its employees working on the project is aware of his or her responsibilities with respect to Information Privacy and Information Security.
- The implementing agency shall ensure that each of its employees working on the project shall undergo security awareness training during induction.
- The Implementing agency shall ensure adherence to Data classification scheme of the CGA organization for maintaining segregation between the various levels of sensitive information and to make available information only on a need to know basis.
- The Implementing agency shall use the known standards of Information Security Governance while dealing with the data.

4.8.13 Personal Information Processing / Storage Equipments

- All information storage media (e.g. hard disks, magnetic tapes, CD ROMs etc.) will be physically secured.
- Physical access to magnetic tape, disk, CD libraries etc. will be restricted to authorized personnel based on job responsibilities.
- Back-up media will be stored in fire resistant safes or cabinets.
- Any storage media (e.g. hard disks, magnetic tapes, CD ROMs etc.) should not be allowed out of the office locations, without adequate clearances / approvals. All movement of storage media from the office locations should be appropriately recorded with reasons for movement.
- The inventory of all information storage media (e.g. hard disks, magnetic tapes, CD ROMs etc.), used within the office locations should be maintained. The inventory should be reconciled on a monthly basis.

4.8.14 Computing Environment

- All workstation hardware and associated peripheral equipment will be marked with a unique asset identification code. The asset identification code will follow a defined naming convention that would uniquely and appropriately identify the asset.
- USB ports will be deactivated in all desktops / laptops, so as to prevent use of pen drives, external disk drives etc.

- Any unauthorized connections to the Internet by using external or inbuilt modems, broadband connections data card etc. will not be permitted.
- Modems will be disabled in desktops / laptops. Use of application & OS level hardening features for securing the computing environment.

4.8.15 General guidelines on computer virus control

- Latest version of anti-virus should be installed on all workstations, laptops and servers.
- The anti-virus software will be run on network file servers on a regular basis (preferably daily).
- All servers and desktops shall automatically update the virus definitions from centralized server on daily basis. The centralized server at would be deployed and managed by implementing agency.
- The Antivirus solution should support automatic and manual program and definition update.

4.8.16 Disaster Recovery / Business Continuity Planning

- Business continuity plan should comply with zero data latency i.e. the recovery point objective (RPO) for the database stored at BCP would be 0 minutes. However, it does not mean that application should be running on a no downtime policy. The replication process configured should not cause any effect over the transactions conducted over primary database, i.e., the primary and BCP database should be decoupled.
- In case the primary site is down, the traffic coming from all internal users as well as those coming through Internet would be redirected to the BCP.
- The switchover from DC to BCP should not result in any data loss and similarly switchover from BCP to DC, after DC is restored back, should also not result in any data loss. Thus both databases should synch with each other such that at any point of time when switchover to the corresponding site is required the databases at both the places are completely synchronized.
- The Implementing agency should also suggest whether during the course of the project post go-live it would be feasible to reduce the RPO and RTO any further.

4.8.17 Compliance

- The operation and management of information systems may be subject to statutory, regulatory and contractual requirements. The objective for ensuring compliance is to avoid breach of any criminal and civil law, and statutory, regulatory or contractual requirements. It is the responsibility of implementing agency to ensure that any

commercial software acquired, is used only in accordance with licensing agreements. Likewise, it is also their responsibility to ensure that any proprietary software is properly licensed before being installed.

- Usage of: Unlicensed commercial software, any reversed engineered "Cracked" software or license keys acquired from sources other than authorized sources such as the vendor shall not be allowed. In the event license keys are obtained from other sources, evidence of procurement must be maintained.
- No unlicensed software, shareware (beyond its period of free use), public domain software or pirated software will be used. Implementing agency should provide and reconcile all licenses with software installed on hardware and should also maintain audit of increase or decrease in numbers of users / licenses. Implementing agency should maintain this inventory or audit of licenses in electronic and paper repository which shall be in the custody of CGA.
- Implementing agency should also ensure that all updates, upgrades of all licensed software are obtained and installed.

4.8.18 Incident Reporting

- The Implementing agency shall be responsible for reporting any security incidents to designated officials.
- Implementing agency shall follow the Incident reporting policy and use standardized templates for incident reporting.

4.8.19 Backup & Recovery

- The backup and restoration policy should be framed and provided to the department as a deliverable by the Implementing agency.
- The Implementing agency shall be responsible for taking backup of all data that is stored within the new system in accordance with the backup policy.
- The Implementing agency shall implement the required backup solution for regular / scheduled backups.
- A backup schedule shall be prepared by the Implementing agency and the same shall be implemented with approval of the department.
- The Implementing agency shall also make arrangement for offsite storage of the backup media. The offsite location shall be arranged by the department. Transportation of backup media shall be arranged by the Implementing agency.

- The system shall ensure asymmetric encryption of data backup files such that encryption can be done using a public key of authorized user and decryption can be done using the private key of the same user.
- The Implementing agency should periodically (once every month) test the backed up data by restoring the data, to a media device, in order to check its consistency.

4.9 Business Intelligence and Data warehousing

Adding business intelligence (BI) to the architecture moves the current architecture towards enterprise architecture by considering the operational business systems and how they are logically interrelated.

BI primarily refers to computer-based techniques used in identifying, extracting, and analyzing business data. As of now, the web based application, e-Lekha, is catering to the reporting functionalities required by the CGA. However, it has been noted that Processes at e-Lekha for obtaining and generating reports are to be made efficient for faster data access and reporting

For the purposes of the CGA, BI technologies would be extremely helpful in providing historical, current and predictive views of business operations. Common functions of business intelligence technologies such as reporting, online analytical processing, analytics, data mining, process mining, complex event processing, business performance management, benchmarking, text mining and predictive analytics would provide the required slice-and-dice views of the available information to the CGA for analysis purposes.

There are three key layers in the business intelligence architecture:

Source data and ETL (Extract Transform Load)

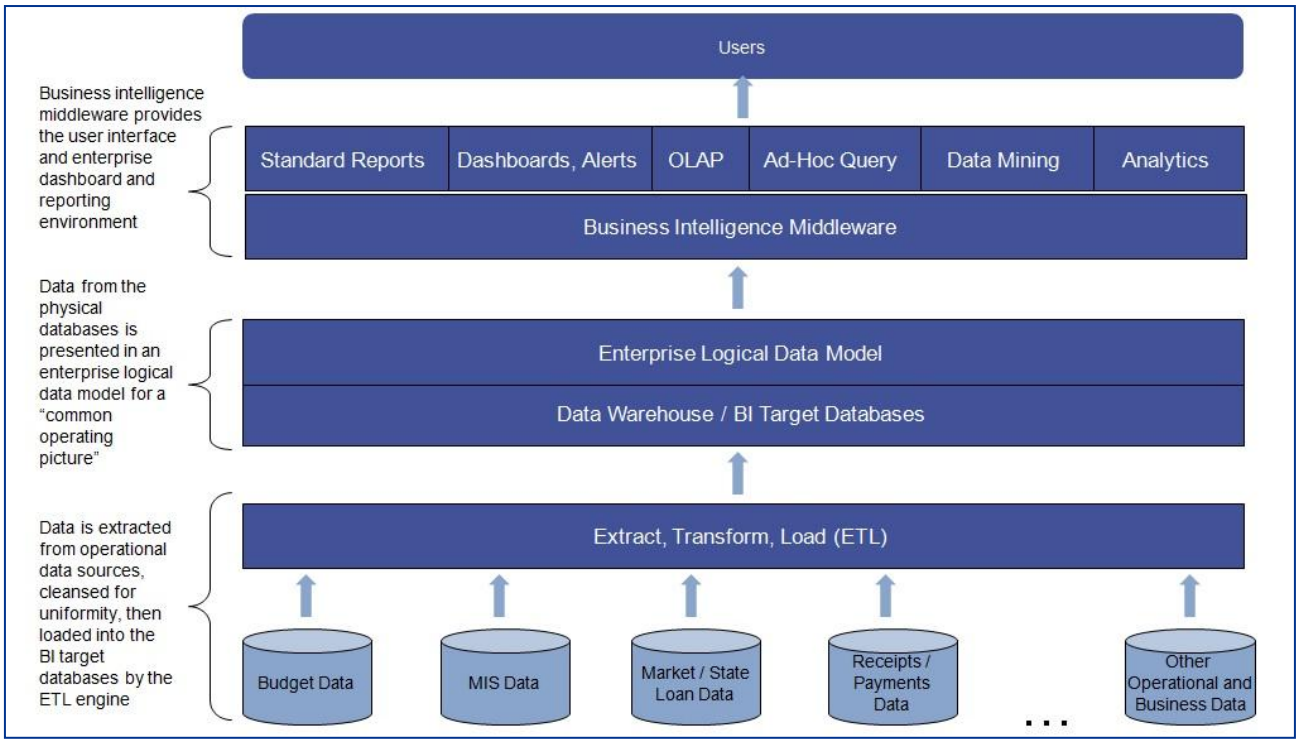
Composed of the existing systems and other data sources, as well as the proper middleware to extract the source data, and an ETL engine to cleanse and normalize data.

Data Warehouse/BI Target Databases

Data from the source systems is collected, normalized, and loaded by the ETL engine into the data warehouse or other BI target databases. An enterprise logical model resides here in conjunction with the data warehouse to describe the data relationships.

Application Interface

The user will interact with the BI application front-end to perform analysis, run calculations, and report on performance metrics. The application interface includes the BI engine, OLAP (Online Analytical Processing) engine, dashboard and reporting engine, and alerts engine.



The output of the BI tool is derived from the data warehouse. The selection of data warehouse technology, for both hardware and software, depends on many factors, such as:

- Volume of data to be accommodated;
- Required response time;
- Current infrastructure available;
- Level of data being built and kind of analysis to be performed;
- Number of user;
- Cost of technology.

5 COTS Evaluation

The applications that were described in earlier sections for covering the functionality of budget, payments, receipts and loan & debt management can be developed as bespoke applications with some COTS products being used to cover specific functionalities such as payroll processing, management of document, internal audit and business intelligence. Another approach could be deployment of a complete COTS solution with required customizations.

In adopting the first approach mentioned above, the following applications/modules will need to be developed:

i) Application for budget preparation, authorization, commitment control and cash management.

ii) Application for payment management including module on payroll processing and document management.

iii) Application for revenue management.

iv) Application for loan and debt management.

Other functionalities such as business intelligence, rule engine, internal audit and asset tracking can either be developed in bespoke fashion or can be deployed using available/suitable COTS solution.

The second approach requires deployment of COTS solutions available from leading OEMs/companies. The leading COTS solutions to provide the functionality of integrated financial management system are - Oracle e-Business Suite, SAP Integrated Business Suite and FreeBalance Accountability Suite.

5.1 Bespoke Development -Technology Options

The application/module developed as a bespoke solution may have various technology options for development of user interface, choice of programming language, choice of database and reporting requirements. Out of these, the important technology options i.e. database and business intelligence are covered in detail in this section.

5.1.1 Database

There are several options that can be considered, while selecting the prefered/suitable database management system. Details of some of the leading database systems are provided below.

Oracle Database

The Oracle Database is an object-relational database management system produced and marketed by Oracle Corporation. There are various editions that are available for Oracle database systems, these are as follows:

Standard Edition (SE): This is the edition that provides the base database functionality. Oracle Corporation licenses this product on the basis of 'per user' or on the basis of per 'processor', typically for servers running from one to four CPUs. If the number of CPUs exceeds 4, the user has to convert to an 'Enterprise' license. SE has no memory limits, and can utilize clustering with Oracle Real Application Cluster (RAC) at no additional charge.

Enterprise Edition (EE): The key feature of the EE is that it has extended security in comparison to the Standard Edition mentioned above. Apart from this, it has no memory limits, and can utilize clustering using the Oracle RAC software.

Express Edition (XE): The Express Edition offers Oracle 10g, which can be configured on Windows and Linux platforms. It has a footprint of only 150 MB and is restricted to the use of a single CPU, a maximum of 4 GB of user data. Support for this version comes exclusively through on-line forums and not through Oracle support.

Oracle Database Lite: This is meant to be deployed on mobile devices.

The Oracle 11g database supports a variety of platforms including Linux, Microsoft, Solaris, HP-UX, and AIX. Users who have Oracle support contracts can use Oracle's "My Oracle Support" web site. The support site provides users of Oracle Corporation products with a repository of reported problems, diagnostic scripts and solutions. It also integrates with the provision of support tools, patches and upgrades.

One of the potential advantages of using Oracle databases is that it can help you create customized database applications. Instead of getting a standardized database program out of the box, you get a program that can be customized to fit your needs. Also, Oracle databases provides data mining capabilitie. But one of the potentional drawback is that, the per user license cost is high compared to other databases. Another potential drawback of using Oracle databases is that there is a learning curve involved. This is not something that you can pick up in a short period, if you are unfamiliar with it.

IBM DB2

IBM DB2 is a relational model database server developed by IBM. There are three versions of DB2- DB2 for LUW (Linux, Unix, and Windows), DB2 for z/OS (mainframe), and DB2 for iSeries (formerly OS/400). Thus, the DB2 database system caters to the requirement being suitable for use on a large number of platforms. DB2 can be administered from either the command-line or a GUI. The GUI is a multi-platform Java client that contains a variety of wizards suitable for novice users. DB2 supports both SQL and XQuery. DB2 has native implementation of XML data storage, where XML data is stored as XML (not as relational data or CLOB data) for faster access using XQuery. The potential problem with DB2 is related to a data portability from other databases.

Microsoft SQL Server

Microsoft SQL Server is a relational database server, developed by Microsoft. There are several editions of SQL Server available that cater to the different needs of different user groups. Microsoft SQL Server's primary query languages are T-SQL and ANSI SQL.The major challenge with MS SQL is scalability, though , MS SQL Server can support high-volume transactional systems in the terabyte range, but it cannot support the same size warehousing environments. Also, in scaling SQL Server to large size, issues related to security and flexibility might arise.

Firebird

Firebird, an open-source database management system, is based on the code base for the commercial DBMS InterBase version 6.0. Firebird uses two licenses which are both similar to the Mozilla Public License (MPL). Firebird runs on Windows, Linux, FreeBSD, and MacOS X. On- disk bitmap indexes are not supported, but Firebird can combine indexes and form bitmaps in memory. Firebird does not support materialized views, star joins or partitioning. Replication is not available in the Firebird distribution itself, but 3rd party tools (both commercial and open source) provide this. With respect to data sizes, it should be noted that tables are limited to 2 billion rows in Firebird, but that there is no limit on the byte- size of databases.

The user can implement stored procedures (SPs) in Firebird's procedural language PSQL. Further user-defined functions (UDFs) can be loaded from external shared object libraries and, thus, the user can implement in C, C++, Delphi, etc. The potential problem with Firebird is related to scalability. Also, some of the standard features available in other databases such as integration with other database systems, temporary tables etc. are not avilable in Firebird.

Ingres Database

Ingres Database developed by Ingres is an open-source database management system and available under a commercial license ("Enterprise Edition") or under the General Public License (GPL). Ingres supports its products for 15 years, but support and maintenance from Ingres is only available for the Enterprise Edition. Ingres Database runs on Windows and a variety of different UNIX-like platforms. Active community forums exist and Ingres also offers 25 free manuals for its product. Materialized views, bitmap indexes, and star joins are not supported. Multi-master replication and partitioning (based on range, value, or hash) including sub-partitioning are supported out-of-the-box in Ingres Database. With respect to scalability, Ingres claims that Ingres Database is capable of handling many terabytes of data easily. SQL can be used for stored procedures and further user-defined functions can be implemented in C. Though Ingres provides various functionalities, there could be potential problems related to technical support.

LucidDB

LucidDB, an open-source database management system, is developed by the software company LucidEra and the non-profit organization The Eigenbase Project. The LucidDB server is licensed under the GPL while the LucidDB client is licensed under the LGPL. LucidDB is specially built for datawarehousing and business intelligence purposes. This is in contrast to the other considered tools apart from MonetDB (see below). LucidDB and MonetDB are among the few databases to support column-store. In a column-store, all data tables are split vertically at the physical layer such that each column is stored on-disk independently of other columns. This is different from traditional rowstores where data from different columns is stored together in rows.

LucidDB runs on 32 and 64 bit Linux and on 32 bit Windows (using Cygwin). LucidEra does not sell support or commercial licenses for LucidDB. LucidDB supports B-tree and bitmap indexes. LucidDB chooses itself which indexes to create and can also combine the two types; star joins are also supported. User-defined functions can be created in Java. It is also possible to wrap external data sources like files or tables from another DBMS and use them as traditional tables from LucidDB. While LucidDB offers many features relevant for data warehousing, it should be noted that it is still not a mature DBMS. For example, foreign keys, sub-queries, transaction handling, and support for altering table definitions are still missing.

MonetDB

MonetDB, like LucidDB, is not a DBMS made for on-line transactional processing (OLTP) with highly concurrent workloads; instead the focus is on efficient handling of query-intensive access patterns. MonetDB is developed by the research institute CWI and runs on Windows and different UNIX-like operating systems. In the implementation, care has been taken to use the hardware very efficiently. No commercial support is provided for MonetDB, as of now. Like LucidDB, MonetDB itself picks which indexes to create. However, bitmap indexes seem to be unsupported. Partitioning, replication, and materialized views are also currently unsupported, but future additions are planned for these areas. The user can define stored procedures in SQL as well as external functions in MonetDB's proprietary MAL language and in C. MonetDB is rated low on quality and security as compared to other databases.

MySQL

MySQL developed by MySQL (now owned by Oracle Corporation), is available under a commercial license or under the GPL. It can be downloaded in two versions: The "Community Server" which is free and the "MySQL Enterprise" edition which is not free, and for which extra features and commercial services exist. Oracle Corporation offers a wide range of commercial support, consulting, and training. It is reported that MySQL-based data warehouses larger than 30 terabytes exist. MySQL runs on Windows and a large collection of UNIX-like systems.

There is no support for star joins or materialized views. The 5.1 series offers range, list, hash, and key partitioning functions. Statement-based master-slave asynchronous replication has been available in MySQL since version 3.23, but from release 5.1, row-based replication is also available. On-disk bitmap indexes are not supported in MySQL, but MySQL can perform an index merge where a bitmap is built in-memory. The user can implement stored procedures in SQL and user defined functions in C/C++.

MySQL has some drawbacks such as it does not support very large databsas size as efficiently as other leading databases and there might be trade-off between speed and capabilities. But there is an active development team which releases newer versions to incorporate the required functionalities

PostgreSQL

PostgreSQL is released under the BSD license (free software license), and runs on Windows and on a large collection of UNIX-like operating systems. PostgreSQL's development is led by its community and not by a single company. Due to its non-restrictive BSD license, several (open source and commercial) derivatives exist. For example, Netezza, EnterpriseDB, and Greenplum offer PostgreSQL-based products. Several companies also offer commercial support, training and consulting. Materialized views and star joins are not supported in PostgreSQL. On-disk bitmaps are not supported yet, but they are planned for inclusion in a future version. Partitioning is to some degree supported by means of PostgreSQL's table inheritance features. PostgreSQL offers several languages for stored procedures: PL/pgSQL, PL/Tcl, and PL/Python.The user can also create external functions in C libraries.Apart form these PostgreSQL has some such as suitability/usability of the user interface and lack of availability of some of the functionalities such as temporary table.

5.1.2 Business Intelligence Suites

Business intelligence tools are a type of application software designed to retrieve, analyze data and to prepare reports.There are several BI tools that are available, some of these have been described in the following pages.

IBM Cognos Series 10

IBM Cognos BI includes both web-based and Windows based user interfaces that

allow users to view the required data in required formats. IBM Cognos Business Insight is the product that lets the user create interactive dashboards using IBM Cognos content, as well as external data sources. The content of the dashboard can be viewed and manipulated. IBM Cognos Report Studio is a report design and authoring tool. Using IBM Cognos Report Studio, report authors can create, edit, and distribute a wide range of professional reports. IBM Cognos Query Studio, is to be used by users with minimal or no training to quickly design, create, and save ad-hoc reports that are not covered by the standard reports created in IBM Cognos Report Studio. IBM Cognos Analysis Studio is the product used to explore and analyze data from different dimensions. Analyses created in IBM Cognos Analysis Studio can be opened in IBM Cognos Report Studio and used to build professional reports. IBM Cognos Event Studio is used as a monitoring tool for the data and performs tasks when business events or exceptional conditions occur in the user's data. When an event occurs, people are alerted to take action. IBM Cognos Framework Manager is the IBM Cognos BI modeling tool for creating and managing business related metadata for use in IBM Cognos BI analysis and reporting. Metadata is published for use by reporting tools as a package, providing a single, integrated business view of any number of heterogeneous data sources.

Based on this it can be interpreted that, Cognos is a complete performance management system built from the ground on a single, purpose-prepared SOA (Service-Oriented Architecture) platform. However its scalability leaves much to be desired – the loss of performance is significant while adding hardware and users in the same proportion.

Business Objects XI 3.0

Business Objects XI 3.0 is a BI product suite of Business Objects, an SAP company. New Crystal Reports 2008 is used as the report designer in the Business Objects Suite. The Business Objects Web Intelligence tool can be used as a rich client and can even be used in an offline mode to modify reports. Dashboard creation is possible using the Business Objects Dashboard Builder product. SAP Business is created as a single intelligence platform to reduce the effort necessary for cooperation of different users. Further, the clear and transparent structure of the platform enables an insight into the whole operations – every process within every level could be easily tracked/checked out (and modified if it's required).

JasperSoft Business Intelligence Suite

JasperSoft Business Intelligence Suite, an open source package, from JasperSoft is packaged with MySQL and the web server Tomcat such that it can be used out-of-the-box.

Further, it includes JasperServer for ad-hoc queries, reports, charts, crosstabs and dashboards. It is also possible to schedule, share, and interact with reports using JasperServer. JasperSoft Business Intelligence Suite also includes JasperAnalysis for OLAP and JasperETL. These are based on Mondrian/JPivot and Talend, respectively. Finally, the JasperReports reporting tool is included in the suite.

The suite's open source codebase also enables it to support third-party commercial and open source BI tools, which gives it its broad range of capabilities. One disadvantage of this approach is that while these tools extend the suite's functionality, Jaspersoft does not own or control these key BI components, or their roadmap or integration

Pentaho Open BI Suite

Pentaho Open BI Suite (open source software) from Pentaho does not have a DBMS in the package., however, preconfigured setups that use Firebird or MySQL do exist for easy testing. The suite includes Pentaho Data Integration, also known as Kettle. It also includes Pentaho Analysis with Mondrian and JPivot as well as Pentaho Dashboards. A reporting tool (based on JFreeReports) and the data mining tool Weka are also included.

Pentaho is an excellent choice for reports that are of simple to moderate complexity and don't require crosstabs or charts because Pentaho Report Designer does not offer as many levers to customize the report's contents, look, and behavior as the other tools.

5.2 COTS Deployment Options

There are several Commercial-off-the-Shelves (COTS) products/solutions available that either partially or almost completely provides the functionalities of integrated financial management system, described in section 4.7 of this report. The features of some these COTS products/solutions are set out in the section below:

5.2.1 Oracle E-Business Suite

The Oracle E-Business Suite has in its ambit several products that cater to the needs of an accounting organization. These products are:

- Oracle General Ledger
- Oracle Cash Management
- Oracle Purchasing
- Oracle Receivables

- Oracle Assets
- Oracle Hyperion Planning

The Oracle E-Business suite has been implemented successfully in government setups. Few such cases have been discussed in the sections 3 of this report.

Features

The key functionalities required by the CGA are listed below. An attempt has been made to map these functionalities against the respective Oracle products of Oracle E-Business suite

Functionality	Requirements	Product and Features
Budget Module	• Budget Preparation • Budget Authorization • Re-appropriation	**Oracle Hyperion Budgeting Solution** • Streamlined enterprise-wide planning. • Preparation of budget estimates / revised estimates of the respective departments at any level. • Prepare budgets based on 5 year historical data. • Budget Groups & hierarchies to control access to budget information. • Use of Workflow for distribution, submission, notification and approval to appropriate users at any given level of budget preparation process. • Microsoft Office integration reduces manual reporting and data entry efforts. • Built-in financial intelligence reduces administration efforts and enhances plan reliability. • Offline planning allows users to work on their plans anytime, anywhere.

.

Functionality	Requirements	Product and Features
		• Intuitive Web interface connects all users online. Plans can be accessed online from any location and approved online by the supervisory authority. • Task List wizard guides frequent users step by step through the planning process. • Scalable architecture supports large deployments to thousands of users.
Commitment Sanction Module	• Fund Commitments • Proposal Based Sanctions	**Oracle General Ledger (Oracle Financials Suite)** Certain aspects of the Oracle General Ledger product cover the functionalities of a Commitment Sanction Module. The features of the product are as follows: <u>Chart of Accounts</u> • Flexible Chart of Accounts catering to Governments requirements of Fund, Economic, Functional, Organizational & Program classification. • Journaling functionality with Validations & Approvals. • Maintenance of Departmental accounts in the respective departments. • Maintenance of User Charges Accounts. • Distribute appropriation and commitment authorizations to spending departments • Distribute funds allocations to spending departments. <u>Audit and Reconciliation functionality</u> • Internal audit of the Department Unit Offices and follow-up action for settlement of the audit objections. • Pre-audit of Bills and post audit of Vouchers. • Reconciliation of the receipts and expenditure of the department.

Functionality	Requirements	Product and Features
		• Reconciliation of the Department receipts and Expenditure. Payment and Receipt Records • Payment of Govt. Securities such as Stock Certificates, bearer bonds, promissory Notes and Income Tax deductions. • Debt management. • Receipt of Money into Treasury System. • Record revenue and other receipts against appropriate account heads Controls and checks • Budgetary Control & Funds Check • Structured control over allocation of Budget Funds across Ministries & Spending Units Reporting Functionality • Analyze, Budget, Forecast, Inquire and Report on Financial Data • Rendering financial advice to the Head of departments (Reporting)
Cash Management Module	• Revenue Projections • Expenditure Projections • Cash Position Monitoring	**Oracle General Ledger (Oracle Financials Suite)** The reporting functionality of the Oracle General Ledger caters to the requirements. Reporting Functionality • Analyze, Budget, Forecast, Inquire and Report on Financial Data. • Rendering financial advice to the Head of departments (Reporting).
Payment Management	• Budget Verification • Sanction Verification • e-Payment • Salary, Vendor Payments etc. • Accounting	**Oracle Payables** Bill Processing • Bill processing from concerned department DDO to treasury. • Record expenditure against fund allocation and budget. • Match bills with Purchase Orders for control.

Functionality	Requirements	Product and Features
		• Automated accounting with centralized accounting rules. • Multi level approvals engine with auto escalation. <u>Payment</u> • Payments Management including generating payments in batch mode with payment methods such as check, electronic or wire. • Generate EDI files as required by the Bank for payments through banks. • Streamlines Pay Cycle with budgetary control & Funds Check. • Print checks against payment instructions and/or make arrangements for the electronic transfer of payment information to an external paying entity (e.g. a bank) if required. • Prioritize payments based on different parameters. • Interface with Cash Management for e-scroll upload and reconciliation. • Online reporting for status report.
Loan Management		No Product Available
Internal Audit		**Oracle GRC Manager (Governance, Risk & Controls)** • Workflow enabled and helps automates the process of documenting the business process, testing, and certification with complete audit trail thus increasing the process efficiency of the audit function. • Helps organization to reduce audit spends and scoping challenges on financial, operational, compliance audits and certifications across the business functions. • This tool is also is very useful for non-financial audits also e.g. reviewing/auditing

Functionality	Requirements	Product and Features
		HR recruitment process. • Provides real time visibility into risk status through heat maps for example mitigated/unmitigated risks by business process/units with drilldown capabilities and also indicates when process or control is last tested and validated. It also has a prebuilt audit reports. • Ability to record NCR/issue to be tracked during the audit/ certification process and it can also generate necessary alerts. • Helps organizations to monitor the changes in business process with a version control and standardize business processes across different units within the organization.
Asset Tracking		**Oracle Fixed Asset (Asset Account Management)** • Ensure accurate accounting of assets, property and inventory. • Automate asset creation process by integrating with Disbursement system and Project Management. • Reduce the administrative effort of managing asset expenses, and optimize accounting strategies. • Facilitate massive processing of asset transfers, disposals, reclassifications, financial adjustments, and legacy data conversions. • Provide a global view of assets.

5.2.2 SAP Integrated Business Suite

SAP provides a solution covering all critical functions of required for a integrated financial management system. The functions are mentioned below:

- Planning, budget preparation, budget release, real-time budgetary monitor & control, approvals, workflow
- Expenditure management integrated with budgetary monitoring & control
- Recruitment to Retirement, Pension, Service Record maintenance complying to changing statutory
- Revenue Management
- Civil Account with complete Audit Management
- Debt, Investment and Guarantee Management
- Ways & Means Management
- Business Intelligence Tools
- Mobility Platform
- Document Management System
- Audit Para Management System

SAP offers a built-in flexible Analytical Reporting tool, which can be used by any end user to create his/her own report dynamically. The SAP Financial Accounting solution not only automates the Revenue Accounting operations, but also facilitates to ascertain real-time surplus/deficit of fiscal position. This helps to manage funds more prudently on a day to day or weekly basis.

The user can also look at different Revenue and Expenditure heads and compare their planned revenues and expenditures against the actual. Real-time availability of information would assist the user to take preventive actions to avoid deficits in the end of the year. The feedback loop created through these dashboards would increase revenue.The solution portfolio would cover the Finance Department operations integrating all the DDO, PAOs, Accounts General Office and other Government departments like PWD,Highways etc for their Contract Management and Bill passing and payment. SAP applications enable smooth functioning and provide information to enable Ministry/Bureaucrats to take optimized

decisions and improve government fiscal performance. SAP ERP Application can also be implemented in shared services format with other departments like PWD, Irrigation covering all the Public Administration operations including - Human capital management, Financial Management, Government procurement, Project Management, Tax and Revenue Management, Social services and Social Security and Citizen Relationship Management. All the solutions would be implemented in the flexible NetWeaver technology.

Highlights

SAP is Natively Integrated:

- SAP offers all the functionalities as a single application. All the functions envisaged for the proposed IGFMS are available as natively integrated applications on a single interoperable open platform.
- SAP Enterprise support at 22% has SLA based support, which not only ensures time bound resolution but also delivers robust mission-critical support (including custom code), 24x7 root cause analysis, and continuous quality checks, Shortened testing cycles and coordinated change management procedures,
- SAP Enterprise support has built-in, standardized tools for performing diagnostics, change impact analysis, and test administration, along with system and business process monitoring

India Localization:

- SAP has complete end to end - India localization features like TDS, Payroll etc.
- SAP may be available in Hindi from Q3 2012 onwards.

Technology :

- SAP enables real time postings.
- With the SAP Foundation Pack, a DMS, Portal, Workflow & Business Engines, the entire ERP Stack(HR/MM/PS) comes as part of the package without any additional cost.
- SAP is Database and OS Independent and runs on all leading Databases and OS.
- SAP provides wide range of security features such as authentication and authorization based on various parameters like location, function, transaction, etc, and single sign-on.

Features

The key functionalities required by the CGA are listed below. An attempt has been made to map these functionalities against the respective SAP products from the SAP Integrated Business suite.

Functionality	Requirements	Product and Features
Budget Module	• Budget Preparation, • Budget Authorization • Re-appropriation	**SAP Business Planning** • The SAP Business Planning solution completely covers all the Budget Preparation processes as explained below: 1) Number statement planning 2) Non plan expenditure budgeting 3) Receipt Budgeting 4) Aggregate resource budgeting 5) Top down allocation to PAOs 6) Top down allocation to DDOs 7) Plan expenditure budgeting by DDOs • SAP Business Planning delivers Workflow management, allowing Finance Dept to easily monitor the status of the planning process by Ministry structure. • The SAP Business Planning workflow status indicates entities that are in process, entities that have passed system validation rules, and allows to proactively identify if there have been changes which would impact the budget (i.e. impact to revenue projections, etc). • Managers/administrators have clear understanding of how the budgeting cycle is progressing. • Quickly identify process bottlenecks • Ensure compliance by enforcing review/approval requirements • Easily identify modifications that have impacted the planning process
Commitment Sanction Module	• Fund Commitments • Proposal Based Sanctions	**SAP Revenue and Expenditure Management** Commitment Creation

Functionality	Requirements	Product and Features
Cash Management Module	• Revenue Projections • Expenditure Projections • Cash Position Monitoring	**SAP Revenue and Expenditure Management** • Receipts of revenue collections through bank transfers • Upload the bank statements into the system with collection details • Account for funds credited into bank accounts • Account for the revenue collected in the respective revenue accounts • Check balance as per books and balance as per bank
Payment Management	• Budget Verification • Sanction Verification • e-Payment • Salary, Vendor Payments etc. • Accounting	**SAP Revenue and Expenditure Management** • Display of Budget distributed for DDOs • Commitment Creation • Bill Preparation at DDO's office • Checking and approval of bill • Budget availability check • Accounting of Bill • Issue of token number • Payment and agency bank • Bank reconciliation process
Loan Management		**SAP Treasury Management** • Deposits, Loans, Borrowings and Investments
Internal Audit		**SAP Account and Audit Management** • The SAP solution is very strong in carrying on the transactions with strong audit trail and internal check based SAP's Audit Management Solution enables Auditors from CAG office, to plan the Audit and raise queries during the course of audit, record the finds in the application itself. The same solution helps respondents to record their clarifications for the queries raised. Queries and Clarifications forms part of the records available for future reference, as long as the department wants to keep such records.

Functionality	Requirements	Product and Features
Asset Tracking		**SAP Asset Management** • Ensure accurate accounting of assets, property and inventory.

5.2.3 FreeBalance Accountability Suite

FreeBalance Accountability Suite is a Government Resource Planning suite which helps in improving the effectiveness of Public Financial Management (PFM) systems.
Some highlights of FreeBalance Accountability Suite are listed below:

Language and Localization

The FreeBalance Accountability Suite is a multi-language GRP that adapts to meet unique language requirements of a specific client. Some of the functionality provided by FreeBalance to meet the client specific language requirements is mentioned below:

- Language support facilitated through uploading translation files
- Multiple character set support includes Unicode
- Terminology adjustment after uploading translation

Integration

GRP systems need to integrate with a wide variety of automated sub-systems. The FreeBalance Accountability Suite leverages a component-based Services-Oriented Architecture (SOA) to facilitate integration:

- Supports integration with banks
- Supports integration with various revenue and expenditure systems of Government across different tiers
- Systems Management integration includes integration tools and support for identity management

Configuration

Configuration options enable rapid implementations and adjustments to support government legal reform. This approach includes:

- Built in support for International Public Sector Accounting Standards
- Configuration of functions through parameterization including supporting unique needs that require customization in traditional software
- Progressive Activation to support PFM reform and modernization

International Standards

The FreeBalance Accountability Suite supports good fiscal practice and is compliant with internationally recognized standards such as:

- United Nations Common Functions of Government (COFOG)
- The International Monetary Fund Government Finance Statistics (GFS)
- The International Monetary Fund Code of Good Practices on Fiscal Transparency
- Generally Accepted Accounting Principles (GAAP)
- International Accounting Standards Board, International Financial Reporting Standards (IFRS)
- International Federation of Accountants International Public Sector Accounting Standards Board
- International Public Sector Accounting Standards (IPSAS)
- Millennium Challenge Corporation (MCC)
- Medium Term Expenditure Frameworks (MTEF)
- The World Bank Treasury Reference Model

Configuration

As a standard configuration (out-of-the-box), the FreeBalance Accountability Suite supports a wide range of budgetary controls in compliance with international public finance rules and codes of good fiscal practice:

- **Aggregate Fiscal Controls**: The initial approved budgetary funds are mapped to the Chart of Accounts (COA) at a pre-determined COA hierarchy level for aggregate fiscal control
- **Multiple Levels of Allotment Controls:** Support for approved appropriations, warrants, cash controls, supplemental budgets and allocations, mapped to summary or detailed levels within the COA and to fiscal periods
- **Multiple Commitment Levels**: Pre-encumbrance, commitment and obligation controls
- **Multi-Funds and Project Controls** - Projects and Programs are linked with fund sources, including linking specific budgets, projects or programs to specific revenue sources or donors

The FreeBalance Accountability Suite adapts to meet many unique country needs including:

- **Chart of Accounts** design supporting consolidation, reporting objects, international standards, valid code combinations and accounting offsets multiple currencies, adjustment of fiscal periods, multi-year commitments, year-end and period-end procedures

- **Multiple accounting methods** (cash, modified cash, modified accrual and full accrual)
- **Workflow, business rules, forms and report configuration**
- **Custom domains** to support unique government information integrated with workflow, rules, forms and reports

Progressive Activation

Progressive activation supports the sequential activation of additional functionality though allowing ongoing changes to support evolving political processes and capacity building including:

- **Multiple year Chart of Accounts** to support changes to government structures, reporting requirements and performance considerations
- Upgrading accounting methods to full accrual accounting
- Adapting budgetary controls to support de-centralization, performance objectives, fiscal discipline and improved decision-making
- Adding additional modules to support the best-practice of phased PFM reform

Key Features

The key functionalities required by the CGA are listed below. An attempt has been made to map these functionalities against the FreeBalance Accountability Suite features and functionalities.

Functionality	Requirements	Product and Features
Budget Module	• Budget Preparation • Budget Authorization • Re-appropriation	The FreeBalance Accountability Suite is comprehensive Government Resource Planning (GRP) software designed to support Public Financial Management (PFM) including Budget Preparation, Authorization and Re-appropriation. The functionality is achieved through **Performance Budgeting** module to support credible budgets, forecasting and improved government performance including budget preparation, government performance management and a Key Performance Indicator (KPI) library. The system has built in **Multiple Levels of Allotment Control** for approved appropriations, warrants, cash controls, supplemental budgets and allocations, mapped to summary or detailed levels

Functionality	Requirements	Product and Features
		within the Chart of Accounts and to fiscal periods
Commitment Sanction Module	• Fund Commitments • Proposal Based Sanctions	FreeBalance has **Public Financial Management** module which helps in Budget and Commitment Accounting to support core government financial functions for federal government, line ministries, and projects. The module supports the following functionality: • **Multiple Commitment Levels**: Pre-encumbrance, commitment and obligation controls • **Multi-Funds and Project Controls** - Projects and Programs are linked with fund sources, including linking specific budgets, projects or programs to specific revenue sources or donors
Cash Management Module	• Revenue Projections • Expenditure Projections • Cash Position Monitoring	The Government Treasury Management Module in FreeBalance system has **Cash Management** sub-system to optimize liquidity including cash forecasting based on the commitment cycle, historical trends and manager reports The **Government Performance Management** module in FreeBalance helps in: • **Performance Budgeting** to support credible budgets, forecasting and improved government performance including, government performance management and a Key Performance Indicator (KPI) library • **Monitoring and Evaluation** to support improved decision-making including records management, reporting, data mart, dashboards and alerts • **Government Transparency** to support publishing performance and budget information
Payment Management	• Budget Verification	**FreeBalance** has in built system which supports **Aggregate Fiscal Controls** where initial approved

Functionality	Requirements	Product and Features
	• Sanction Verification • e-Payment • Salary, Vendor Payments etc. • Accounting	budgetary funds are mapped to the Chart of Accounts (COA) at a pre-determined COA hierarchy level for aggregate fiscal control. **Public Expenditures Management** module has following functionalities: • **Expenditures and Purchasing** to support expenditure controls for standard expenditures including payment management, multiple purchasing vehicles and the purchasing cycle • **Procurement** to support fiscal discipline on large scale government acquisitions including tendering, e-procurement, contract and spend management. **Government Receipts Management** module serves following functionality • **Non-Tax Revenue** to support government sales and other income including sales, permits and licensing • **Tax Revenue** to support tax administration for income, business, import and property • **Billing and Receipts** to support receipts collection including utility billing, collections and cashiering **Bank Reconciliation** sub-system of the Government Treasury Management supports multiple currency bank management including **reconciliation** processes. **Civil Service Management** module of FreeBalance has following sub-systems • **Human Resources** to support civil service reform and management including movement, capacity building, salary planning, performance appraisal and recruitment • **Payroll and Pensions** to support government rules for payroll and pensions • **Benefits and Self-Service** including civil service

Functionality	Requirements	Product and Features
		benefits, travel and subsistence and self-service portals
Loan Management		**Debt and Investment Management** sub system supports debt servicing and the modelling of debt and investment financial vehicles **Grants and Social Programs** sub-system of Public Expenditures Management module accounts for government grant, loan and contribution management
Internal Audit		**Government Transparency** sub-system supports publishing performance and budget information to a transparency portal and **computer-aided audit**
Asset Tracking		FreeBalance **Assets and Inventory** is a fully integrated web-based module. Assets and Inventory includes four optional sub-modules to manage Fixed Assets, Property and Facilities, Inventory and Stores, and Fleet Management which enables efficient management of public assets and real-time information on purchases, asset sales, maintenance, operation, and disposal of assets. FreeBalance Assets and Inventory supports fixed asset accounting, depreciation and inventory stores, consistent with the move to accrual accounting.

A comparison of the above COTS products/solutions has been done vis-a-vis the requirements of the integrated financial management system by the office of CGA. The comparison is in the table below:

Parameters	Oracle e-Business Suite	SAP Integrated Business Suite	FreeBalance Accountability Suite
Conformance to CGA requirements	Almost all requirements are covered, except full-fledge loan and debt management functionality. But covers loan and debt functionality as required by the office of CGA	Covers all the functionalities as required by the office of CGA	Covers all the functionalities as required by the office of CGA
Ease of Implementation	The solution/product will be customized by an Implementation Agency (IA)/System Integrator (SI).		The implementation will be carried out

Parameters	Oracle e-Business Suite	SAP Integrated Business Suite	FreeBalance Accountability Suite
	The ease of implementation will depend on the ability of the IA/SI to work with a particular OEM (Oracle/SAP)		FreeBalance team. The ease of implementation will solely depend on the ability of FreeBalance to implement/customize its solution/product.
Cost of Implementation	The cost of licenses and customization/implementation is higher in case of SAP		*[9]
Success Stories of implementation of Financial Management System in Government	UK –Department of Works and Pensions, UAE	Israel, Govt of Catalonia Spain, Singapore	States in Canada, Vietnam (around 19 countries of the world).

5.2.4 Budgetary Estimates for COTS Implementation

Budgetary Estimates for COTS implementation are set out below:

Budgetary Estimates (in Crs)									Assumptions
S. No	Item	Details	Y1	y2	y3	y4	y5	Total	
1	Cots Software Cost (one time cost for 40000 users)	This is the cost of application and database. It's a one time cost. Only additional licenses beyond 40000 are to be bought.	45	0	0	0	0	45	40000 users will be working on the system once its fully functional
2	Payroll Processing (one time cost for 3000000)	This is the cost of a the running payroll. It's a one time cost. Only additional licenses beyond 3000000 are to be bought	15	0	0	0	0	15	2000000 employees and 1000000 pensioners
3	Licence Support Cost for 5 years	22% of the total license cost	0	13.2	13.2	13.2	13.2	52.8	Industry standard is 22%

[9] Cost estimates of FreeBalance are not available

Budgetary Estimates (in Crs)									Assumptions
S. No	Item	Details	Y1	y2	y3	y4	y5	Total	
4	Customisation and Implementation Cost Plus Support Cost for SI	Normally taken as 1:1 of cost of license cost as a budgetary estimate. Details in Implementation Effort Sheet	30	30	6	6	6	78	Customization Cost is in the ratio of 1:1 of total license cost. It is assumed it would be spread over first to years equally (i.e. 30 in year 1 and 30 in year 2). From year 3 onwards 10% support cost is estimated as per the industry norms
5	Hardware	50% of the Services Cost	30	0	0	0	0	30	Industry estimate for budgetary purposes
Total			120	43.2	19.2	19.2	19.2	220.8	

6 Data Centre and Disaster Recovery (DR) Planning

The Data Centre is a key element of the IT Infrastructure for hosting the applications and data reliability, availability and serviceability. The guidelines for data centre mentioned at **Annexure 13.1** provides better operations & management control and minimizes overall cost of data management, IT management, deployment etc.

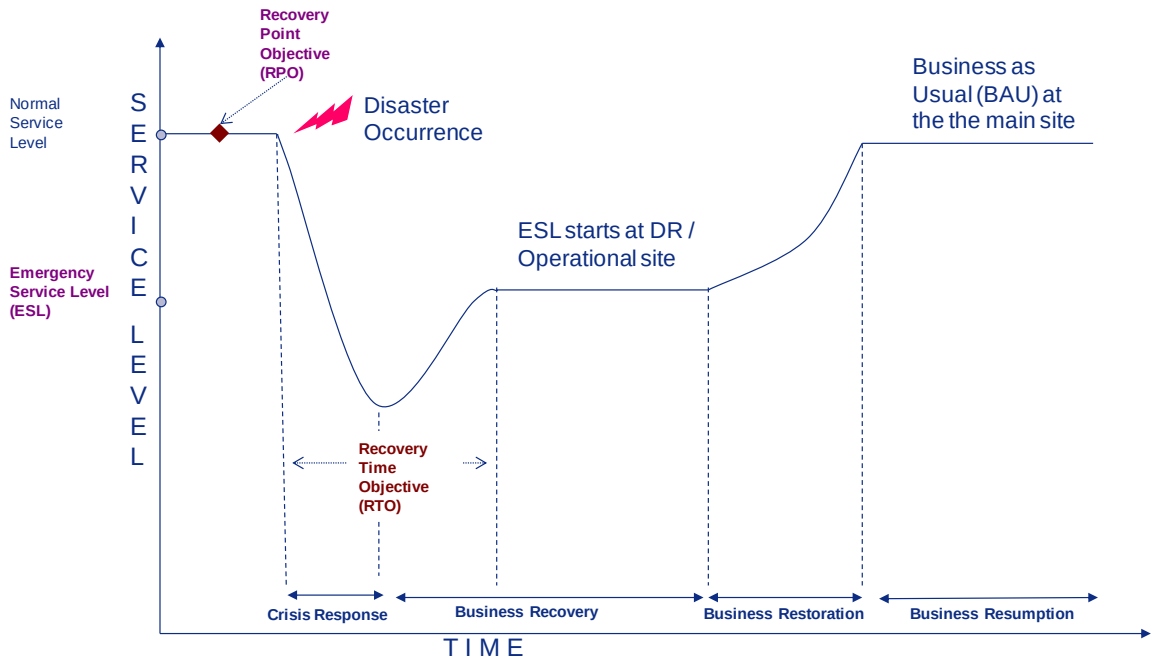
6.1 Disaster Recovery Planning

Disaster Recovery is the strategic and tactical capability of the organization to plan for and respond to disruptions in order to continue IT operations at an acceptable pre-defined level The Disaster Recovery Planning (DRP) aids an organization in:

- Formulating **strategies to reduce the impact** of disasters;
- **Shortening of response time** during a disaster;
- **Prioritization of systems** for recovery;
- **Ensuring continuity of core IT systems/ applications**; and
- **Optimally utilizing** the available resources

6.2 DR Key Concepts

Disaster recovery plan focuses on applications, databases, servers and device level recovery plans. The schematic below shows the key terminologies of a disaster recovery plan.



Maximum Tolerable Period of Disruption (MTPD)

It is the disruption period, after which the organization's viability will be irrevocably threatened, if product/ service delivery cannot resume.

Recovery Time Objective (RTO)

Target time set for resumption of product/ service delivery after a disruption.

Recovery Point Objective (RPO)

It is the maximum data loss acceptable in event of a disaster. Also it is defined in terms of backup frequency.

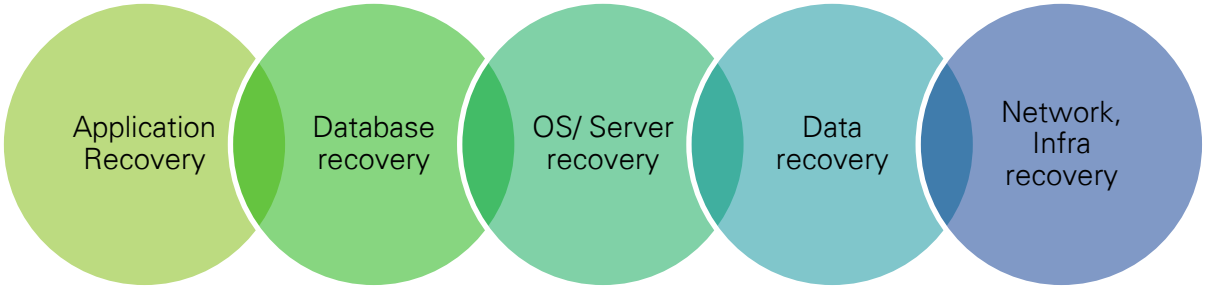
Essential Service Level (ESL)

It is the minimum acceptable level of operations required during business continuity/ disaster recovery phase. **ESL is defined in terms of network throughput/ latency/ application load/ licenses etc**

The Disaster recovery solution needs to meet all of the above parameters.

6.3 DR Strategy

A set of strategic options are selected to manage the impact of a disaster and recover its operations these includes:



6.3.1 Network/ Infra Recovery

Key Network and Infra Components

- Domain Controller
- DHCP
- DNS
- WAN
- LAN (limited scope)

Recovery Strategies

- Active Directory
    - Local DCs synced with parent domain controller

- DNS Server
  - Secondary DNS Server at DR site
  - Routing and MX records
- Alternate DHCP server at DR site/ Local DHCP server
  - Routers/ firewall configuration
- Resilient WAN
  - Redundant links (two MPLS, leased lines, radio or VSAT links etc)
  - VPN
- LAN
  - Wireless access points
  - Segregate key LAN segments
  - Redundant LAN for data centre

6.3.2 Data Recovery

There are four key options for Data Recovery

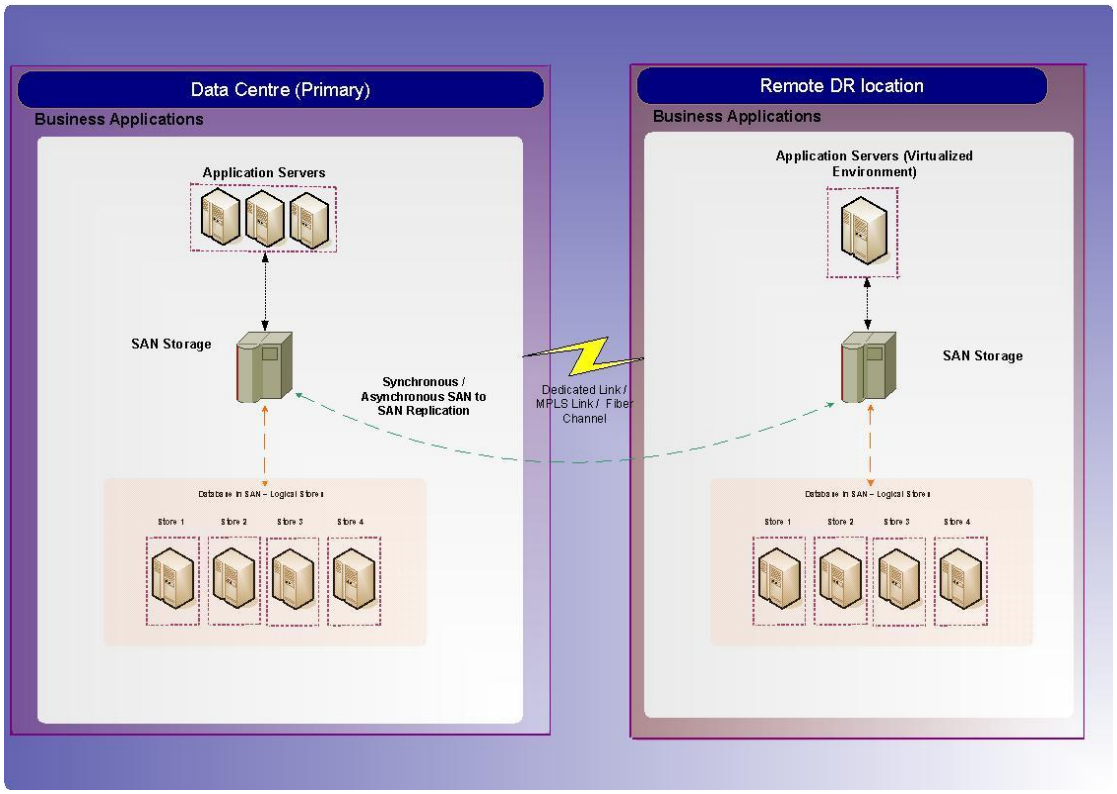
a) Storage based solutions

b) SAN/ Fabric based solutions

c) Host based solutions

d) Backup and Restore

The diagram below provides overview of data recovery strategy.



a) Storage based solutions

Overview

- Two identical storage solutions (SAN) – one at primary and one at DR site
- Data transfer over IP
- Logical volumes and corresponding replication frequency can be defined
- Two way replication

Licensing Model

- Per storage solution (box) based – does not depend on number of servers/ data transferred

Key Vendors

- EMC, NetApp*

The advantages and challenges of data recovery mechanism using storage based solution are mentioned as under:

Advantages	Challenges
1. Does not impact host server performance 2. Simple to implement and maintain 3. Value adds – Snapshot, flexible volume tech etc	1. Does not optimize bandwidth utilization 2. Heterogeneous environment not supported 3. Servers' local disk data needs to be migrated to storage device

b) SAN/ Fabric based solutions

Overview

- Two SANs (not necessarily of same vendor) - one at primary and other at DR
- Fiber Channel/ IP converters at each site
- Direct SAN to SAN replication

Licensing Model

- Data volume based

Key Vendors

- EMC, NetApp, Hitachi, IBM etc

The advantages and challenges of data recovery mechanism using SAN/ Fabric based solutions are mentioned as under:

Advantages	Challenges
1. Does not impact host server performance 2. Allows heterogeneous environment 3. Bandwidth optimization possible	1. High cost of FC/IP converters 2. Licensing model concerns

c) Host based solutions

Overview

- A software (agent) is installed on each server
- Replicates server's data to corresponding server at DR
- Supports any storage mechanism (local disk, SAN, NAS etc)
- Primary and DR storage mechanism may be different (e.g. SAN to local disk)
- Data transfer over IP

Licensing Model

- Physical server based
- Virtual Machine licensing

Key Vendors

- Symantec Veritas, EMC

The advantages and challenges of data recovery mechanism using host based solution are mentioned as under:

Advantages	Challenges
1. Ease of implementation and maintenance 2. Supports all storage mechanisms	1. Performance concerns

d) Backup and Restore

Overview

- A backup utility is used at primary site
- Backup media (such as tapes) is sent to the DR site
- Data is restored on to DR site storage

Licensing Model

- Multiple models

Key Vendors

- Symantec Veritas, Microsoft etc

The advantages and challenges of data recovery mechanism using Backup and restore solution are mentioned as under:

Advantages	Challenges
1. Ease of implementation and maintenance 2. Low cost	1. Cannot support low RTO/RPO

6.3.3 OS/ Server Recovery

There are two key options for Server/ OS Recovery

Hot / Live DR

The servers at DR site are always 'live'. The switchover to DR site servers may be automatic or manual. The data is typically near real time replica of primary site.

Cold/ Need based DR

The servers at DR site are bought 'live' on need basis. The data at the DR site may be as per the last backup.

6.3.4 Database Recovery

All leading databases have their own solutions for Database level recovery. Also all leading Storage vendors provide specialized solutions for DB.

Oracle Database

Oracle Streams

- Integrated with Oracle
- Satisfies all data sharing needs, is manageable and flexible

Oracle DataGuard

- Included with Oracle Enterprise Edition and above
- Provides automatic failover and easy-to-manage switchover

Microsoft SQL Server:

Microsoft SQL Server 2000 Enterprise Edition offers the following integrated features for disaster recovery

Transaction replication

– For less data to protect, and for a fast recovery plan

Log shipping

– For maintaining Warm standby server

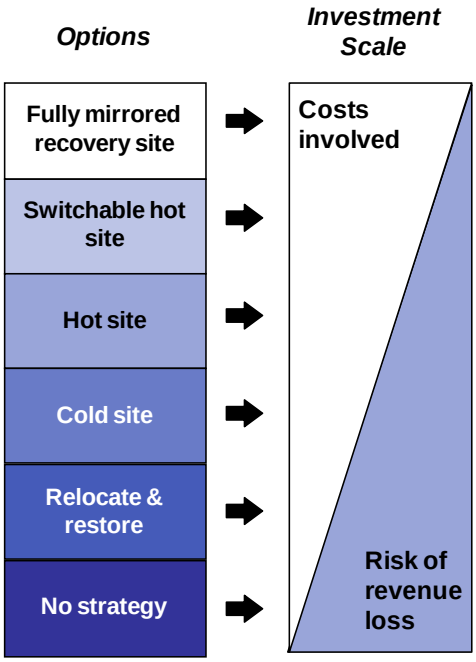
DB2

- RepliData
  - Requires DB2 Universal Database, Version 6 or later
  - To provide remote Hot-Site backup
  - Provides High performance at low latency
- FlashCopy
  - FlashCopy Cloning (FC Cloning) is a component of Tivoli Storage Manager (TSM) based FlashCopy Solutions for SAP (FC Solutions), especially powerful for improving operational flexibility and administration productivity in SAP environments.

- Ideally suited for database cloning, esp. for large and intensively used databases, because it is fast (short time to recover and to access copy) and can be used in an adhoc manner.

6.3.5 Application Recovery

Many leading applications have their own application level recovery solutions. Customized solutions may be built using appropriate storage replication and application server replication.



a) Lotus Notes

- Dominos based replication
- SAN to SAN replication in case the database is on SAN
- Network device / appliance based replication of the mail database

b) MS Exchange

- Exchange Cluster Continuous Replication (CCR) for

c) MS Exchange 2007

- Logical structures of mail database for faster recovery
- Providing blank email boxes to user till recovery of mail database

Other options include

a) Local continuous replication (LCR): LCR is a single-server solution that uses built-in asynchronous log shipping and log replay technology

b) Standby Continuous Replication: Offers separation of high availability and site resilience.

d) ERP

DRP for leading ERP applications are mostly customized; may be built using appropriate storage replication and application server replication

SAP

- SAN to SAN replication in case the database is on SAN
- Database level replication based on the database employed
- No separate licensing requirements

BAAN

- SAN to SAN replication in case the database is on SAN
- Database level replication based on the database employed
- No separate user based licensing requirements; server licensing required

Disaster Recovery Planning (DRP) includes planning for recovery at all levels – application, database, OS/server, data, network/infrastructure, various options/mechanisms have been defined for disaster recovery at these levels. But as a prerequisite to determine which option is suitable for a particular DRP a detailed **Risk Assessment** and **Business Impact Analysis** for key business functions is required, based on which RTO, RPO and ESL can be determined. The implementing agency after the implementation of the system could suggest whether it would be feasible to reduce the RPO and RTO any further.

7 Electronic Data Archival System

Data archiving and retrieval is an important task for the CGA, and has become even more essential with the enforcement of the RTI. The CGA is bestowed with the responsibility of maintaining accounts related data of over several years and, whenever required, should be in a position to retrieve any archived data in a matter of a few minutes. Thus, the numerous challans, bills and other hard-copy documents that are at the moment archived manually should be digitized first and then archived electronically. The electronically archived documents should be tagged with the required meta-data to enable quick electronic searches whenever required. To meet such needs there is a requirement of a proper data archival mechanism.

In order to have an efficient data archival system there are certain standards that should be followed. The standards that should be taken into consideration for this purpose should cover:

- Designing and maintaining records classification systems;
- Identifying records with archival value;
- Determining the conditions for the management of electronic records;
- Training government officials in records management; and
- Inspecting the records management practices of governmental offices

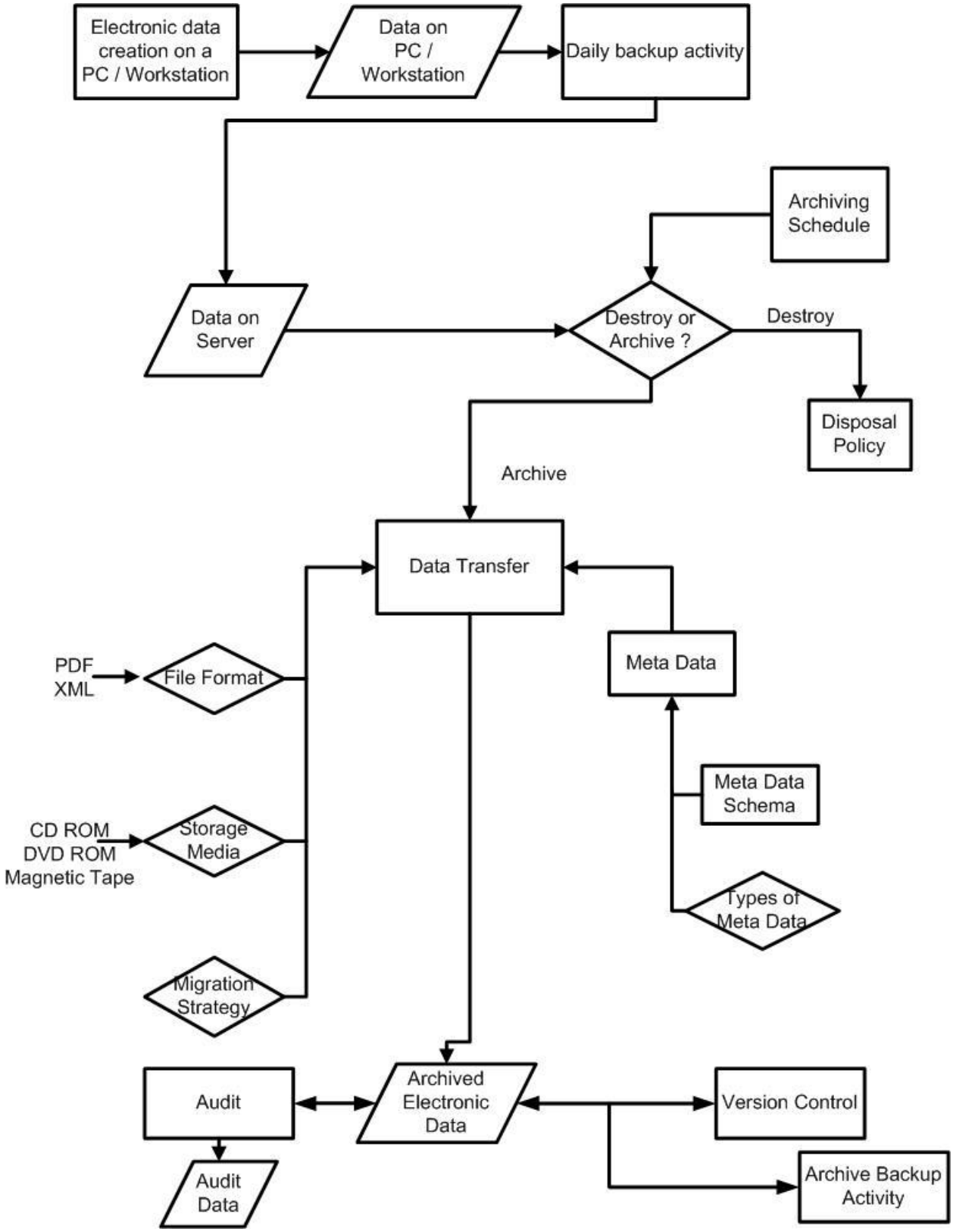
In addition to these, there are many useful international standards from the International Organization for Standardization (ISO) covering detailed technical issues related to electronic document formats. There are also guidelines and standards available from other countries and other international bodies.

To implement an archival mechanism there is a need to implement and bring in place a digital archival policy. With respect to archiving digital information, the following are important examples of archiving standards that are applicable for digital archiving in a government department:

- ISO 18938:2008, Imaging materials – Optical discs – Care and handling for extended storage.

- ISO/TR 18492:2005, Document Management Applications – Long term preservation of electronic document-based information.
- ISO 19005-1:2005, Document management – Electronic document file format for long term preservation.
- ISO 15489-1:2001, Information and documentation – Records management. Part 1: General
- ISO/TR 15489-2:2001, Information and documentation – Records management. Part 2: Guidelines

A typical data archival mechanism work flow that could be followed and implemented at the CGA's organization is shown in the figure on the following page. The workflow depicts the archiving of electronic data based on a pre-determined archive schedule and a disposal policy. The electronic data that is to be archived would be in a standardized format such as PDF and indexed using meta-data. The archived electronic data should have a proper version control mechanism for audit purposes and should be backed up regularly as per the data backup policy.


Electronic data creation on a PC / Workstation
Data on PC / Workstation
Daily backup activity
Archiving Schedule
Data on Server
Destroy or Archive ?
Destroy
Disposal Policy
Archive
Data Transfer
PDF
XML
File Format
Meta Data
Meta Data Schema
CD ROM
DVD ROM
Magnetic Tape
Storage Media
Types of Meta Data
Migration Strategy
Audit
Archived Electronic Data
Version Control
Audit Data
Archive Backup Activity

8 Quality assurance and Quality control

8.1 Quality assurance

Quality assurance with in terms of development of an IT system refers to means of monitoring the software engineering processes and methods used to ensure quality. The methods by which this is accomplished are many and varied, and may include ensuring conformance to one or more standards, such as ISO 9000 or a model such as CMMI. But the proposed system is required to be tested by STQC before the rollout. The STQC testing would include both functional and nonfunctional tests which may also include the performance load.

8.1.1 Adherence to Standards

The standards to be followed in SDLC (Software development Life Cycle) are mentioned below:

- Software Requirements Specification IEEE 830
- Software Design Description IEEE 1016
- Software Validation & Verification Plan IEEE 1012
- Software Test Documentation IEEE 829
- Software Project Management Plan IEEE 1058
- Software Quality Assurance Plan IEEE 730
- Software Configuration Management Plan IEEE 828
- Portal development Guidelines for Indian Government website (GIGW)
- Information access/transfer protocols: SOAP, HTTP/HTTPS
- Interoperability: Web Services, Open standards, XML Standards
- Master Data: Metadata standards
- Scanned documents: Pdf (ISO 32000)
- Digital signature: PKCS#7 (As per the IT Act 2000)
- Document encryptions: PKCS specifications
- Information Security system to be ISO 27001 certified
- IT Infrastructure management ITIL / EITM specifications

- Service Management ISO 20000 specifications
- Project Documentation IEEE/ISO/CMMi (where applicable)

8.2 Quality Control

It includes set of procedures used to ensure that the proposed IT system meets requirements related to quality. The parameters of quality control are mentioned below:

a) Application Audit

Comprehensive application audits to be conducted at regular intervals through a 3rd party to ensure application functionality and integrity.

b) Version Control

The application software shall be version controlled, adopting the industry standard practices like Version Control System (VCS), Source Code Management System and Software Configuration Management (SCM) etc.

c) Role Segregation

The roles of different personnel responsible for designing, coding, accepting the changes and authorizing the changes to be carried out into the production environment shall be clearly defined by the implementation agency.

9 IT Governance Structure

Putting a governance structure around CGA's future IT implementation plan is essential to ensure that project implementation stays on track, achieve its strategies and IT goals. It acts as a mechanism to measure IT system's performance. It makes sure that all stakeholders' interests are taken into account and that new systems provide quantifiable outputs. Also IT systems today are subject to many regulations governing data retention, confidential information, financial accountability and recovery from disasters; an IT governance framework is an efficient system to ensure regulatory compliance.

A four-tier IT Governance structure may be constituted considering the wide scope of work and large number of stakeholders in CGA Accounting organization. This four-tier structure can be divided into the following groups:

1 Project Steering Committee (PSC)

2 Project Management Group (PMG)

3 Project Advisory Group (PAG)

4 Project Implementation Group (at CGA and Ministry)

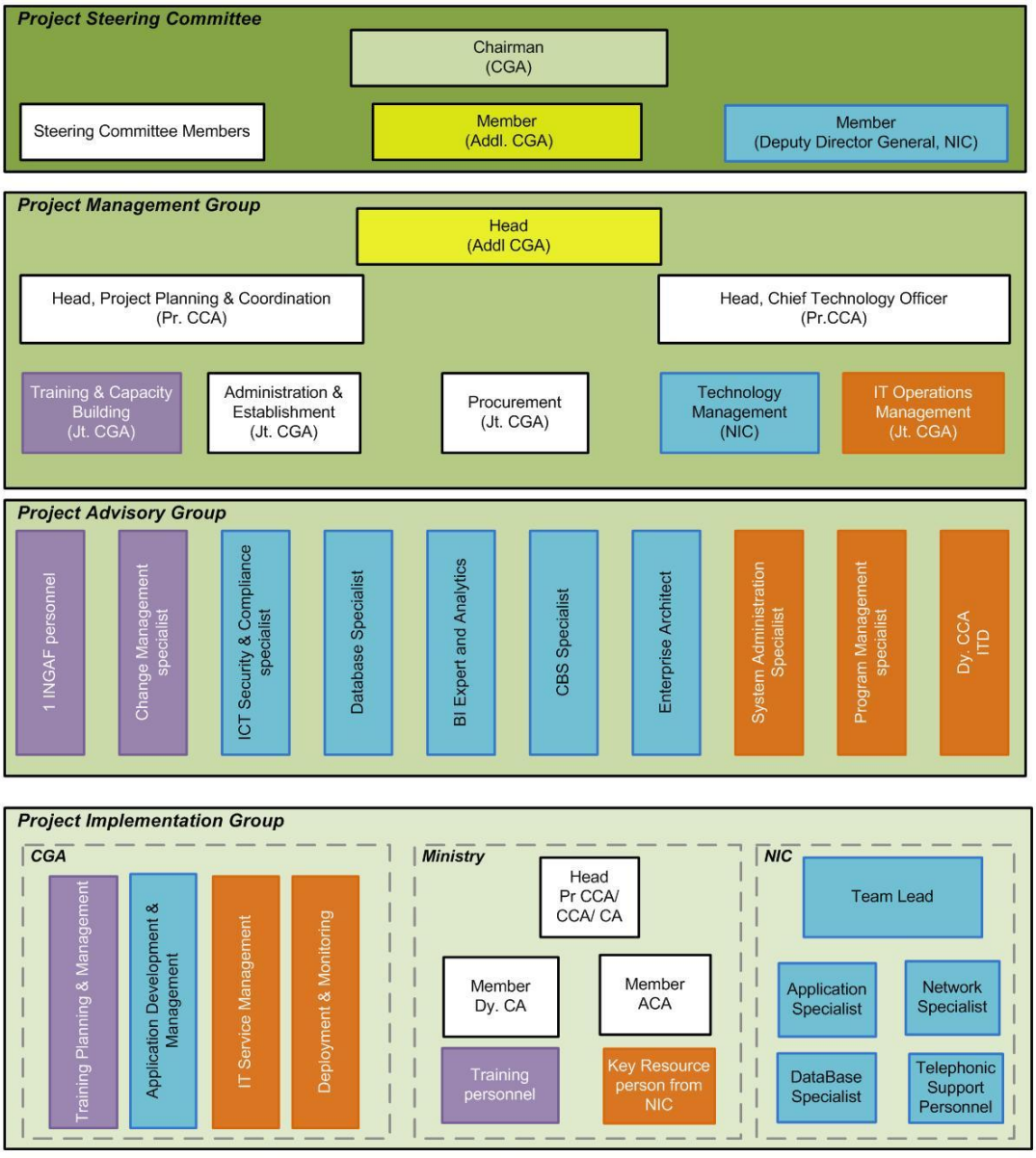
The Project Steering Committee (PSC) headed by CGA shall function as the apex unit for policy advice and strategic guidance on various project aspects. PSC shall be responsible for all the key decisions for the project. The existing Steering Committee members shall be the part of PSC along with Additional CGA and DG (NIC)

It is proposed to setup a **Project Management Group**. This shall function as Mission Execution Team and shall be assisted by **Project Advisory Group** which would consist of consultants with experience in various domains ranging from technology, banking and government accounting and shall bring necessary synergy in Project Management Group.

At the support level **Project Implementation Group** shall act as a bridge between the various stakeholders and Project Management Group in implementation of various project components. The implementation group shall have specialist from implementing agency in the areas pertaining to Application Development & Management, IT Services Management, and Deployment & Monitoring and shall be responsible for day to day operational activities.

All team members in Project Advisory Group shall report to respective Divisional heads in Project Management group.

The proposed schematic of IT Governance is set out below:



9.1 Roles and Responsibility

Considering the impact on overall Public Finance Management system in the country, it is proposed that dedicated teams of people from diverse backgrounds with clearly identified roles and responsibilities shall be appointed. The indicative roles and responsibilities chart is set below:

S. No	Role Description	No. of Positions	Roles & Responsibilities	Responsibility Centre
1	Head Project Management Group	1	• Overall responsibility for IGFMS implementation is consultation with PSC. Shall head the Project Management Group in the O/o CGA, New Delhi and supervise the implementation of the IGFMS. • Shall also be a member of the PSC, update the unit on project progress, highlight dependencies and take necessary approvals for Project Management group functioning. • Conduct monthly review meetings of Project Management and Advisory Group and assess the IGFMS status • Shall have the authority to approve deliverables, authorize changes, release circulars/notifications, recruit requisite manpower and take critical decisions with respect to IGFMS implementation	Addl. CGA or equivalent
2	Head of Division- Policy, Planning and Coordination	1	• Ownership for strategy to sensitize all Ministries, departments about the IGFMS, from creating awareness about	Jt. CGA Admin/ Co ordination

S. No	Role Description	No. of Positions	Roles & Responsibilities	Responsibility Centre
			the same, taking stakeholders buy in at various Ministries, and departments. Shall be further supported by dedicated training & capacity building team. • Shall spearhead the Coordination strategy for IGFMS across all stakeholders. • Shall coordinate within various Project Management Group to finalize a comprehensive reporting framework which shall cater to various stakeholders especially decision makers for supervising implementation.	
3	Head of Division- Chief Technology Officer	1	• Ownership for defining technology framework for IGFMS. Finalize technology integration framework for various heterogeneous IT environments across Ministries, NSDL, Core Banking System, RBI and CPAO. • Shall liaison with various Government Departments functioning in technology domain such as NIC, STQC, UID and Department of Information Technology. Shall ensure compliance to the specifications defined by these departments in the area of Application design, Infrastructure and management. • Define business needs and ensure compliance to	Jt. CGA ITD

S. No	Role Description	No. of Positions	Roles & Responsibilities	Responsibility Centre
			information security guidelines, interoperability standards, data storage requirements and business continuity principles are adhered to. • Assess technology obsolescence risk and propose technology risk mitigation plan. • Ownership of operational level Project management activities on day to day basis. Shall be responsible for defining the business requirements for change management, finalizing the scope of work for various outsourced agencies/consultants, guidance for vendor selection through bid management process, vendor management in terms of agreement, SLA compliance and payment recommendations. • Shall define project monitoring framework, project risk assessment framework and risk mitigation plan. Shall be instrumental in assessing the effectiveness of IGFMS implementation.	
4	Administration & Establishment	1	• Shall manage all administrative activities of IGFMS, from physical security, facility management, financial approvals/payments to outsourced resources, salary of	Dy. CGA

S. No	Role Description	No. of Positions	Roles & Responsibilities	Responsibility Centre
			in-house IGFMS resources, and release of official circulars to maintenance of administrative records.	
5	IT Operations Management	1	• Shall be the Head of IT Operations for IGFMS, managing the technology requirements of IGFMS, define technology standards to be adopted, define Information Security framework, ICT infrastructure policy, Quality assurance framework, Business Intelligence requirements, integration approach for CBS and Treasury. • Periodic review of solution architecture, overall technology standards and relevance to emerging technology trends. • Shall coordinate with Project advisory group and implementation group. • Shall define technical support and maintenance guidelines for IGFMS • Shall ensure user support for various stakeholders and users in ministries, departments	Dy. CGA
6	Training & Capacity building	1	• Shall be responsible for overall implementation of Change management plan. • Shall identify various stakeholders groups, training needs and suggestive training	Dy. CGA

S. No	Role Description	No. of Positions	Roles & Responsibilities	Responsibility Centre
			modules. • Shall design overall change management framework including communication plan, training content guidelines, training plan for various level users and other change management related activities throughout the project duration • Shall be responsible for assessment of Change management program and required upgradation. • Shall play key role in empanelment of Change Management and training agencies at Project implementation group.	
7	Procurement	1	• Shall be responsible for all the operational activities related with hiring of Consultants/ Vendors from RFP publication, bid management, contract finalization, termination, extension to sub contracting activities	Dy. CGA
8	Technology Management	1	• Shall be responsible for anchoring the design and development of the IGFMS application from the Technology perspective and providing technical inputs to various other verticals whenever required on the domain	Sr. Tech Director NIC
Project Advisory Group				

S. No	Role Description	No. of Positions	Roles & Responsibilities	Responsibility Centre
9	Program Management Specialist	To be decided by PSC and PMG	• Run IGFMS from design and development to production. • Define requirements and plan project lifecycle deployment. • Define resources and schedule for IGFMS project implementation. • Create strategies for risk mitigation and contingency planning. • Plan and schedule project deliverables, goals, and milestones. • Direct and oversees project implementation team and manages conflicts within group. • Efficiently identifies and solves project issues. • Define requirements for project risk. • Develop Requests for Proposals (RFP) for external services. • Design and maintain technical and project documentation.	Outsourced agency
11	Enterprise Architect	To be decided by PSC and PMG	• Develop information technology model that meets the needs of IGFMS according to the strategy and goals envisaged. • Provide guidelines and training other members of staff on how to utilize the system • Document the development and changes in the enterprise architecture.	Outsourced agency

S. No	Role Description	No. of Positions	Roles & Responsibilities	Responsibility Centre
			• Keeping track of the business plans and any current plans that are being made which shall require IT resources • Monitor and review the success of the system and ensuring its effective and efficient running • Incorporate the needs of the organization with IT. This involves fusing together the functional needs of the business with IT systems • Work in connection with other IT experts in the organization • Perform Business modeling, Business Process design, Role design, Organizational design and application design. • Analyze systems behavior, solutions modeling, building Blocks design, Architecture views and viewpoints design and awareness of IT industry standards.	
12	Business Intelligence and Analytics Head	To be decided by PSC and PMG	• Identify and document key business processes related to the use of information • Identify data sources, develop a conceptual data model , ensure adherence to data standards and develop prototypes for reports • Review report designs and prototypes with project team,	Outsourced to agency

S. No	Role Description	No. of Positions	Roles & Responsibilities	Responsibility Centre
			business users.	
13	System Administration Specialist	To be decided by PSC and PMG	• Oversee SLA configuration and monitoring. • Monitor configuration management and submit configuration amendment reports • Administer and monitor the helpdesk/problem handling system. • Create strategies for risk mitigation and contingency planning. • Provide regular feedback/reports to users with regard to problem solving, quality of data, customer needs, network planning, environmental problems and resources. • Monitoring of corrective action post reporting of problems to customer service centre. • Provide technical consultation and IT business advice. • Participate in system commissioning including testing and acceptance. • Monitor records and statistics with respect to IT and related equipment, network infrastructure user location, network hardware etc. • Ensure conformance to quality standards, liaison with service	Outsourced to agency

S. No	Role Description	No. of Positions	Roles & Responsibilities	Responsibility Centre
			organizations. • Maintain technical documentation. • Strong organizational, presentation, and customer service skills	
14	Core Banking System Specialist	To be decided by PSC and PMG	• Conceptualize a process integration model that meets the needs of IGFMS according to the strategy and goals envisaged and involves minimum change / modification is the Banking business processes. • Providing guidelines and training to members of staff responsible for developing and maintaining the CBS-IGFMS interface • Coordinate between Banks and IGFMS project team and mediating process changes required at both ends • Track changes in Banking regulation and new Banking technology developments, identifying and communicating the impact of the same on CBS-IGFMS interface to the IGFMS project team. • Monitor and review the success of the interface and ensuring its effective and efficient running. • Proficiency in Business	Outsourced to agency

S. No	Role Description	No. of Positions	Roles & Responsibilities	Responsibility Centre
			modeling, Business Process design, Role design, Organizational design and application design.	
15	Information Security & Compliance specialist	To be decided by PSC and PMG	• Address key security and privacy requirements and implement using appropriate technologies and thereby design secure business solutions. • Provide recommendation and solutions to make appropriate use of PKI, intrusion detection /prevention, VPN, single sign-on, firewalls, and all elements of application-level security. • The information Architect should provide solutions to complex security-related architectural issues.	Outsourced to agency
16	Database expert	To be decided by PSC and PMG	• Serve as the lead technical resource in the strategic oversight and planning of data models and database structural design and development • Oversees the design, evaluation, selection, implementation and support of major databases and metadata structures, review and evaluate database performance, risk and financial analysis feasibility studies. • Develop data and metadata policies and procedures for	Outsourced to agency

S. No	Role Description	No. of Positions	Roles & Responsibilities	Responsibility Centre
			structural design and development to build, maintain and leverage the data model, ensuring integration with corporate data standards. • Provide extensive technical, strategic advice and guidance of the highest level to senior managers and technical resources in the creation and implementation of new data standards and databases • Provide technical oversight and direction to designated boards for integrating new technology or major new mission capabilities into the metadata and data standards and structures • Provide complete assessments of the technical characteristics of proposals and alternatives considered to optimize database performance. Reviews and assesses technical proposals requesting changes or upgrades to the existing databases	
17	Change Management Specialist	To be decided by PSC and PMG	• Coordinate with Project Management Group (Jt. CGA, Training and Capacity Building) and drive the vision for change management • Active planning in change management initiatives at	Outsourced to agency

S. No	Role Description	No. of Positions	Roles & Responsibilities	Responsibility Centre

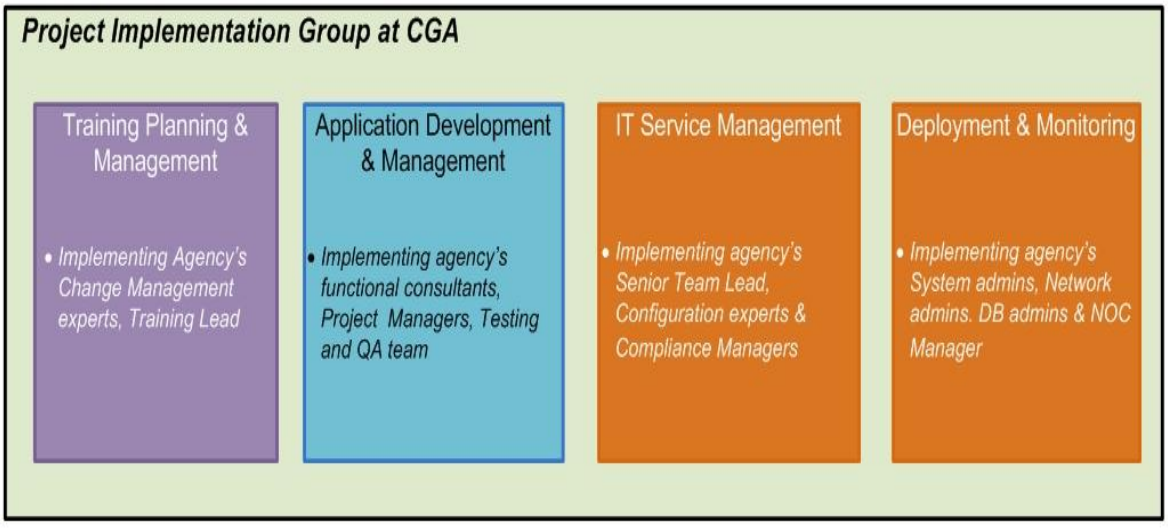
			policy level.
			• Monitor the progress of the project and facilitate Implementation Teams in overcoming training related issues
			• Draft overall Change management framework for teams including-
			  • User profiling
			  • Training needs assessment
			  • Guideline for training content creation and key training modules
			  • Detailed training calendar
			• Training feedback mechanism and overall assessment of Change management initiatives
			• Resolve conflicts, identify bottlenecks that may arise during the implementation of the change management plan	

18	In-Charge, ITD Section CGA	1	• Coordinate with ITD staff and INGAF to identify the capacity building requirements • External coordination including liaison with field offices, stakeholders, state governments, UTs, Audit, government department, other sections in CGA office • Coordinates with ACID (NIC) during the transition period.	Dy. CGA or equivalent
19	INGAF representative	To be decided by	• Devise plans and strategy to build in-house capacity to take-	To be decided by PSC and

S. No	Role Description	No. of Positions	Roles & Responsibilities	Responsibility Centre
		PSC and PMG	up the new IT initiative • Coordinate with Head, Project Planning & Coordination in IT training. • Design/customize courses to augment and sensitization /creation of awareness on IT initiatives and programs in field offices	PMG
20	Finance Accounts Subject Matter Expert	1	• Subject Matter Expert	Dy. CGA
21	Appropriation Accounts Subject Matter Expert	1	• Subject Matter Expert	Dy. CGA
22	Monthly Accounts Subject Matter Expert	1	• Subject Matter Expert	Dy. CGA

The Project Implementation Group shall comprise of representatives from the implementing agency in the areas of

- Training Planning & Management
- Application Development & Management
- IT Service Management
- Deployment & Monitoring



The Primary roles and responsibilities of the Implementation Group would be to ensure the following:

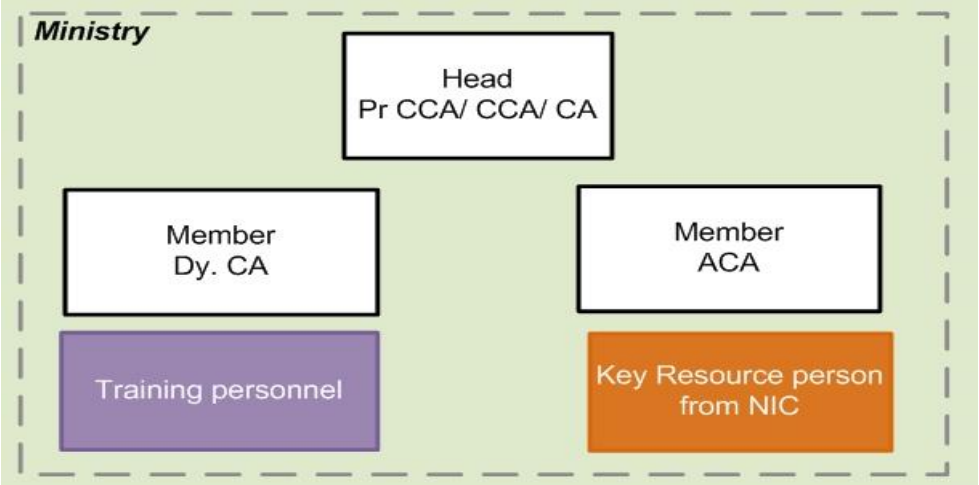
- The system performs functions and acts in conformance with the requirements and provides desired outcomes (deliverables/Service Levels).
- The application system and the databases are designed, developed, installed and managed exactly in conformance with the procedures laid down for delivery of services.
- The security of the overall system is of the appropriate order following recommended Standards.
- Any change required in the IGFMS application is with specific approval of competent authority.
- The processes, including legal enablement and capacity within the government are in place to take-over the entire system in case of an exit of the implementing agency (premature or planned).
- There is an ability to make necessary mid-course changes to the IGFMS application.
- Control over all intellectual property, source code and associated documents of the IGFMS application.
- There shall be non leakage of critical Information beyond the prescribed limits.
- There shall be a complete control over audit trails and a regular monitoring of service levels prescribed by the CGA.

9.2 Project Implementation Group at NIC

The implementation group within NIC would have the requisite technical resources including application specialists, network specialists, database specialists and support personnel. This team will be headed by team lead(s). An adequate number of such resources will be required at NIC considering the size and scale of operations and the contours of the proposed system which is spread across the country. This group shall provide the on ground help and support necessary for implementing the project seamlessly.

9.3 Project Implementation Group at Ministry

The implementation group within the Ministry would be headed by the Pr. CCA/ CCA or CA & Dy. CA, ACA shall be the members. The group shall frame the ministry specific training requirements and training personnel required for smooth implementation of the project.


Ministry
Head
Pr CCA/ CCA/ CA
Member
Dy. CA
Member
ACA
Training personnel
Key Resource person
from NIC

10 System Support and Maintenance Mechanism

The system support and maintenance mechanism of the IT systems becomes a crucial aspect when there is a requirement of an optimal level of service. Technical support may be delivered by different technologies depending on the scope of the proposed solution e.g. example, basic software problems can be addressed over the telephone or, by using remote access repair services; while more complicated problems with hardware may need to be dealt with in person.

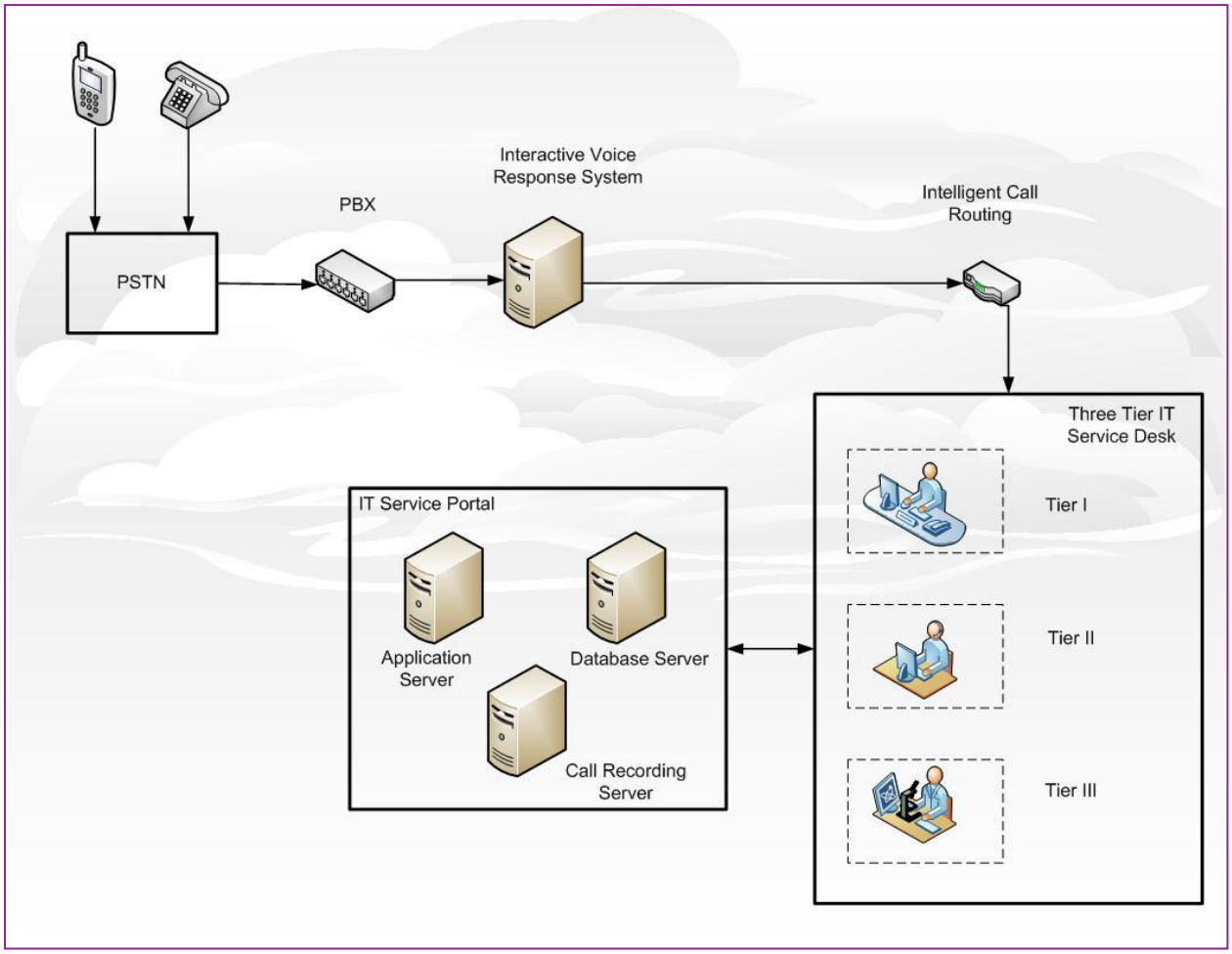
It has been observed that at the CGA's organization, there is a need to establish a dedicated centralized IT service desk that is available 24 x 7 to provide technical support to the users and respond to all the queries and incidents pertaining to the software systems being employed. The IT service desk should be designed to function on a transparent structure and facilitate an accountable incident management mechanism that is geared up to be at the user's disposal. The service desk should be an intelligent, state-of-the-art infrastructure and should be architected to scale enormously to meet all future needs of the organization.

Advantages of establishing an IT service desk:

- Enable responsive, stable and repeatable IT Service Delivery.
- Provide for improved incident and problem Management.
- Status tracking of logged incidents.
- Accountability of the logged incidents.
- Service Level Agreement (SLA) based service.
- Improved transparency in working of the IT division.
- One point of contact for the users for IT related services.
- Standardization of processes and better management of IT services.
- Creation of a central repository of information of the type of incidents being raised.

10.1 Mechanism of Working

The infrastructure and operations of the IT support mechanism can be handled in various ways and are discussed in subsequent pages. The diagram below, broadly, depicts the functioning of the proposed IT service desk.



1) The users, such as PAOs and DDOs, from various ministries call up the IT helpdesk for

   - Raising IT incidents
   - Getting password resets
   - Raising complaints about the lack of functionality of certain systems
   - Service request for hardware failure

2) The Interactive Voice Response System (IVRS) recognizes the user's requirement

3) Based on the option selected by the user, the system transfers the call to the required personnel.

4) The customer care executive, depending on the nature of the issue reported, logs the incident in a software application and provides the user a unique reference number.

5) The incident raised is then allotted to the technical team for resolution. The status of the ticket can be tracked using the unique reference number.

10.2 Business Model of the IT Support Desk

A very systematic approach should be taken for operating the IT service desk. Carrying out operational activities of the IT service desk would require strict tracking and monitoring to ensure that the agreed SLAs are maintained and optimum service is provided to the users. Some of the operation options for the service desk are:

- Complete in-house model
- Complete outsourcing model
- Hybrid model

10.2.1 Complete In-House Model

This is a complete ownership model where the O/o CGA would keep the ownership of each activity of the support desk. In this model the hardware infrastructure, network, manpower and complete management would remain with the O/o CGA. This will require the O/o CGA to make a major investment and would also require the O/o CGA to maintain a technical team in-house.

10.2.2 Complete Outsourcing Model

In this model of operation, the O/o CGA can outsource each and every activity of the IT service desk to an external agency. Setting up of the infrastructure, managing data synchronization, managing multilingual manpower etc, all would be the responsibility of one or more external agencies. This model would save the O/o CGA from creating a huge infrastructure asset. The external agency may charge on an annual basis or on any other transactional model. This model will bear least management concerns to the government and ensure good quality of service.

10.2.3 Hybrid Model

As the name suggests, this model can be a mix of the complete in-house model and the complete outsourcing model. The infrastructure setup can be owned by the government, and the operations may be transferred to an external agency. Another method can be to setup the service desk on a BOOT (build own operate transfer) model where an external agency would setup and run the service desk for few years and transfer it to the O/o CGA.

10.3 Establishing the Service Desk

Achieving an optimum level of service requires certain best practices to be followed. Adopting best practices can help the service provider to create an effective service management system. Best practices in this regard can come from many different sources, including public frameworks (such as ITIL, COBIT and CMMI), standards (such as ISO/IEC 20000 and ISO 9000), and proprietary knowledge of people and organizations. As a best practice, technical support should be subdivided into a three-tier structure in order to better serve a business or customer base. The reason for providing a multi-tiered support system instead of one general support group is to provide the best possible service in the most efficient possible manner. A brief description of the each tier of the support desk is given below:

Tier/Level 1(T1/L1): This is the initial support level responsible for basic customer issues. Tier / Level 1 (T1/L1) support shall be available 24*7. The task of the Tier I layer would be to gather the customer's information and to determine the customer's issue. Once identification of the underlying problem is established, the specialist can begin sorting through the possible solutions available. Technical support specialists in this group would handle straightforward and simple problems such as, resolving username and password problems, uninstalling/reinstalling basic software applications, verification of proper hardware and software set up, and assistance with navigating around application menus. The goal for this group is to handle 70%-80% of the user problems before finding it necessary to escalate the issue to a higher level.

Tier/Level 2(T2/L2): This would be a more in-depth technical support level than Tier I. Tier / Level 2 (T2/L2) shall resolve incidents as per the SLA in case the incident remains unresolved at Tier / Level 1 (T1/L1). Specialists in this tier would be responsible for assisting Tier I personnel in solving basic technical problems and for investigating complex issues by confirming the validity of the problem and seeking for known solutions related to these more complex issues. Prior to the troubleshooting process, the Tier II specialist would review the work of the Tier I specialist to see what has already been accomplished by the Tier I technician and how long the technician has been working with the particular customer or user. This is a key element in meeting both the customer and business needs as it allows the technician to prioritize the troubleshooting process and properly manage his or her time to maintain the required Service Level Agreement (SLA).

Tier/Level 3(T3/L3): This would be the highest level of support in the three-tiered technical support model, responsible for handling the most difficult or advanced problems. The individuals in this tier would be responsible for not only assisting both Tier I and Tier II personnel, but also for the research and development of solutions to new or unknown issues. The Tier III specialists would have the same responsibility as Tier II technicians in reviewing the work and assessing the time already spent with the customer so that the work is prioritized and time management is sufficiently utilized. This group would responsible for designing and developing one or more courses of action, evaluating each of these courses in a test case environment, and implementing the best solution to the problem. Once the solution is verified, it would be delivered to the customer and made available for future troubleshooting and analysis.

11 Change Management

11.1 Need for Change Management

Introducing radical reforms has to be necessarily accompanied by efforts to change the mindsets of people – both within and outside the department. For instance, the service seekers need to know how to avail services with the new system implemented; the staff should be skilled to operate and work in a significantly newer way. A well-calculated and well-designed strategy has to be followed for staff to be trained work effectively in the new environment. It is necessary to formulate a change management plan with appropriate interventions for capacity building, training and stakeholder communications.

A successful Change Management Programme will ensure:

- A smooth transition to the new way of working
- The organization/people support the changes implemented
- Individuals know how the changes affect them and the role they have to play
- The new system and its underlying concepts are understood
- People are aware of how roles and responsibilities are changing
- Everyone is motivated and committed to the change programme
- The success and progress of the programme is monitored and measured

11.1.1 Key Change Management Implications

The implementation of a new IT ecosystem in the Office of CGA will have several change implications emanating from the following changes:

- Process and procedural (necessary introduction of some new process and systems emanating from the need of changing core functional information flow in a few cases)
- Technical and technological (introduction of new technologies for enabling the new / unaddressed business requirements)
- Organizational (transformation of existing organizational structure and redefined roles and responsibilities)

The following change implications can be clearly identified at the outset of the implementation of the new system:

Change Element	Change Implication	Change Issues
Process and procedural	• Standardization of procedures • Redefined processes and new work methods • Elimination of certain activities / functions and addition of new ones • Redefined service levels • Customer centric approach • Standardized MIS reporting systems to monitor the progress	• Reorientation of staff to new processes and work methods • Reorientation of staff to any applicable service levels • Augmentation of customer focus • Loss of control over discretion on procedures by staff • Enhanced process driven systems with clear accountabilities and responsibilities • Preparation for dealing with public grievances in the defined service levels
Technological	• High usage of technology and system enabled processes • Automated controls and validation • Creation of centralized online grievance redressal mechanism • Reduction of paper work	• Work systems changed from slightly automated to highly automated work methods • Preparation for use of technology and system enabled processes • Orientation towards a paperless processing system
Organizational / People	• Some change in roles and responsibilities • New skill set requirement for staff • Introduction of a incentives and reward system	• Reluctance to work in tandem with external agencies involved in implementation • New work environment and changed peer relationships

For an effective change management plan, it is necessary to categorize change issues according to impact they might have on successful implementation of the new system and the urgency at which they need to be addressed.

Impact of issues on successful implementation is measured by the following parameters:

- Issues which are most critical for new system implementation to succeed

- Issues which are necessary ensuring present level of service will be maintained during the change phase

- Issues which if not resolved, will still be least disruptive to the new system implementation

These issues in order of their importance have been listed below in the table:

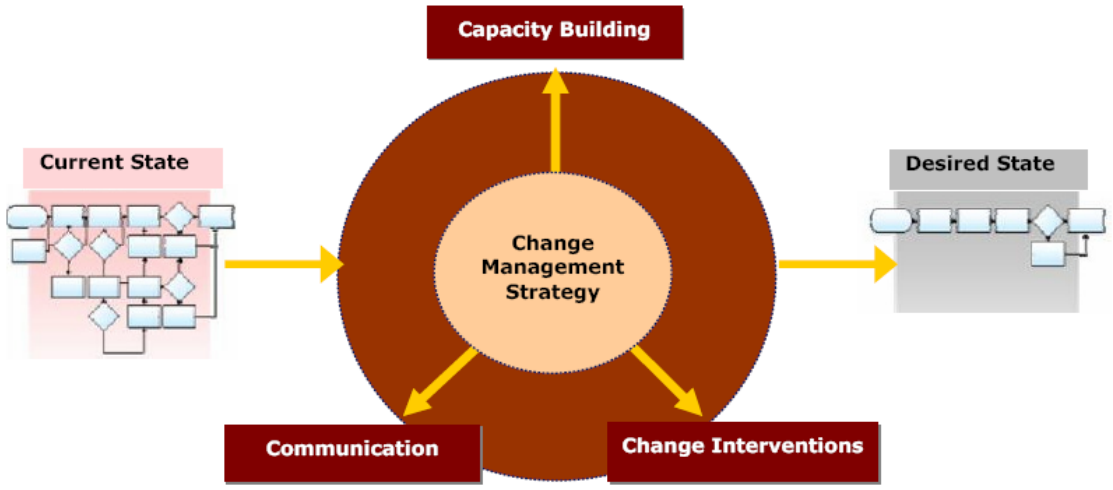
Change Issue	Impact on Implementation	Issue Resolution Time Frame
Reorientation of staff to new work methods	High	Immediate
Augmentation of customer focus	High	Immediate
Preparation for use of technology and system enabled processes	High	Immediate
Orientation towards a paperless processing System	High	Immediate
Loss of control over discretion on procedures by staff	High	Immediate
Reorientation of staff to concept of service levels	High	Medium Term
Preparation for dealing with public grievances in the defined service levels using technology	Medium	Medium Term
Process driven systems with clear accountabilities and responsibilities due to standardized MIS and reporting	Medium	Long Term
New work environment and changed peer relationships	Medium	Medium Term

11.2 Change Management Plan

Going forward, it will be critical to assess those issues that will have the highest impact on the change management plan and manage them through appropriate interventions. Some of the interventions proposed are listed below:

- Help to make staff realize the benefits of the new system
- Highlight the improved public perception and image of staff within the new system
- Identification and preparation of change agents (Change champions) to deal with change at local level
- Rationalized and planned work schedule and workload
- Highlight the learning and growth opportunities in the new system
- Highlight the easy of working in the new system with better technology and simpler processes

To enable the key intervention strategies a three pronged approach to change management is proposed for Office of CGA. This will ensure successful transition onto the desired state. The key elements of the approach are illustrated in figure below:



Communication: Primary tool for managing perceptions and developing commitment to change among key stakeholders

Training: Useful for developing required skills and providing clarity on new process

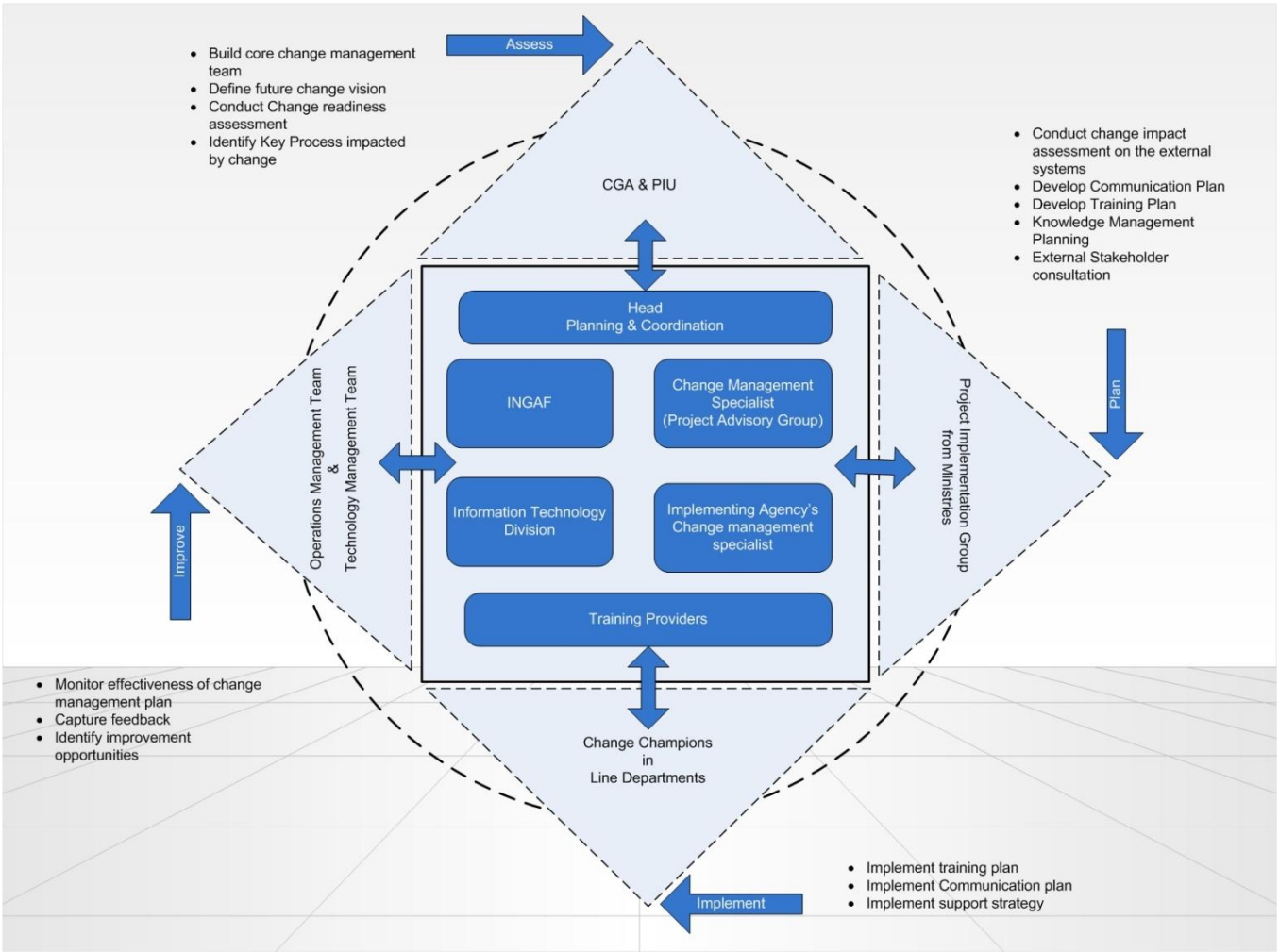
Change interventions: Formation of "Change Management Teams" – used for implementing change initiatives and addressing unique challenges arising out of change

Training and Change interventions have specific and time bound objectives while Communication is an ongoing and adaptive process which seeks to manage all stakeholders and their perceptions about the change over a period of time.

11.2.1 Necessary infrastructure required for Change

Institutional Framework

To start with, it is important to have a suitable institutional framework in place to drive training, implementation and handling change management aspect of the project. The proposed institutional framework for managing change is depicted in the schematic below.



1. Local Change Management Teams (Change Champions)

The local change management teams would consist of officials who demonstrate aptitude for early adoption of changes and act as change agents for the rest of the staff members. It is recommended that the local change management teams should consist of local officials and experts in the following areas:

- Technology
- Process & Procedure
- Communication & Training

One of the key requirements of implementing a change management plan at the Office of CGA offices is to identify "Early Adopters" of the system at the various offices. These Early Adopters can form part of the "Change Management Team" along with the senior members in the department and act as change agents to spearhead the change process.

Effective change agents at the department offices (Members of the Change Management Teams) must possess skills to complete the following tasks:

– Explain the system change (along with any associated processing change) and its implications to staff
– Focus on the smaller issues of change at the various offices
– Solicit and monitor the workforce support for change
– Provide honest information regarding the change process

Since the change management team can heavily influence the outcome of the change management initiative, formation of the team is very critical to the overall success of the interventions.

2. Responsibilities of Change Management Teams

The key responsibilities of Change Management Teams at various offices would be as follows:

- Assessing and building staff capability to implement change quickly and effectively
- Preparing key officers and their direct reports to meet the challenges and opportunities they will encounter as they implement new processes
- Implement and monitor training plans
- Helping to increase individual skills, knowledge, and abilities

- Developing and implementing change communication plans
- Facilitation to concerned staff for transition to new roles
- Work towards minimizing employee resistance to re-engineered processes and new organizational setup

3. Managing Job Allocations / Redeployment in New System

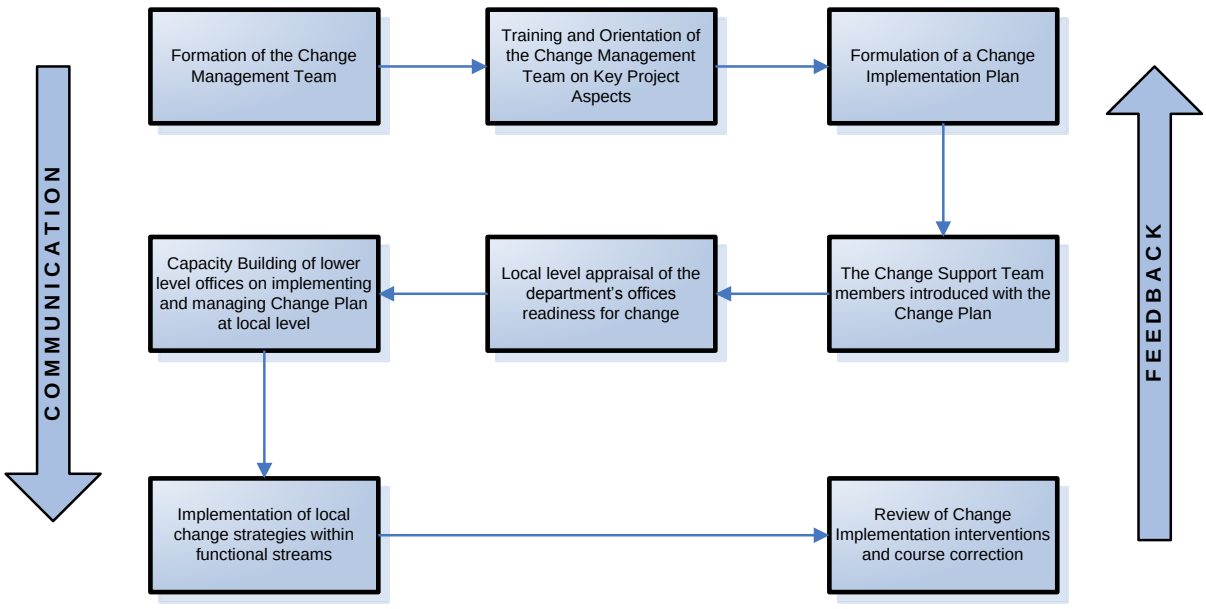
Redeployment requires a number of essential components that must be carefully coordinated with meticulous attention to details. Leadership may aid redeployment purposes by implementing the following steps:

- Build an employee skills data base
- Utilize the database for internal redeployments
- Establish staff members who are best suited for various processes / activities within the reengineered system
- Provide process specific trainings and also create cross-training opportunities for staff as positions disappear/emerge in the new system

11.2.2 Key steps for change implementation

The various phases of change implementation are highlighted in the figure below:

Figure: Steps to Implement Change



Interventions at various levels are needed to mitigate staff's resistance to change and facilitate an environment which encourages staff to pro-actively volunteer within the new system.

Some of the strategies to ensure quick-wins would be:

- Organizing workshops with users on
  - The proposed changes highlighting the positives in the system and creating a buy-in from them
  - Provide them with answers to key questions which users will encounter from their customers - "Helping them deal with their stakeholders"
  - Communication to them the key requirements of the proposed system- "What we want from them"
- Creating forums for dialogue and exchange of ideas
- Exposure to other such computerization initiatives in similar set-ups worldwide
- Encourage Two-Way communication and feedback loops

11.3 Capacity Building

11.3.1 Approach to capacity building

It is important to build capacities of the Office of CGA staff in terms of necessary knowledge and skills to initiate, successfully implement the new system. It is equally important to generate an attitude that is receptive to largely technology based operation of all functions. Merely developing and implementing a new system will not help deliver the quality results envisaged unless staff members are aligned to provide the right results with the right tools at the right time.

The nature and scale of implementation planned for the Office of CGA processes demand a considerable enhancement in the capabilities of the organization to effectively address the objectives. For achieving this, the Change Management Team needs to provide overall direction, standardization and consistency across the implementation.

Hence in this backdrop, Office of CGA staff leading the implementation initiative and its constituent projects needs to be adequately trained to meet the managerial and technological challenges for driving the project. However, a number a people at remote offices might not be adequately equipped to take up the challenge. Some of the real problems faced at the various levels are:

- Little knowledge of essentials of IT
- Minimum technology exposure
- Lack of in-depth understanding of the benefits
- "What's in it for me?" factor

To address the training needs, the change management team should prepare guidelines that identify the training needs of all stakeholders and provide suggestive training curriculum to address the training needs. Such guidelines will assist local change teams to formulate its own training plans and aid the progress of the implementation of new system at efficiently at local levels.

11.3.2 Critical capacity building needs and training

The key training needs for successful implementation of the new system were established through a two pronged approach; stakeholder questionnaire administration assessment stage, and identification of key success factors for the new system at the solution conceptualization stage.

The key training areas are summarized below:

- Program and Project Management
- Change Management
- Process and Procedures
- Basic Computer & IT
- SLA Monitoring
- Customer Service and Delivery
- Stress and Time Management
- Budgetary Control
- Additional / New Functionality

Based on the suggested institutional framework, there are 3 levels at which capacity building is required:

- Top Level - Change Management Team / Core Group / Senior Officials
- Middle Level –Change Support Teams / Identified Change Champions
- Lower Level - Individual Staff Level

The following table illustrates the potential areas of training required for the above mentioned levels:

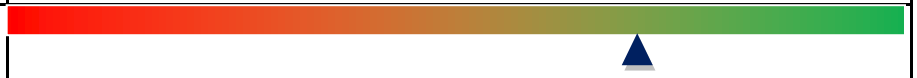
S. No.	Training Level Envisaged	Envisaged Role under Change Plan	Potential Areas for Capacity Building
1.	Top Level	Training required for taking up the role of leading implementation of new system. This role would involve managing the implementation initiative overall and would be responsible for: • Program management • Permanent Advisory role for new IT System implementation • Setting up of guidelines and procedures for any new functionality required • Potential benefits expected post computerization • Costs • Critical issues – including BPR, financial sustainability etc.	Develop skill-sets to handle the issues of overall policies, strategies, technologies, common infrastructure etc. in an effective manner. Illustrative areas for the training are: • To impart working knowledge and skills related to: ♦ Implementing and managing the new system ♦ Managing external agencies (IT vendors / service providers) ♦ Program Management • Program Insights into: ♦ Project evaluation and award ♦ Key technological requirements for the redesigned systems and awareness on IT security ♦ Standards for systems, applications and processes required for program management ♦ Need analysis, solution recommendation, vendor selection, implementation, training, and post-installation support ♦ Budgeting
2.	Middle Level	Training to provide inputs to the identified champions at	• Project Management Training

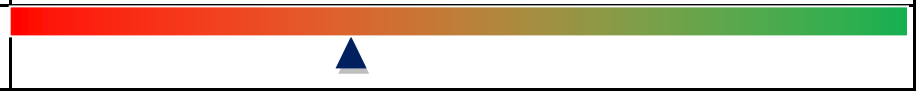
S. No.	Training Level Envisaged	Envisaged Role under Change Plan	Potential Areas for Capacity Building
		local department offices to initiate and manage the project implementation. Since this would be the "hands-on team" managing the change, training should aim to provide skills to manage the project.	♦ Basic Project Planning ♦ Project plan integrating timelines, roles and responsibilities ♦ Monitor/track and report status regularly ♦ Develop communication plans ♦ Monitor SLAs with vendor(s) ♦ Establish project control mechanisms like responsibility matrix, escalation matrix, etc. ♦ Budgeting at local level • Change Management Training ♦ Objectives of change management in the new system ♦ Change Management planning & implementation ♦ Capacity building and Change Management ♦ Working with change teams and change agents ♦ Interpersonal communication ♦ Hands-on practical tips for Change Managers through toolkit and FAQs ♦ Dos & Don'ts ♦ Conflict management at local office / remote level ♦ Implementation of change management strategies including incentive schemes

S. No.	Training Level Envisaged	Envisaged Role under Change Plan	Potential Areas for Capacity Building
			♦ Ensuring Feedback
3.	Lower Level	Training to enhance capabilities of staff members at the Office of CGA offices to successfully integrate with any legacy / retained systems and progress towards achieving the desired functionality / efficiency / service levels within the shortest time possible	• User Level basic computer training • System specific training • Reorientation of staff to new work methods • Reorientation of staff to new service levels • Training on functional procedures and standard rules & norms • Customer Service Training • Communication training • Time and stress management training

Further to this it is imperative to recapitulate the areas where the relevant IT training would help the users at various levels maximize the benefits of the proposed new IT systems. During the assessment phase it was found that the basic knowledge of IT systems is sufficient for daily usage of these applications and systems however aspects pertaining to IT security, data security and backup form the key concern areas with regards to IT skill augmentation of the users.

The recommended level of skills to operate new IT systems at various user levels is given below:

Readiness to use computer for general typing work	Office of Pr.AO	
	PAO	
	DDO	
Readiness for Actual use of application	Office of Pr.AO	
	PAO	
	DDO	
Familiarity with Office Suite(MS Office)	Office of Pr.AO	
	PAO	
	DDO	
Readiness to use internet & email facility	Office of Pr.AO	
	PAO	
	DDO	
Internet Banking concept / e-Commerce & e-Payments systems concept / awareness	Office of Pr.AO	
	PAO	

	DDO	
Awareness of Digital signature & encryption concepts, Computer security & hacking concepts	Office of Pr.AO	
	PAO	
	DDO	
Awareness of Computer Virus concepts and protection	Office of Pr.AO	
	PAO	
	DDO	
Awareness of Data access policy	Office of Pr.AO	
	PAO	
	DDO	
Awareness of Backup & Disaster recovery concept	Office of Pr.AO	
	PAO	
	DDO	
Readiness for Day-to- day trouble shooting	Office of Pr.AO	

	PAO	
	DDO	

Legend: **Low**  **High**

Within the above constraints and training requirements, the structuring of training has been left at the discretion of the implementation agency in collaboration with Office of CGA.

11.4 Communication Plan

11.4.1 Communication and Change Management

Office of CGA staff may resist change for a number of reasons, including fear of losing their discretion, fear of the unknown, reluctance to make the effort involved, upsetting a well established routine, fear of failure, lack of confidence in the change implementers, lack of proper communication but possibly, the most important reason is the fear of being worse of afterwards.

Office of CGA staff (rather than IT) is the central focus of the change management and communication plan. For successful project implementation, Change Management interventions should particularly aim at supporting those who will be most affected by the change of systems and any associated processes / functionality.

The objectives of the communication and change management plan are to:

- Use communication mechanisms for providing the Office of CGA staff with critical information, feedback mechanisms and support during the change of system
- Assist with the operationalization of the project objectives as stated within the project charter
- Ensure least resistance from staff with respect to proposed changes in the systems

Some of the key messages of the communication and change plan are:

- Uniform and simple functionality / system for staff leading to rationalization of workload and accountability
- Skill enhancement through training of the staff (functionality and technology)
- Recognition to efficient staff through a recognition program
- Low level activities being automated, hence higher growth opportunity for the staff
- Better office environment and comfortable work area due to proposed changes

11.4.2 Preparing Officers to be Change Agents

Office of CGA office staff may resist significant changes. Officers should acknowledge these feelings and address them through face-to-face meetings, rather than withholding

information or not acknowledging employee reactions, fears, and doubts. Officers may effectively deal with the negative effects of change if they understand how change affects their staff.

The following list in table below provides reasons staff may resist change and strategies that officers can use to reduce that resistance:

Reasons Employees Resist	Strategies for Officers
• Employees feel they will suffer from the change • Organization does not communicate expectations clearly • Employees perceive more work with fewer opportunities • Change requires altering a long-standing habits • Organization lacks adequate reward processes • Organization lacks sufficient resources • Organization has poor internal communication • Change has poor introduction	• Use communication strategy that asks for employee input • Do not send mixed signals regarding the change; this will increase employee distrust • Communicate clear vision of the change • Provide timely information on change • Identify employee concerns and unresolved implementation issues • Provide staff with a timeline and a defined approach and outcome • Communicate how staff will benefit from the change • Develop procedures to address staff who will be negatively affected by the change • Allow staff to express their grief; criticizing change creates defensiveness in those who like the traditional ways

Tips for Office of CGA Officers to preserve employee morale during change implementation:

- Spend a day walking around subordinates to find out what their new working environment is like
- Hold routinely scheduled officer meetings to discuss implementation progress of new systems
- Publicly reward desired behaviour by staff during implementation phase
- Be open to feedback
- Keep staff in the information loop as much as possible.

11.4.3 Specific Communication Interventions

The following table illustrates the potential communication interventions at various levels:

Audience	Key Change Issues	Message Theme / Purpose	Medium / Vehicle
Stakeholders	• Information on new systems • Confidence building on ease and reliability of new system	• Communication on new channels & modes of interaction with the CGA Office • Communication on new service levels • Communication on use of online system / applications • Communication on grievance redressal mechanism	• Electronic Media/ internal circulations • Office of CGA Website • Information Boards at various CGA offices
Change Management Team / Core Group / Senior Officials	• Ability to implement new systems • Managing resistance from staff • Ensuring undisrupted services to customers	• Communication on new functionality, procedures and standard rules & norms • Changes in the system, its implications and way forward • Strategies for implementation and best practices for managing workforce in times of transformation	• Handbooks / Change Guides • Workshops • Seminars • Communication Toolkits for Change Agents
Individual Staff	• Resistance of staff to new processes and work methods • Reluctant to accept external agencies • Loss of control over discretion on procedures by	• Changes in the work methods • Reorientation of staff to new service levels • Benefits to the staff with introduction of new systems • Benefits to the customers • Workload balance and ease	• One – to – One Meetings • Workshops • Video Films demonstrating the new system and benefits • Posters • Checklist of new work

Audience	Key Change Issues	Message Theme / Purpose	Medium / Vehicle
	staff • Reluctance to learn new technology	of working • Communication on the proposed organizational structure • Working with private players • Addressing fears on outsourcing of activities • Ongoing communication support on technology	requirements • FAQs • Bulletin Boards • Handbook of New Procedures

11.4.4 Implementing Communication Plan

Communication interventions described above are to be implemented at 3 levels across various stakeholder groups. These interventions would be led by the Change Management Team and the Core Group, followed by the change champions / change agents. Listed below are some of the key roles and responsibilities of these teams / individuals at various levels.

- Central level – All central level communication will be handled by the designated officials under the guidance of the Change Management Team. The key responsibility at this level would be to generate awareness about the new channels & modes of stakeholder interaction, service delivery and service levels, and communication on use of new system.

  Also it will be responsibility of this team to ensure the heads of various offices are well equipped to implement and adopt new systems, managing resistance from staff and ensuring undisrupted services to customers. This team will provision for the required toolkits, FAQs, communication toolkits for Change Agents and organize workshops with officers to sensitize them on change objectives and implementation strategies.

- Remote Office Level –Change Agents and Champions under the guidance of Change Management Teams and Core Group would be responsible for all stakeholder communication at the remote level. This would also include locally available communication channels and communication mediums in local languages. It will ensure

that all stakeholders have buy-ins for the proposed changes and ensure effective adoption of the new system.

- Individual Level – This will be driven by the individual staff of Office of CGA through various means of communication among their peers. The key medium for this would be interpersonal communication - creating forums for dialogue and exchange of ideas, exposure to other such initiatives and encouraging two-way communication and feedback loops. Communication aids like checklists, bulletin boards, employee handbook etc can re-enforce the benefits of new system to the staff.

In order to maintain morale and enthusiasm during transformation, Office of CGA should clearly communicate the overall goals of the change so staff can see where the organization is going and can give them a sense of purpose.

Officers will need to communicate a number of vital questions during change management. Following are tactics they need to employ during the change phase:

Tactic One: Communicate Timely

- It is recommended that each office has its own well laid communication plan which details pre-implementation communications messages and methods in advance and alerts staff as soon as possible so that staff will hear this information personally from their officers, not from the grapevine.

Tactic Two: Communicate Clearly

- Employees during change often have many unanswered questions, in addition to anxiety regarding their future and increased stress. Recommended strategies for addressing employee concerns include communicating clearly and honestly with staff throughout the change process, demonstrating continuous appreciation for each individual.

Tactic Three: Communicate Need for Change

- Employees must understand why Office of CGA needs to change and they must buy into the change management efforts. Communicate the "people"

implications of upcoming process change, including what the changes will mean for staff' positions within the office.

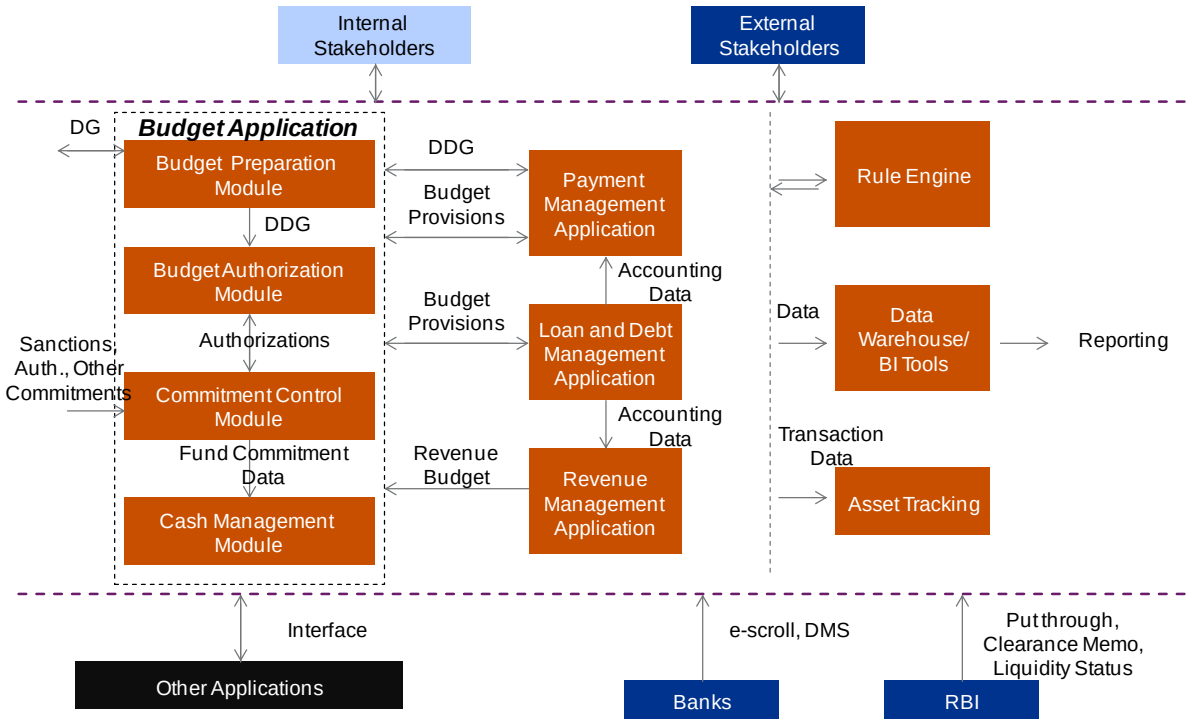
Tactic Four: Communicate Personally

- Employees must be told how the change will affect them personally. Individual concerns should be addressed. Senior and middle management must be trained to ensure they have the skills to provide essential information to staff in an effective and timely manner.

12 Project Implementation Roadmap

The proposed IGFMIS broadly consists of four core applications - budget application, payment management application, revenue management application, loan and debt management application and few other applications such as rule engine, business intelligence and asset tracking tools. Functionalities of these applications/modules is explained at section 4.6.

The schematic below represents high level view of the proposed IGFIMS for the CGA's organization, it also shows various applications/modules and linkages/data flows.



In order to define the implementation roadmap it is important to first list options for devlopment of these applications/modules and also the precedence/order in which these can be devloped.

These applications can be developed as bespoke applications with some CoTS products to cover specific functionalities such as payroll processing, document management system, internal audit, business intelligence. Another approch can be deployment of complete CoTS solution with required customizations.

Inorder to evaluate options for each acpplication/module of the proposed IGFMIS interms of precedence of development and also evaluate option for development as bespoke or deployment of CoTS, each application/module is assessed against the following parameters:

Criticality : The importance of the application /module amongst the set of appliactions, how postponing the development of this application will affect overall solution. High criticality means that it is an important application/module in the overall system and development of the applications is dependent on it. Medium criticality means that the application/module can be implemented post development of the core applications/modules. Low criticality means that the development of the application will add value to the overall system, but is not an immidiate requirement.

Dependency : This parameter shows the dependency of the application/module on development/interface with other application/module or dependency on availability of data from other application/module.

User base: This includes the number of users who will access the particular application

CoTS available/Bespoke development required: It will include description of available CoTS of the particular functionality, and whether development of bespoke application will be required or suitable.

Tentative precedence for development or customization: It will describe tentative precedence of the develpment/customization of the application.

The evalution of applications/modules of the proposed system for IGFMIS has be done in the following section.

12.1 Application Development and Prioritization

a) Budget Application

S. No.	Criteria	Description
1	Criticality	**Budget Preparation** – High (Payment and Receipt Management applications are dependent on it) **Budget Authorization** – High (Payment and Receipt Management applications are dependent on it) **Commitment Control** – Medium (can be implemented once the core modules are implemented) **Cash Management** – Medium (can be implemented once the core modules are implemented)

S. No.	Criteria	Description
2	Dependency	Availability of data from PAOs and budget division Ministry of Finance (MoF)
3	User base	Approximately 3000 to 4000 users. It includes users from Budget Section of Ministries, IFDs, Program Divisions, HoDs
4	CoTS available/Bespoke development required	**Budget Preparation – Oracle:** Hyperion, **SAP:** Business Planning, **FreeBalance:** Performance Budgeting **Budget Authorization - Oracle:** Hyperion, **SAP:** Business Planning, **FreeBalance:** Performance Budgeting **Commitment Control – Oracle:** General Ledger (GL), **SAP:** Revenue and Expenditure Management **,** **FreeBalance :** Public Financial Management **Cash Management - Oracle:** General Ledger (GL), **SAP:** Revenue and Expenditure Management, **FreeBalance:** Government Treasury Management
5	Tentative precedence for development or customization	Budget preparation and Budget Authorization modules to be implemented at the beginning of the development/deployment along with the development/ deployment of core system, Commitment Control and Cash Management modules can be implemented post development/ deployment of core system. But if CoTS based solution is deployed then these modules/functionalities will be part of a larger suite and around 30-40% customization will be required.

b) Payment Management Application

S. No.	Criteria	Description
1	Criticality	High (It is the core application for payment management and accounting)
2	Dependency	Data from Budget preparation application
3	User base	Approximately 35000, it includes users at office of DDO, PAO, Pr.AO and CGA
4	CoTS available/Bespoke development required	**Oracle:** Payables, **SAP:** Revenue and Expenditure Management, **FreeBalance:** Public Expenditures Management

S. No.	Criteria	Description
5	Tentative precedence for development or customization	To be implemented at the beginning of the development/deployment along with the development/ deployment of core system

c) Revenue Management Application

S. No.	Criteria	Description
1	Criticality	High (It is the core application for payment management and accounting)
2	Dependency	No major dependency
3	User base	Approximately 7000 users it includes users at office of DDO, PAO, Pr.AO and CGA
4	CoTS available/Bespoke development required	**Oracle:** General Ledger, **SAP:** Revenue and Expenditure Management, **FreeBalance:** Government Receipts Management
5	Tentative precedence for development or customization	To be implemented at the beginning of the development/deployment along with the development/ deployment of core system

d) Loan and Debt Management Application

S. No.	Criteria	Description
1	Criticality	Medium (can be implemented once the core modules are implemented)
2	Dependency	Availability of accurate legacy data
3	User base/transaction volume	Approximately 300 users which includes users at office PAO (state loan and market loan), Pr.AO and CGA
4	CoTS available/Bespoke development required	**SAP:** Treasury Management, **FreeBalance:** Debt and Investment Management ,Grants and Social Programs
5	Tentative precedence for development or customization	The application can be implemented post development of the core applications/modules

e) Data warehouse, BI-tools, Asset Tracking, Internal Audit application/tools

S. No.	Criteria	Description
1	Criticality	**Data warehouse/BI tools:** High (All core applications will be linked to the data warehouse) **Asset Tracking:** Medium (can be implemented once the core modules are implemented) **Internal Audit:** Medium (can be implemented once the core modules are implemented)
2	Dependency	**Data warehouse/BI tools:** Availability of accurate data from other applications **Asset Tracking:** Mandate required for using asset tracking applications by ministries and departments **Internal Audit:** Implementation of checks and controls at all systems
3	User base	**Data warehouse/BI tools:** Approximately 250-200 users, it includes users at office of Pr.AO, CGA and HoDs of departments/ministries **Asset Tracking:** It is difficult to make an estimation of number of users as it will be used by multiple people of different ministries/departments **Internal Audit:** Approximately 200 users, , it includes users at office of Pr.AO and CGA
4	CoTS available/Bespoke development required	**Data warehouse/BI tools: Oracle:** Functionality inbuilt in Oracle Financials, **SAP:** Business Object, **FreeBalance :** Government Transparency **Asset Tracking: Oracle:** Oracle Fixed Asset **SAP:** Asset Management , **FreeBalance :** Assets and Inventory **Internal Audit: Oracle:** In-built **SAP:** In-built **Others:** Teammate **, FreeBalance :** Government Transparency
5	Tentative precedence for development or customization	**Data warehouse/BI tools:** To be implemented at the beginning of the development/deployment along with the development/ deployment of core system **Asset Tracking:** The application can be implemented/deployed post development of the core applications/modules

S. No.	Criteria	Description
		Internal Audit: The application can be implemented/deployed post development of the core applications/modules. Internal audit functionality can be achieved by using datawhare house and BI tools.

12.2 Project Implementation Roadmap

Based on prioritization and options for application development a high level implementation roadmap is prepared.

The project implementation roadmap/plan highlights broad timelines for project initiation, implementation and monitoring; also activities in each of these phases are mentioned.

The project will begin with project initiation phase, which will be after approval of the proposed solution and finalization of system development approach out of the options as defined at section 12.3. System development will be carried out based on one of the option finalized by the project steering committee.

The project initiation activities include setup of project governance structure as described in section 9 of the report, plan for project implementation lifecycle, preparation of functional and non functional requirements, service level agreement, assessment of IT and non IT infrastructure, defining project risk mitigation plan and escalation mechanism etc. These activities will be carried out by the members of project advisory group as defined in the project governance structure.

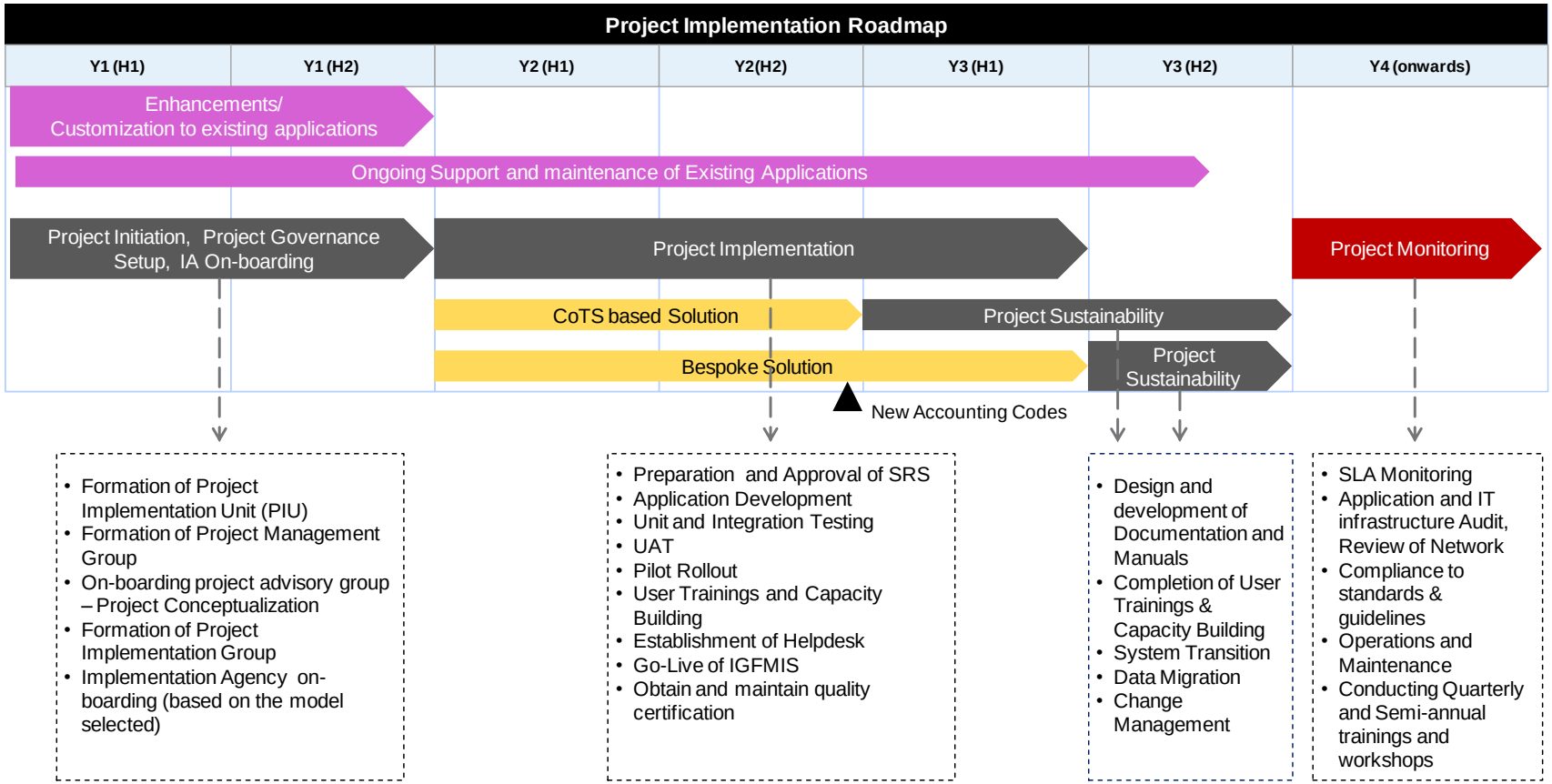
Project implementation phase will include application development. As the application development option will be finalized at a later stage, the implementation roadmap shows timelines for deployment and customization of overall CoTS based solution and development of bespoke solution. In both the cases the application development / deployment will follow complete Software Development Life Cycle (SDLC) which includes requirement gathering, designing the solution, coding and testing. Project implementation phase is followed by project sustainability phase which includes transition time to the new system by the end users, design and development of user manuals, completion of trainings and capacity building, data digitization etc. The final phase of the project will require project monitoring which includes SLA monitoring, application and IT infrastructure audit, review of network, compliance to standards etc.

The implementation roadmap also shows that in the immediate short term some changes/customizations will be required in the existing IT systems; this will be carries out within the period of 6 months, stretching up to a maximum of 1 year. These changes are detailed out in the table below:

S. No.	Enhancement/Changes
1	Enhancements in e-lekha by providing feature of generation of customizable/intelligent reports.
2	Use e-DDG to populate budget data in COMPACT, it can be mapped with respective PAO, DDO codes, which will facilitate spending unit wise budget allocation
3	Develop commitment module for e-Lekha and start using it for cash projections that shall be populated by Pr.AOs for their immediate, short-term and long-term cash needs.
4	Develop an automated link using Service Oriented Architecture (SOA) between COMPACT and e-Lekha to automate the generation and uploading of text file automatically into e-Lekha in batches. The batch can be programmed to pull data at pre-defined intervals (hourly / every 3 hours / end of the day).
5	Develop the data exchange mechanisms like put-through of RBI to PAO for mandatory remittances and reconciliation
6	Development/deployment of an stock/inventory tracking application for the office of CGA
7	Ongoing support and maintenance of existing applications

Also, the implementation roadmap shows that ongoing support and maintenance will continue for the existing system till the time the new system is fully developed and deployed. The implementation roadmap shows tentative implementation of new accounting codes being devised by the office of CGA. The new accounting codes are expected to come from financial year 2014-15. It is expected that the new accounting codes will be implemented, during the project implementation phase, and at that time the anticipated changes will be incorporated in the new system.

The diagram below describes the project implementation plan.



The table below details out phases of the project implementation roadmap:

CGA IT Strategy - Project Implementation Plan																																
S. No.	**Activity**	**Timelines (Months)**																														
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
	Trigger- Approval for implementation of IGFMS in O/o CGA																															
	1- Organization Setup & Project Initiation Activities																															
1	Constitution of Organization set up which includes **Project Implementation Unit (PIU), Project Management Group** and **Project Advisory Group** as suggested in the IT Governance Structure																															
2	Define requirements and plan project implementation lifecycle																															
3	Define resources and schedule for project/program implementation																															
4	Defining of Functional and Non Functional Requirement Specification for the proposed system																															
5	Development of detailed Service Level Agreement																															
6	Detailed Assessment of IT and non IT-infrastructure required at data centre and field offices.																															
7	Define detailed training and capacity building plan (Number of people to be trained, number of trainings to be conducted, batch size, type of trainings etc.)																															
8	Define project risk mitigation plan and escalation mechanism																															
9	Assessment of data digitization requirement																															
6	Formation of **Project Implementation Group**																															
7	On-boarding of Implementation Agency (IA) (approach for system development and vendor on-boarding defined at section 12.3)												M1																			

Project Milestone:
M1- Implementation Agency on-boarding

S. No.	Activity	Timelines (Months)																												
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
	2-Project Planning & Execution																														
8	Existing application augmentation as per the short-term goals set out in the IT Strategy Document																														
9	Formulation detailed project implementation plan																														
10	Preparation of SRS document by Implementation Agency																														
11	Approval of the SRS document by NIC / CGA															M2															
12	Customization of the IGFMS solution																								M3						
13	Development of the IGFMS solution																													M3	
14	Hardware installation and configuration at existing data centre facility																														
15	Integration with various department applications / banks / RBI etc																														
16	Testing of various modules and the integrated systems																														
17	UAT at existing data centre facility																														
18	Establishment of Helpdesk																														
19	Go-Live of IGFMIS Application																														M4
20	Obtain and maintain quality certification																														
21	Development of Change Management Framework and Training Content																														
22	Site selection for dedicated DC & DR																														
23	Necessary approvals, signing of agreement for DC & DR site																														
24	DC & DR Site preparation																														
25	DC & DR migration																														

Project Milestones:
M2- Preparation of SRS
M3- Application Development/Customization
M4- IGFMIS application Go-Live

S. No.	Activity	Timelines (Months)											
		25	26	27	28	29	30	31	32	33	34	35	36
	Trigger- Approval on IGFMIS Application, CM plan, Training manuals, Training Infra/lab												
	3 (a) -Project Sustainability & Migration												
25	Migration of Master Data (Employee Master, Vendor Master, Mapping of PAO and DDO codes etc.) from existing applications to IGFMIS												
26	Data migration from COMPACT, COMPACT (REVACT & RAMS) and COMPDDO to Budget Preparation, Payment Management, Revenue Management, and Budget Authorization Applications/Modules												
27	Availability of employees data for Payroll Processing												
28	Data related to Loan and Debt to be migrated to IGFMIS Loan and Debt Management, Commitment Control & Cash Management												
29	Migration of legacy data from e-Lekha for Data warehouse and BI												M5
	3 (b)- User Trainings												
30	Finalization of Training Plan												
31	Finalization of Batches for Training												
32	User Trainings												
33	Training feedback and Assessment of Change Management program												M6

Project Milestones:
M5- Completion of Migration
M6- Completion of Trainings

S. No.	Activity	Timelines (Months)																							
		37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
	Trigger- Sign off on Migration and Trainings																								
	4-Project Monitoring and Support																								
34	Review meetings with CCAs on project implementation status																								
35	Development of Assessment framework																								
36	Assessment of System acceptance by users																								
37	Future roadmap- linkage with other Ministry's IT systems																								
38	User Grievance Management																								
39	Steering Committee decision on project sign off					M7																			
40	Cost Benefit analysis																								
41	SLA Monitoring																								
42	Application and IT infrastructure Audit, Review of Network and websites																								
43	Technology assessment- Scalability, reliability, Support and security																								
44	Compliance to standards & guidelines																								
45	Operations and Maintenance																								

Project Milestones:
M7- Project Sign Off

12.3 Solution development option

Options for development of the proposed system are described in this section; it includes:

a) In-house development by NIC development team

b) Development of bespoke application along with some COTS products for document management, payroll processing etc.

c) Deployment of COTS with customizations

d) Complete outsource solution with monitoring of service levels

These development options for the proposed system are evaluated on the following parameters:

a) **Cost:** A qualitative comparison of costs among these options is mentioned.

b) **Feasibility/ease of implementation:** It describes the any major dependency and any mandatory requirements for that particular option.

c) **Timelines for implementation:** A comparison of tentative timelines for solution development/deployment is described.

d) **Change Management:** A comparison of management of technological changes is given.

S. No.	Criteria	In house development (NIC)	Be-spoke (Implementation Agency)	CoTS (Customization by Implementation Agency)	Complete Outsource (SLA Monitoring)
1	Cost	Minimal in comparison to other options	Average	High	Average to High (Depending on bespoke or CoTS based solution
2	Feasibility/ease of development	NIC team at the CGA's office needs to be	Clear terms and conditions of application	Clear terms and conditions of application	Stringent service levels to be defined. Project

S. No.	Criteria	In house development (NIC)	Be-spoke (Implementation Agency)	CoTS (Customization by Implementation Agency)	Complete Outsource (SLA Monitoring)
		adequately augmented to meet these new enhancements and emerging requirements. Implementation period will be more than deployment of CoTS	development need to be defined, along with stringent SLAs, Implementation period will be more than deployment of CoTS	development need to be defined, along with stringent SLAs, Implementation period will be shorter than Bespoke as around 30-40% customizations will be required.	Management overheads related to application development, deployment of hardware etc. are lower as service levels needs to be monitored
3	Timeline	1.5 - 2 years (Approx)	1.5 - 2 years (Approx)	1 Year (Approx)	Depends on bespoke or CoTS based solution
4	Change Management	Managing technological changes is easier due to in-house team	Mechanism for change request for issues related to application development and deployment of hardware to be established.	Mechanism for change request for issues related to application development and deployment of hardware to be established.	Mechanism for change request with respect to non compliance of service levels to be established.

13 Annexure

13.1 Network Costing[10] - Annual Cost Estimate

		Amount	Total (A)	Annual Charges for VPN Connectivity (256 Kbps) in Rupees (B)	Annual Expenditure for VPN Connectivity (256 kbps) in Rupees (A*B)
PAOs	Remote PAOs	44	496	**1,95,619**	**167,89,97,887**
	Non-remote PAOs	452			
DDOS	DDOs in Tier 1 Locations	4487	8087		
	DDOs in Tier 2 Locations	1143			
	DDOs in Tier 3 Locations	1337			
	DDOs in Remote Locations	1120			
Total			**8583**	**1,95,619**	**167,89,97,887**

Assumptions:

- Costing provides only VPN connectivity annual operational expenditure
- The costing does not include initial capital expenditure such as switches, routers, modem, VPN devices etc.
- The annual charges for providing VPN connectivity by BSNL are:
  - ✓ Rs. 6,62,362 per year for 2 Mbps line.
  - ✓ Rs. 1,95,619 per year for 256 Kbps line
  - ✓ Rs. 1,17,697 per year for 128 Kbps line.
- Assumed 256 Kbps VPN connectivity is provided across all PAOs and DDOs

[10] The cost is in addition to that provided in section 5.2.4, Budgetary Estimates for COTS Implementation

13.2 Guidelines for Data Centre

Physical Security and design guidelines for the Data Centre

- The Data Centre should ideally be built in a central location within the building complex.
- It should never be built in the basement or at the top floor. Since it would be difficult to maintain the environmental & physical controls at the basement or at the top floor.
- The Data Centre area may be logically divided in zones based on the level of security as described below:
  - Zone A: is the DC Server room area that has server racks, storage racks and networking equipment.
  - Zone B: comprises of NOC room, reception area, Help Desk area, Call Centre, Testing/Monitoring room.
  - Zone C: comprises of room for power panels, BMS Manager Room, AHU, UPS, Telecom Room, etc.
- Modeling techniques such as Thermal modeling may be used to arrive at the placement of racks in the DC server room. The rack should be designed taking into consideration the maximum amount of cooling for equipments / servers.
- The server room should have an emergency panic latch door with automatic alarm system. The vendor should provide a fireproof cabinet to store on-site backup tapes taken daily, weekly, monthly and half-yearly. Walls for the Data Centre should be Fire-Rated to prevent any further spread of fire

Electrical System

- The distribution system should meet with Tier - 1 requirement and should have enough provision to scale up if required in a later stage. It should have provision for Dual Bus configuration in order to have dual power supplies to each rack, thus minimizing downtime during maintenance operations. Dual feeders should also be provided for incoming feed from the main feeder.
- Power Supply for each rack should be from different power sources. The concept is based on n + 1 redundancy, where n is the number of systems or main items of equipment required to maintain the specified operational requirements. That means, failure of a single such system or equipment item can be tolerated.

- All switchboards should be designed to support non-linear load with neutral conductors at least 1.7 times or 2x phase/line conductors, this is as per IEEE1100- 1999 specifications. Panel boards should be divided into two, one from UPS and the other from generator. These panels should be installed separately in their respective zones.

- Incoming electrical lines should have primary and secondary Transient Voltage Surge Suppressors (TVSS) installed, primary TVSS just after the Main LT switchboard and secondary just before the UPS. The primary should take care of very high transients (kilovolt range) caused by lightning strikes or HT surges and the secondary should take care of whatever manages to pass through (several hundred volts in range) the primary TVSS.

- Adequate illumination (Lux) should be designed for the Data Centre. The illumination can be divided into two zones; specific rooms & other areas. Power source for lighting in these specific rooms should be from Emergency Panel for high availability purpose.
- Lighting on rack area and cage area need to be adjusted in order to eliminate lighting in un-proper areas such as over the top of the rack for the purpose of energy saving and cost saving.
- Design of grounding should be a single ground system with separated ground window for power and data conforming to international standards.
- UPS System design concept is based on redundancy and availability, with true- online system. To support the dual bus system configuration, two units of UPS should be installed. The Zone A area should be having two parallel redundant UPS and other areas like NOC and help desk should have another UPS system
- The solution should be automatic with power supply from the transformer as the primary source and automatic switchover to DG set as a secondary source for the data centre. Earthing should be provided from the electrical room control panel to the Earthing pits.
- The Data Centre should have generator set to take care of high availability. The generator should have adequate capacity to supply to full load specifications
- Surge protection should be installed at switchboard to suppress surge and EMI conforming to IEEE62.41 and UL1283.
- The Data Centre should have an AMF Panel connecting the DG, UPS such that automatic switchover takes place during power failure.

Surveillance

- Video Surveillance or CCTV System has to be provided mainly for security purposes. Adequate units of cameras should be installed to cover all areas of the Data Centre and premise surveillance. All these cameras should be coupled with motion sensors so that cameras can start recording only when they detect movement in the corresponding area. All the data should be recorded in digital format onto hard disk/Tapes for future investigation. There should be a central monitoring room to monitor the movement in the Data Centre & premises.

Access Control

- Proximity card reader and proximity access control system should be installed with its software for monitoring the access of individual persons in the Data Centre. This should be installed inside as well as outside the Level 2 premises.
- Biometric authentication should be deployed at the main access door of the server room area (Level 3). This device should support fingerprint scanning and numeric authentication.

Water Leak Detection System

- Sensing cable should be installed along room perimeter especially along the glass windows, and wall area, toilet adjacency area, and under air condition units in order to sense liquid leakage.

Fire Detection & Suppression

- Industry standard ionization and photoelectric detectors should be installed all over the Data Centre area. A separate fire alarm panel should be deployed for Data Centre area. In case of fire detection, this panel should communicate the alarm signal to the master fire panel that monitors the entire premise. It should also have the capability to send audio/visual signal at security area.
- The whole system should have fire detection and alarm panels along with manual call stations. For added protection, Very Early Smoke Detection System (VESDA) should be installed for the server room area only. The technology is based on lasers and very effective for detecting fire possibilities.
- The entire Data Centre is divided into two major areas, critical and non-critical. The critical area consists of server room (Zone A) and non-critical areas consist of other areas (Zone B, C).
- NFPA standard 2001 compliant fire suppression system should be installed for Zone A. For other areas, hand-held fire fighting devices should be installed at accessible locations; these are primarily CO2 gas based Fire Extinguishers

Pest Control & Rodent Repellent & System

- Pest Control system should be provided for the entire Data Centre & Rodent repellant system should be provided mainly in areas where false flooring is provided within the Data Centre. The electronic Repellent system shall be provided in such manner so as to protect the entire volume of space under consideration including above false ceiling, below false ceiling and below false floor.
- A separate entrance is recommended for access to UPS/Power room, and client room maintenance. The technician and engineers will frequent these areas.

Monitoring System

The monitoring system for all the installed equipments should be installed in one centralized panel at NOC room, which can monitor the following equipment(s):

- Water leak Detection
- On and Off of Air-conditioning system, and its alarm
- Humidity and Temperature

All the systems proposed should be connected to a BMS system. Planning for the BMS should accordingly be carried out.

Best practices and Guidelines on Data Security, Privacy, Confidentiality and Protection

Accessing Data but staying in control of data security

To ensure that security is implemented and maintained within the Data Centre, a security policy may be developed and enforced. The security policy must include the following:

- The overall security goals.
- An outline of the overall level of security required.
- The security standards, including auditing and monitoring strategies.
- Definitions of training and processes to maintain security.

Formulate and implement Trust and Identity Management Policy

- This is done to permit only authorized users and administrators to access Data Centre resources.
- Authenticate users prior to accessing services from the DC, which would provide accountability for the transactions/activities performed within the system.
- Using Public Key/Private Key infrastructure for AAA access mechanism to the users for providing access to the sensitive transactions.
- Undertaking risk assessment of the services/transactions processed using the information systems. For the critical and sensitive transaction (e.g. e-Payments), PKI based authentication shall be used.
- Using use digital Signature, Digital certificates/biometrics for authentication of users performing critical transactions in the system (e.g. for performing tax changes to the tax related values (master tables in the system, PKI/biometrics based authentication is required).
- In case of less sensitive data, using token based or strong password based authentication mechanism for services/transactions where public key certificates are not feasible.
- Conducting security posture assessment to identify vulnerabilities and risks, with specific breakdown by host, operating system, application, data, network devices, and links. This assessment provides vital information for determining appropriate risk levels for each asset and the maintenance requirements for maintaining each one to the desired security level and should be incorporated into the security policy**.**
- Setting security levels for each zone: These separate the data centre into areas that are logically separated from one another to contain an attack at minimal impact. Zones can support individual applications or application tiers, groups of servers, database servers, Web servers, e-commerce zones, and storage resources. User access can be limited to Web servers, protecting the application and database tiers from accidental or malicious damage. .
- Deploy control access between zones with firewalls and routers. Firewalls provide perimeter control for state-full inspection of connections to and from the data centre while blocking access to non-public services and hosts through ingress and egress filtering. Routers provide Layer 3 segmentation between zones, inter-VLAN routing, bandwidth rate limiting, and traffic analysis.

- Implementing Perimeter Firewall (Separating Internet from DMZ) and Internal Firewall (Separating DMZ from internal network) to increase the defence against vulnerabilities.
- Using advanced tasteful packet and application-layer inspection firewall, virtual private network (VPN), and Web cache solution that enables internet clients to retrieve the static content from the cache by improving network security and performance for both the Perimeter Firewall and Internal Firewall.
- Implementing network IPS for critical network segments. Network IPS is used for analyzing traffic streams to identify and thwart attacks such as DoS and hacker activity. The system alerts the management console and/or invokes an automated response within the network infrastructure to "shun" or block attacks as they are identified. IDS can also dynamically command firewalls or routers to block packets from identified malicious sources, reducing the effort needed to mitigate the attack.
- Deploy endpoint protection for critical servers and hosts by deploying Host based IPS. This functionality discovers attacks in progress, protects operating systems and applications, and sends alarms to the management console when an exploit is detected.

Secure the storage network at the DC and may consider SAN security as follows:

- Securing the SAN from external threats, such as hackers and people with malicious intent.
- Securing the SAN from internal threats, such as unauthorized staff and compromised devices.
- Securing the SAN from unintentional threats by authorized users, such as mis-configurations and human error.
- Securing and isolate each storage environment from other storage environments even if they share the same physical network.
- SAN should support cloning (creating copy of production disks) onto less expensive disks from which the backup would be performed without affecting the performance of the production disks/LUNs.

Data Privacy policy guidelines for accessing data

- Formulate a privacy policy statement and place on all relevant Intranets, Internet and Extranet sites. On-line privacy policy statement would reflect approach to data/information privacy that addresses internal and external aspects of best privacy practices.
- Mandate privacy policy statement in all relevant internal and external documents and press/media. For higher security of the documents they have to be stored a database. The solution should support versioning capabilities to ensure effective and responsible management of the documents.
- Obtaining consent, when appropriate, from individuals for any personal data collection activities that the O/o CGA declares in its privacy policy. Consent can be obtained by using online forms containing checkboxes or by asking individuals to sign and return a written consent form.
- Mandate access to the database/production servers and thus access to the data must be in control of system administrator. The root or administrator password must be

known to both the nominated representative of user group and system group so that both should agree before making any major changes in the database.
- Other users accessing the server would be provided with captive account so as to confine and control their action.
- Each activity related to delete or update operation on the database even if the nominated authorized person does it must be logged for the purpose of audit trial and the logs must be protected via proper security mechanism.
- Console operator would also be given captive accounts for performing routine and repetitive jobs such as taking backup, doing recovery and generating the accounting reports. They must not be allowed to come on the OS prompt.
- Use enterprise backup software to perform backups onto Automated Tape Library and these tapes should be transferred to a safe place away from the Datacenter to avoid loss of data in an event of disaster.
- Mandate to have hierarchical layered structure defined for different types of users falling between super users (root user, account holder) and console operator with different access rights for the proper safety of the data.

Data Confidentiality

- O/o CGA may allow the Operator to come into possession of highly confidential records whereupon the Operator shall maintain the highest level of secrecy, confidentiality and privacy with regard thereto.
- Additionally, the Operator shall keep confidential without any disclosure of all the details and information with regard to the Project, including systems, facilities, operations, management and maintenance of the systems/facilities.
- Retain all rights to prevent, stop and, if required, take the necessary action punitive or otherwise against the Operator regarding any forbidden disclosure.
- The Operator shall ensure that all its employees, agents and sub-contractors execute individual non-disclosure agreements, which have been duly approved by the O/o CGA, with respect to services provided from the DC.
- The aforesaid provisions shall not apply to the following information:
    - Already in the public domain; and
    - which has been received from a third party who had the right to disclose the aforesaid information; and
    - disclosed due to a court order.
- The stakeholder of the data/applications and the party using the same should sign a Non-Disclosure-Agreement (NDA) with the O/o CGA.
- O/o CGA would formulate the policy of Intellectual Property rights with the concerned line departments while hosting/keeping their data into the DC with overall control being with the O/o CGA

Data Protection mechanism from loss

- Implement proper RAID mechanism to avoid loss of critical and comparatively less sensitive data.
- Use Enterprise Storage Area Network based storage system for critical applications running on different hardware server machines.

- The SAN Storage system should be capable of Selective Storage Presentation (A feature by which storage volumes designated for access by a specific server would be fire-walled from all other devices on the SAN) and should support heterogeneous environments.
- The Storage system should also support hot add, hot removal and disk layout reconfiguration without the need to restart the system.

Disaster recovery and business continuity plan guidelines

- Establish a Disaster recovery and Business Continuity Plan for Data Centre considering various approaches/strategies and selecting the best, suiting the O/o CGA's DR & BCP requirements provided the recovery location is in different seismic zone.
- Follow best practices for Application, IT infrastructure, Network and Data at the DC as per the IDC standards.
- Formulate a backup policy to periodically backup the data from online machine (hard disk) to offline. Database consistency check utilities must be run to verify that the data backup is consistent and can be used confidentially to recover data at the time of crisis. Periodic checks should be conducted on the backup tapes by way of restoration.
- Advise the DC operators to apply patches/upgrades regularly on the IT infrastructure including Servers, Operating systems, databases, application related, network equipment and on the storage system protecting the resources from known issues.
- Mandate to check the health of storage box including functioning of controllers of hard disk and be monitored regularly.
- Form proper database recovery policy for different kind of failures to avoid even the slightest piece of data being getting lost. To reduce the recovery time of database, the database size should be kept under control by regularly purging the data and archiving it on the offline media, which is not required for online operation.
- Organize and manage a dedicated contingency planning team. They will develop the detailed work plan and schedule for development of BC & DRP. They will determine which aspects of the services and operation of the DC are most critical and creates the justification for the overall plan. The preliminary analysis assesses the potential risk and impact on the service delivery and operations, identifies recovery requirements and lists alternative strategies. In case of contingency, the BCP technical support team determines the feasibility of the plan from a technical standpoint and ensures that all critical alternate locations have the equipment and technical support to continue the services and operations.
- Come out with a clear definition of individual responsibilities, including who has the authority to declare a disaster and initiate BCP procedures; with a list of contacts of key personal as and when required in case of emergency.
- O/o CGA would encourage keeping a vital system/software documentation at the backup site.
- O/o CGA would ask the partners to lay down the procedures for retrieving and restoring information and data from off-site storage facility and be clearly documented.
- O/o CGA would keep a copy of complete Recovery Plan and steps involved at the off-site (backup site) with authority defined to use this documentation.

- The data replication between DC and DR site should be done by replicating the transaction logs that would be restored automatically at the DR Site supporting near real-time data availability at the DR Site

Monitoring and Management of DC

- O/o CGA would implement state-of-the art monitoring tools. These tools are deployed for centralized policy provisioning, monitoring, and troubleshooting of security components and IOS Software features. This solution should include event monitoring and correlation to filter alerts sent to the management console. Communication with data center network devices is most secure using an out-of-band network or through a dedicated administration VLAN. It is recommended to encrypt management traffic with SSL, Simple Network Management Protocol (SNMP) version 3, or Secure Shell (SSH) technology.
- O/o CGA would need to implement management solutions to proactively manage the servers, which would alert the administrator as, and when each service of the data center reaches the defined threshold before the failure occurs on the servers or devices to ensure increased uptime of the Data Center.
- O/o CGA to deploy solutions to perform automatic patch management to reduce the manual intervention for ensuring that the operating systems and other system software are current, which reduces the impact of vulnerabilities.
- Define polices for periodic monitoring of activity on the firewall server to check for malicious activity
- Define polices for performing periodic health check on the all servers with the Data Center
- Define Backup and restore policy
- Deploy Help Desk solution to track and manage the calls logged and resolved
- O/o CGA to implement antivirus solutions to automatically update to latest anti- virus signature files
- O/o CGA to perform periodic audits on the Data Center using a Third party consultant on the following :
  - Security polices define and its implementation
  - Reviewing of the activities performed for management team
  - Reviewing the Access control to the data center
  - Reviewing the Health Check results and the actions taken
  - Reviewing on the uptime of the service to determine the conformance to the SLAs of the Data Center
- Other important activities that should be managed at the Data Center:
  - Daily maintenance of system configuration
  - Overall security of the network
  - Day to day disk space management
  - Tracking the servers performance and take the remedial and preventive actions in case of problems
  - Proper upkeep of storage media and perform daily backups based on the backup policy
  - Monitor Physical access to the Data Center

Monitoring Access to Data

- Ensure that all IT related infrastructure used would generate granular logs from which information could be derived.
- Using technologies to harvest such logs and to consolidate & analyze logs generated by such infrastructure.
- Periodic analysis of such logs to bring in changes to the security posture to mitigate risks from newly identified threats.

Data Security while Retiring Data/Infrastructure

Prepare guidelines to retire any infrastructure. It is to be ensured that the data on such an asset is backed up and is removed from the asset before it is retired. Data that becomes inconsequential or irrelevant due to various factors must be archived using a proper archival mechanism. Data which needs to be destroyed must be destroyed immediately and proper guidelines need to be defined as a process for the same.

Security Audit

The O/o CGA shall get the security audited by third party expert periodically (once in six months) to ensure and guarantee security of the Data Centre. The audit shall bring out any security lapses in the system and establish that the system is working as desired by the O/o CGA.

Computing requirement Considerations

Computation environment Consideration	Requirements	Standard parameters
Server Management	Monitor critical resources of operating system	• Monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable, using agents on the servers to be monitored. • Configure the operating system monitoring agents to monitor based on user-defined thresholds for warning/ critical states and escalate events to event console of enterprise management system. • Integrate with enterprise management system and support operating system monitoring for various platforms including Windows 2000/2003 and various flavors of UNIX and Linux. • Provision exists for performance scoping and trending to provide real time as well as historical reporting, where specified. • Provide performance configuration to enable agent configuration to be done from a central point of control, using intuitive GUIs that provide a common look and feel across various platforms in the enterprise. Performance profiles could be defined in this GUI, and, using drag-and-drop techniques, delivered to the various specified machines in the enterprise running performance agents. These agents could then dynamically reconfigure them to use the profiles they receive. • The event generated as a part of Server management should go to a common enterprise event console where a set of automated tasks can be defined based on the policy. Events from Network Management monitoring SWAN will integrate together
Database Management	Monitor critical resources and parameters of databases	• Proactively monitor various critical relational database management system (RDBMS) parameters such as database tables / table spaces, logs etc. where applicable, using agents on the servers to be monitored. • Integrate with enterprise management system and support monitoring of various RDBMS including MS SQL Server and Oracle. • Configure the database monitoring agents to monitor based on thresholds. When thresholds are exceeded, the agents would be able to send alerts to event

Computation environment Consideration	Requirements	Standard parameters
		console of enterprise management system. • Monitor various database parameters depending on the database being monitored yet offer a similar interface for viewing the agents and setting thresholds. • The Database Management function would automatically discover all Sever databases as well as configuration information and store it in the object repository. • The Database Management function would be able to enforce sophisticated policies that monitor and correlate multiple events
Help Desk	Provide centralized help desk system	• Provide flexibility of logging incident manually via windows GUI and web interface. • The web interface console of the incident tracking system would allow viewing, updating and closing of incident tickets. The web interface console would also offer power-users tips. • Provide seamless integration to log incident automatically via system and network management. Allow detailed multiple levels/tiers of categorization on the type of incident being logged. • Provide classification to differentiate the criticality of the incident via the priority levels, severity levels and impact levels. • Each incident could be able to associate multiple activity logs entries via manual update or automatically update from other security tools or system management tools. • Provide audit logs and reports to track the updating of each incident ticket. Proposed incident tracking system would be ITIL compliant. • It should integrate with Enterprise Management System event management and support automatic problem registration, based on predefined policies. • It should be able to log and escalate user interactions and requests. • It should provide status of registered calls to end-users over email and through web
Web Management	Monitor critical web servers	• Web Server Management. The Web Servers would be proactively monitored for the availability, health and performance of Web servers. • The Web Management would automatically correlate the status of Server,

Computation environment Consideration	Requirements	Standard parameters
		Services, Disks, Invalid URLs, Polled URL Counters, Server Health, Polled Counters, Polled Events, and would provide alerts to the Web administrators. The alerts could also be integrated with Help Desk Management for efficient call tracking and problem resolutions. • Web Response Monitor. The Web Management would also provide capabilities to monitor and proactively alert Web Responses on availability, health, and performance of one or more Web sites and services from the perspective of a user attempting to access the site. • The Web Management would use combination of HTTP and FTP to determine the availability, round-trip response, and content for select web sites. • Web Traffic Analyzer. The Web Management would analyze the traffic and provide simple and easy to understand reports in tabular or graph formats that show statistical, demographic and trends in the performance and use of internal web sites. The Web Management would provide reports on the central. • Provides integrated management of Web server and components
Security Requirement Considerations		
Network Security	Minimal deployment of the following baseline controls on all network devices	• Use of login Banners at login time • Network traffic filters and Access Control Lists to restrict unauthorized traffic • Strong authentication mechanisms for all console or remote administrative access • Firewalls to permit only authorized traffic • Controls to ensure the integrity and confidentiality of the appropriate Domain Name Server data • Use of network based intrusion detection tools • Use of digital certificate verification between server/severs and server/client • Use of Virtual Private Networks or equivalent
Antivirus	Maintain anti-virus measures	• Host and Web based • Inbound and outbound monitoring on all data transfer mechanisms and all e-mail systems • Early virus alert service from vendors

Computation environment Consideration	Requirements	Standard parameters
		• Real-time on-line access scanning • Timely updates to signature files and search engines • Common solution for antispyware and virus infections. • Integration capabilities with security management solution for management and monitoring. • Heuristic scanning to allow rule-based detection of unknown viruses • 100% certified to protect against "in the wild viruses" by the ICSA
Host Server Security	Deployment of baseline controls on all host servers including detail description of operating/file system controls used to secure servers and access controls (authentication & authorization) on servers, platforms and databases	• Review all default settings • Strong access control lists to restrict unauthorized access • Remove unneeded network protocols, services, default or system user accounts, and any sample application code • Resetting of default passwords (includes periodic password resets) • Use of dedicated servers as required • Super user rights i.e. Administrator for windows and root for Unix should also be contained to them limit of those IDs not able to logs residing on the Operating System • Use of partitioned servers as needed • Provision for an Identity to be auditor with access to only logs and read only rights to configuration. This is to ensure that super users of Operating systems don't have access to logs. • Delegation of rights like maker, checker and auditor with one Identity having access to formulation of policy but not implement it, second identity having access to deploying policy but no access to define policy and auditor with access to logs. • Provision for a warning mode that can be used during implementation to verify policies and their impact before deployment. • The user's permissions must always be governed by the original login ID. Even taking over the root account should not grant the user any additional privileges. • Must be able to prevent hackers with root access from circumventing or shutting

Computation environment Consideration	Requirements	Standard parameters
		down the security mechanism. Must use a self-protected database for storing all security information. • STOP (Stack Overflow Protection) to prevent stack overflow exploits on systems, to ensure that arbitrary commands cannot be executed in order to break into systems • Other measures as recommended by the OS vendor
Identification, Authentication & Authorization,	Restrict electronic access to the Web site or application beyond user level access to only authorized persons	• Security Controls • The users are uniquely identified and authenticated by the systems. The use of any form of generic or shared user identifier is expressly prohibited • User-level access enforce by the "least privilege" principle (i.e. Users/Application • Administrators only have the level of access to the system required to perform their job functions.). • Use of strong industry standard encryption technology (e.g. 3DES or Blowfish) to encrypt data identified by the O/o CGA as per data classification (e.g. "sensitive" or "confidential". • A common security layer for all application reducing the time to launch new application and maintaining security. • The security layer should be able to integrate with all industry leading authentication mechanisms. The security mechanism should not run as a process or service which can be killed or stopped to allow access to entire infrastructure. • Policy information should be stored directly in LDAP, so that a single directory can be used to store both user and policy information. • Applications should use a central LDAP, NT, ADS , SQL DB as authentication directory • For web based application the cookies should be 128 bit encrypted and session management capabilities should also be built in common security layer. • Administrator should be able to specify that a certain directory be used for user authentication, but a different directory be used for user authorization. Option should allow multiple directories to be configured.

Computation environment Consideration	Requirements	Standard parameters
		• Following password management features should be part of common security layer • Management of Passwords: • Passwords changed at least every 45 days • Default passwords changed immediately upon account creation • Password file must be encrypted and secured • Ten (10) unique passwords within a password history cycle • Password length at least 6 characters • Use of strong password structure (Ex: "Pa33WorDS") • Password measures enforced automatically • Management of User Accounts: • User accounts and passwords audited every 90 days for compliance • Accounts disabled or locked after 3 failed login attempts within a 30-minute period. • Locked accounts re-enabled by authorized system or security administrator • Verification information for resetting passwords selected by Client • Time-out feature for inactivity • Inactive user accounts purged after 90 days
Data Transmission Security	Safeguard the confidentiality and integrity of all data being transmitted over any form of data network	• Strong, industry standard encryption for the data identified as 'sensitive' or 'confidential' as per data classification. (Examples include SSL for Web browser sessions, or PGP file encryption for bulk data transfers.). • Secure Socket Layer ("SSL") or stronger encryption techniques for network access via the public Internet. • Strong industry standard tools for monitoring, controlling, and administering electronic transmissions
Firewall Services	Use of firewall tools and services in accordance with the Data Centre	• Controlled implementation and scheduled maintenance of firewall rule set changes • Active monitoring to identify attempted or actual security violations • Controlled emergency maintenance of firewall rule set changes

Computation environment Consideration	Requirements	Standard parameters
	requirements, policies and procedures, including general maintenance and monitoring of firewalls and implementation of firewall rule set changes.	• Two (2) business day turnaround time for firewall rule set changes
Intrusion Detection and prevention Services	Use of intrusion detection/prevention tools to detect unauthorized access to or unauthorized activity on the networks, computer systems and network devices associated with the Data Centre	• Network and/ or Host based • Active monitoring to identify attempted or actual intrusions • Timely updates to signature files
Security Monitoring	Provide monitoring services	• Real time monitoring of all systems and network devices/systems to detect potential security violations. Such monitoring will include but is not limited to operating system access, detection of unauthorized processes or software, unauthorized modification of existing software or data, or unauthorized configuration changes to computer systems and network devices. It will also include the logs of all firewalls, intrusion detection/prevention systems, physical access controls or other security-related systems • Retain the logs of all security-related systems, to include but not limited to firewalls, intrusion detection systems, access control measures (both electronic and physical) and file integrity checker logs for forensic or evidentiary purposes

Computation environment Consideration	Requirements	Standard parameters
Incident Response	Reporting of any and all security incidents	• Security Incident Response Plan acceptable to the O/o CGA • Log of security incidents must be maintained and classified as confidential and proprietary property of the O/o CGA • Incident Report and Action Plan per incident
Storage Requirements		
Backup	Provide centralized online backup for mission critical applications	• Proposed Backup Solution should be available on various OS platforms such as Windows and UNIX platforms and be capable of supporting SAN based backup / restore from various platforms. • Proposed backup solution shall take back-up of databases. • Proposed backup solution shall have same GUI across heterogeneous platform to ensure easy administration. • Backup software should support backup to disk that allows users to use disk technology as an intermediate step in the backup process. This allows faster access speed and higher reliability of disk technologies ensures reduced backup and restore time as well as higher success rate for backups. • The proposed Backup Solution should support the capability to write up to multiple data streams to a single tape device or multiple tape devices in parallel from multiple clients to leverage the throughput of the Drives using Multiplexing technology. • The proposed Backup Solution should have 'Hot-Online' backup solution support for different type of Databases such as Oracle, MS SQL, etc. • Backup software should create a media index (catalog) file on your media to improve performance for merge jobs and database backup jobs. • Backup software should provide command line utilities an alternative method of accessing the operations available from the GUI Manager. • Backup software should also provide report writer that allows designing of report templates which can be used to generate meaningful reports in Comma Separated Value (CSV) or extensible Markup Language (XML) format.
Storage Resource	To manage and	• Discover the infrastructure and monitor file system devices

Computation environment Consideration	Requirements	Standard parameters
Management	monitor storage resources effectives distributed on SAN/ NAS	• Understands application, server, and subsystem performance and availability Capacity management: Collects physical (configuration and information) and logical (volume space) information of SAN components, which shall be used to generate reports Configuration Management: The ability to monitor the storage for applications based on capacity and performance. • Event Management & Reporting: Problem notification for storage administrators, reports generation for daily activities, real time reports for SAN environment • Policy management: Dictates storage policy and enacts actions on hardware, files, users, etc • Shows the components, affected servers, applications • Should provide detailed reports on storage access and usage pattern

Human Resource requirement guidelines

S No	Position	No of resources	Profile	Roles & Responsibilities
1	Data Centre Manager (Project Manager)	1	The desired profile of the candidate should be minimum B.E. (Computer/E&C/Electrical)/ MCA preferably MBA with 6-8 years experience. Candidate should have exposure to BS15000 process /ITIL or ITIL certified and have a proven track record of managing operational IT support teams including establishment of RMC /processes, technology & Staffing. PMP Certification is a plus	Responsible for overall management of the Data Centre, user SLA commitments, performance, availability, response time, problem resolution etc. Candidate should also be responsible for effective Resource management; System & Resource planning based on business forecast and would be the single point contact for managerial responsibilities and direct interface with IT head. Data Centre Manager should have capabilities in team management, capacity planning and process documentation
2	Database Administrator	1	The desired profile of the candidate should be B.E. (Computer/E&C)/MCA with 3-4 years experience in administering production data bases and worked in Oracle 9i, 10g, DB2, MS-SQL etc. Knowledge in PL/SQL Programming with experience in handling standby databases preferred.	Responsible for Database Administration, Web Administration, Application Hosting, Web Designing, Staging and other related services. Candidate should

			Must have technical certification in Data Base Administration	also be responsible for database and application change management procedure.
3	System Administrator	1	The desired profile of the candidate should be B.E. (Computer/E&C)/MCA with 3-4 years experience in sys admin of RDMB data (MS-SQL, Oracle etc.), system admin windows-2000/UNIX/Solaris etc. server, programmer of Java, C, C++, SQL, PL/SQL, Corba etc. Technical certifications on Oracle/SQL/SUN products etc. is must.	Responsible for OS administration / management, database configuration, scalability, performance, load- balancing, troubleshooting & debugging and monitoring of servers. Candidate should implement the back-up plan for storing and retrieving of data, maintain servers, machines, printers and also responsible in resolving the real time (RT) requests raised by users as per SLA.
4	Network Support Staff	2	The desired profile of the candidate should be B.E. (Computer/E&C)/MCA with 3-4 years experience as mentioned above. Certification like CCNA/CCNP/PIX/CCSA would be preferred.	Responsible for network uptime, security, performance, monitoring and other related services. The candidate should be well versed with Routing and Switching devices and technologies like ATM, Frame Relay, MPLS, Wireless, Broadband and Protocol Analysis Tools. Must have

				beginner to intermediate skills in Information Security technologies like Anti-virus, Firewalls, 2 & 3 factor Authentication, IDS, IPS, Content Filtering, Encryption, VPN, Threat Management and be familiar with Information Security Audit parameters.
5	Technical Support Services	4		Responsible for L2-support, H/W &S/W support and would provide help to the Data Centre Operations & Management Core Team in quick resolution of problems. The technical support team would work on shift basis and ensure uptime of services. Candidate should be responsible for escalating the call to the specialized domain and closely work with the domain experts and do the first level of analysis once call is logged by the help desk support team and ensure uptime of services through NMS and generate reports

				to meet the SLAs signed by the O/o CGA with different stakeholders.
6	Help Desk Services	2	The desired profile of the candidate should preferably be Graduates/Diploma holder in Hardware/Networking with good communication skills and proficiency in English and local languages	Candidate should be capable of complete call management process with standard call logging and escalation tool. The requirement of manpower for Help Desk Services may increase as demand grows and more services are added to the Data Centre.
7	Administration/HR -	1	The desired profile of the candidate should be Graduate with Masters/ PGD-HR/PM/IR with 2-3 years working experience in the administration / recruitment / logistic support of manpower and worked either with Data Centre operation or with an IT/ITES industry with good communication & HR management skill.	The persons recruited should be responsible for entire Data Centre administration, Logistic support, procurement, Stationery, administrative co-ordination etc.

13.3 List of DDOs/ PAOs

13.3.1 List of 452 Non Remote PAOs

000162 - PAO(Directorate of Extension),New Delhi
000264 - PAO(Agri-Coop),Mumbai
000365 - PAO(Agri-Coop), Chennai
000476 - PAO(Agri-Coop), Cochin
000569 - PAO(Plant Protection & Misc), Faridabad
000743 - PAO(Sectt)-II, New Delhi
000824 - PAO(Agri-Coop),Kolkata
004797 - PAO(DMI), Nagpur
075602 - PAO AHD and Fisheries, Mumbai
001765 - PrPAO(WR),New Delhi
001793 - PAO(HQ), New Delhi
001872 - PAO(CWC), New Delhi
001954 - PAO(CWPRS), Pune
002032 - PAO(Farraka Barrage Proj),Farraka
002338 - PAO(CGWB), Faridabad
002450 - PAO(CSMRS),New Delhi
003433 - PAO(Food), New Delhi
003521 - PAO(Food), Mumbai
003603 - PAO(Food), Kolkata
003687 - PAO(Food), Chennai
003710 - PAO (Consumer Affairs) Kolkata
003810 - PAO (Consumer Affairs) Mumbai
003850 - PAO (Consumer Affairs),Chennai
071504 - PAO(Consumer Affairs),New Delhi
001710 - PAO, Land Resources
001711 - PAO, Drinking Water Supply
004710 - PrAO cum PAO(Sectt.), New Delhi
005942 - PrAO-(Fert-I), New Delhi
006953 - CPAO(Commerce), New Delhi
007032 - CPAO(CCI & E), New Delhi
007115 - RPAO(Commerce), Kolkata
007202 - RPAO(Commerce), Mumbai
007290 - RPAO(Commerce), Chennai
007377 - PAO(Textile), Kolkata
007468 - CPAO(All Ind.Handicraft Board),New Delhi
007638 - PAO(Textile), Mumbai

007726 - PAO(Textile), Chennai
007815 - PAO(Textile), New Delhi
011751 - PAO (Secondary Education & Higher Education)
011700 - PAO (Deptt. of Elementary Education & Literacy)
012435 - PAO(Min. Of SJ & E),New Delhi
013455 - PAO(Sectt.), Ministry of Power, New Delhi
013533 - PAO (CEA), New Delhi
013617 - PAO(CEA), Bangalore
013693 - PAO(BMCC), New Delhi
014775 - PAO(Coal), New Delhi
014859 - RPAO(Coal), Dhanbad
015200 - PrAO Cum PAO (M/O Tribal Affairs)
015954 - PAO(DE), New Delhi
016001 - PAO, O/O CGA, M/O Finance, D/O Exp.
016100 - PAO, INGAF, New Delhi.
016977 - PAO(Sectt.), Economic Affairs, Min of Finance, New Delhi
017057 - PAO(ERIS and Banking), New Delhi
017136 - PAO(NSO), Nagpur
017242 - PAO(I.G. Mint), Kolkata
017320 - Astt.Dir(Cost)& PAO(I.G. Mint),Hyderabad
017398 - PAO(I.G. Mint), Mumbai
017476 - PAO(ISP), Nasik Road
017555 - PAO(BNP), Dewas
017632 - PAO (SPM), Hoshangabad
017709 - PAO(Accounts), New Delhi
017784 - Asstt. Dir.(Cost) & PAO(SPP), Hyderabad
017859 - PAO(CNP), Nasik Road
017940 - PAO(New Mint Project), NOIDA
019795 - PAO(Revenue), New Delhi
053401 - PAO(CBN), Gwalior
053509 - PAO(GOAW), Ghazipur
053586 - PAO(GOAW), Neemuch
020866 - PAO(Sectt.), Ministry of Health & FW, New Delhi
020946 - PAO(DGHS), New Delhi
021029 - PAO(CGHS), New Delhi
021108 - PAO(Safdarjung Hospital), New Delhi
021186 - PAO(NICD), Delhi
021277 - PAO(MSD), Mumbai

021371 - PAO(H & FW),Kolkata
021468 - PAO(H & FW), Pondicherry
021545 - PAO(H & FW), Chennai
021642 - PAO(RML Hospital), New Delhi
021721 - PAO(LHMC & Hospital), New Delhi
001756 - RPAO, CRPF,Kolkata
001757 - RPAO, CRPF,Nagpur
001758 - RPAO, CRPF,HYD
001760 - RPAO, ITBP,Dehradun
001761 - RPAO, NSG, Kolkata
001762 - RPAO, NSG,HYD
001807 - PAO, National Investigation Agency, NIA
001818 - Pay & Accounts Office, National Disaster Management Authority, NDMA
003266 - Pay & Accounts Office, NATGRID
003709 - RPAO (CRPF), Patna
004009 - PAO, Delhi Police Headquarter (DPH)
022744 - PAO (Sectt.), New Delhi
022878 - PAO(IB), New Delhi
022984 - PAO(Census), New Delhi
023093 - PAO(DCPW), New Delhi
023184 - PAO(ITBP), New Delhi
023283 - PAO(CISF), New Delhi
023608 - RPAO(CISF), Kolkata
023704 - RPAO(CISF), Ranchi
023801 - RPAO(CISF), Chennai
023903 - Dy. Director(A/Cs)CRPF, New Delhi
024055 - PAO, BSF-5, New Delhi
024450 - PAO, National Security Gaurd.
024650 - PAO (Pension & Misc.)
024876 - Shashastra Seema Bal, Patna
024886 - Shashastra Seema Bal, Lucknow
025301 - Shashastra Seema Bal, New Delhi
068447 - PAO No. IV (Delhi Police Tiz Hazari)
070332 - PAO No. XVI (Delhi Police Man Singh Road)
025403 - PrAO(Compilation), Ministry of Industry
025426 - PAO(Industrial Development), New Delhi
025591 - PAO(SSI), New Delhi
025695 - PAO(SSI), Mumbai

025791 - PAO(SSI), Kolkata
025898 - PAO(SSI),Chennai
026005 - PAO(Salt), Jaipur
026103 - PAO(PD & TM), Mumbai
026190 - PAO(Explosives), Nagpur
026281 - PAO(Hi & PE), New Delhi
026704 - PAO (Heavy Industries)
027667 - PAO(Main Sectt.), Ministry of Information & Broadcasting, New Delhi
027752 - PAO(All India Radio), New Delhi
027973 - PAO(DAVP), New Delhi
028062 - PAO(IRLA), New Delhi
028139 - PAO(All India Radio), Lucknow
028233 - PAO(All India Radio), Mumbai
028438 - PAO(All India Radio),Kolkata
028660 - PAO(Doordarshan),Chennai
028750 - PAO(Doordarshan), Kolkata
028825 - PAO(Films Division), Mumbai
029100 - PAO(Doordarshan), Nagpur.
029803 - PAO(Main Sectt.), Ministry of Labour, New Delhi
029922 - PAO(DGET), New Delhi
030050 - PAO(Chief Labour Commissioner),New Delhi
030181 - PAO(Labour Bureau), Chandigarh
030263 - PAO(DGFASLI), Mumbai
030352 - PAO(DGMS), Dhanbad
030461 - PAO, DGE&T-II, Chennai
031438 - PAO(Legal Affairs), New Delhi
031545 - PAO(Legislative Department), New Delhi
031626 - PAO(Electoral Office), New Delhi
031709 - PAO(Supreme Court), New Delhi
003173 - PAO, UIDAI, New Delhi
032714 - PAO(Planning), New Delhi
032800 - PAO(Statistics), New Delhi
032895 - PAO(Statistics), Nagpur
032991 - PAO(Statistics), Kolkata
033500 - PAO(PI),New Delhi
002192 - Regional Pay & Accounts Office, (NH), Bhopal
002193 - Regional Pay & Accounts Office (NH), Hyderabad
034050 - PAO(Sectt.), Road Transport, New Delhi

034415 - PAO(NH), New Delhi
034650 - PAO(NH),Mumbai
034756 - PAO(NH),Kolkata
034807 - PAO(NH),Bangalore
034862 - RPAO(NH),Chandigarh
034975 - PAO(NH),Jaipur
035036 - RPAO(NH), Lucknow
035521 - PAO(Steel), New Delhi
035600 - PAO(Steel),Kolkata
036617 - PAO(Mines), New Delhi
036699 - PAO(GSI),Kolkata-
036794 - PAO(GSI) Central Region,Nagpur
036879 - PAO(GSI),Jaipur
036963 - PAO(GSI),Lucknow
037055 - PAO(GSI),Hyderabad
037141 - PAO(GSI),Bangalore
037307 - PAO Indian Buearu of Mines, Nagpur
000965 - Pr. Accounts Office, Department of Commerce (Supply Division)
038363 - PAO(Supply), New Delhi
038447 - PAO(Supply),Kolkata
038531 - PAO(Supply), Mumbai
038614 - PAO(Supply),Chennai
011120 - PAO(Culture), New Delhi
011210 - PAO(Archeological Survey of India), New Delhi
011309 - PAO(Archeological Survey of India), Hyderabad
011397 - PAO(Culture), Kolkata
040866 - PAO(Sectt.), Ministry of Civil Aviation & Tourism, New Delhi
040951 - PAO (Tourism) New Delhi
041056 - PAO(DGCA & Safdarjung Airport),New Delhi
041255 - PAO(CAD),Mumbai
041386 - PAO(CAD), Chennai
041490 - PAO(CAD), Kolkata
042709 - PAY AND ACCOUNTS OFFICE (PTG.)
042805 - PAO, Printing, Kolkata
042890 - PAO, Printing, Nasik
042972 - PAO, Printing, Chennai
043053 - PAO(DGW), New Delhi
043144 - PAO(New Delhi Zone) CPWD, Min. of Urban Development, New Delhi

043335 - PAO(North Zone) CPWD, New Delhi
043460 - PAO(East Zone) CPWD,Kolkata
043571 - PAO, West Zone CPWD, Mumbai
043729 - PAO(Food Zone) CPWD, New Delhi
043884 - PAO(Sectt.), Ministry of Urban Development, New Delhi
043951 - PAO, CPWD (SZ), Chennai.
045067 - PAO, Heavy Water Board,
045144 - PAO(Heavy Water Plant), Baroda
045221 - PAO(Heavy Water Plant), Kota
045298 - PAO, Heavy Water Plants, Tuticorin,
045453 - PAO(Dirc. of Purchases & Stores), Mumbai
045531 - PAO, Madras Regional Accounts Unit,
045685 - PAO(BARC), Mumbai
045920 - PAO(I.G.C. for Atomic Research),Kalpakam
046151 - PAO(Nuclear Fuel Complex), Hyderabad
046228 - PAO, Atomic Minerals Directorate for Exploration and Research,
046295 - PAO, Department of Atomic Energy
046380 - PAO, Raja Rammana Centre for Advanced Technology,
046390 - PAO(Heavy Water Project), Manuguru
046400 - PAO, Board of Radiation & Isotope Technology
046450 - PAO(General Services Orgn.), Kalpakam
046500 - PAO, BARC Facilities, KALPAKKAM
046550 - PAO, Variable Energy Cyclotron Centre, Kolkata.
046600 - Directorate of Construction, Services and Estate Management
046630 - PAO, Atomic Energy Regulatory Board, Mumbai
046650 - PAO, Power Reactor Fuel Reprocessing Plant, ,
033195 - PAO, NIC, New Delhi.
047315 - Pr. cum PAO(DIT), New Delhi
048406 - PrAO cum PAO(President Sectt.),New Delhi
049429 - PAO(DP & AR), New Delhi
049521 - PAO(CBI), New Delhi
049634 - PAO(Cabinet Affairs), New Delhi
049720 - PAO(UPSC), New Delhi
049801 - PAO(Central Admn. Tribunal), New Delhi
001238 - PAO, Revenue, Kolkata
050005 - PAO, CEX IV, Thane, Mumbai
050045 - PAO, CENTRAL EXCISE & CUSTOMS, BELAPUR & RAIGARH
050090 - PAO, CUSTOMS (PREV.), MUMBAI

050135 - PAO, CENTRAL EXCISE & CUSTOMS, BHOPAL
050170 - PAO, CENTRAL EXCISE, BHAVNAGAR
050240 - PAO, CUSTOMS, AMRITSAR
050275 - PAO, CUSTOMS (PREV), JAMNAGAR
050672 - PAO Hq. (CBEC), New Delhi
050725 - PAO(Collectorate of C&CE), Ahmedabad
050812 - PAO(Collec. of Central Excise),Allahabad
050896 - PAO(Collec. of Central Excise),Bangalore
050982 - PAO(Central Excise Collectorate), VADODRA
051070 - PAO(Central Excise Collec.), Bhubneshwar
051151 - PAO(Collec. of Central Excise-I),Mumbai
051237 - PAO(Collec.of Central Excise-I),Kolkata
051323 - PAO(Collec.of Central Excise),Chandigarh
051408 - PAO(Collec. of Central Excise), Cochin
051493 - PAO(Collec. of Central Excise),New Delhi
051581 - PAO(Collectorate of C&CE), Goa-Panaji
051659 - PAO(Collec. of Central Excise), Guntur
051743 - PAO(Collec. of Central Excise),Hyderabad
051830 - PAO(Collectorate of C&CE), Indore
051917 - PAO(Collec. of Central Excise), Jaipur
052000 - PAO(Collec. of Central Excise), Kanpur
052084 - PAO(Collec. of Central Excise),Chennai
052170 - PAO(Collec. of Central Excise), Madurai
052257 - PAO(Collec. of Central Excise), Nagpur
052338 - PAO(Collectorate of C&CE), Patna
052425 - PAO(Collec. of Central Excise), Pune
052598 - PAO(Collectorate of Customs), Mumbai
052679 - PAO(Collec.of Central ExciseII),Kolkata
052775 - PAO(Collectorate of Customs), Kolkata
052853 - PAO(Collectorate of Customs), Cochin
052930 - PAO(Collectorate of customs), Chennai
053007 - PAO(Collec. of customs), Kandla(Gujrat)
053084 - PAO(Collec. of customs), Visakhapatnam
053161 - PAO(Dirc.of Inspc. & Audit,C&CE),N.Delhi
053245 - PAO(Dirc.of Stat. & Intll.,C&CE),N.Delhi
053755 - PAO(Collec. of Central Excise-II),Mumbai
053844 - PAO(Collectorate of C&CE), Merrut
053929 - PAO(Collec.of Central Excise),Coimbatore
054014 - PAO(Collectorate of C&CE),Tiruchirapalli

054097 - PAO(Collec. of Central Excise), Belgaum
054180 - PAO(Collec.of Central Excise),Aurangabad
054263 - PAO(Collec.of Central Excise-III),Mumbai
054347 - PAO(Collec. of Central Excise), Rajkot
054515 - PAO (Jawahar Customs House),Nhava Sheva
054565 - PAO (Comm. of Central Excise & Customs) Raipur
054700 - PAO (Commissionerate of Customs) New Dehi
054725 - PAO,CEX & Customs, NOIDA
054750 - PAO,CEX & Customs Calicut
054775 - PAO,CEX & Customs,Rohtak
054800 - PAO,CEX & Customs,Ghaziabad
054825 - PAO,CEX & Customs,Lucknow
054851 - PAO CEX KOLKATA-III
054876 - PAO(Central Excise & Customs), JAMSHEDPUR
054901 - PAO,C.EX, MANGALORE
054926 - PAO CBEC, TRIVANDRUM
054951 - PAO C.EX IV, KOLKATA
054975 - PAO CEX & CUSTOMS, NASIK
055005 - PAO, CEX & Customs CHANDIGARH
055055 - PAO,CEX & Customs Ludhiana
055105 - PAO,CEX & Customs Pondicherry
055140 - PAO,CEX & Customs Ranchi
055185 - PAO,CEX & Customs Siliguri
055210 - PAO,CEX & Customs Surat
055240 - PAO,CEX & Customs Tirupati
055275 - PAO,CEX & Customs Tirunelveli
055340 - PAO,CEX & Customs Salem
055370 - PAO,CEX & Customs Mysore
055405 - PAO,CEX & Customs Vapi
004163 - ZAO, CBDT, Bareily
004164 - ZAO, CBDT, Dehradun
004166 - ZAO, CBDT, Ludhiana
004167 - ZAO, CBDT, Shimla
004168 - ZAO, CBDT, Chandigarh
004169 - ZAO, CBDT, Panchkula
004170 - ZAO, CBDT, Udaipur
004171 - ZAO, CBDT, Jodhpur
004172 - ZAO, CBDT, Raipur
004173 - ZAO, CBDT, Indore

004174 - ZAO, CBDT, Coimbatore
004175 - ZAO, CBDT, Madurai
004176 - ZAO, CBDT, Trichi
004177 - ZAO, CBDT, Hubli
004178 - ZAO, CBDT, Trivandrum
004179 - ZAO, CBDT, Vishakapatnam
004180 - ZAO, CBDT, Nasik
004181 - ZAO, CBDT, Thane
004182 - ZAO, CBDT, Panaji
004183 - ZAO, CBDT, Baroda
004184 - ZAO, CBDT, Surat
004185 - ZAO, CBDT, Rajkot
004186 - ZAO, CBDT, Jalpaiguri
004187 - ZAO, CBDT, Durgapur
004189 - ZAO, CBDT, Bhagalpur
004190 - ZAO, CBDT, Ranchi
055461 - ZAO(CBDT), Pune
055500 - ZAO(CBDT)(Revenue), Pune
055542 - ZAO(CBDT), Bangalore
055570 - ZAO(CBDT)(Revenue), Bangalore
055623 - ZAO(CBDT), Patna
055650 - ZAO(CBDT)(Revenue), Patna
055703 - ZAO(CBDT), Bhopal
055730 - ZAO(CBDT)(Revenue), Bhopal
055784 - ZAO(CBDT), Patiala
055800 - ZAO(CBDT)(Revenue), Patiala
055862 - ZAO(CBDT), Nagpur
055880 - ZAO(CBDT)(Revenue), Nagpur
055940 - ZAO(CBDT), Kanpur
055960 - ZAO(CBDT)(Revenue), Kanpur
056017 - ZAO(CBDT), Ahmedabad
056050 - ZAO(CBDT)(Revenue), Ahmedabad
056099 - ZAO(CBDT), Jaipur
056130 - ZAO(CBDT)(Revenue), Jaipur
056180 - ZAO(CBDT), Bhubaneswar
056200 - ZAO(CBDT)(Revenue), Bhubaneswar
056260 - ZAO(CBDT), Lucknow
056280 - ZAO(CBDT)(Revenue), Lucknow
056418 - ZAO(CBDT), Amritsar

056435 - ZAO(CBDT)(Revenue), Amritsar
056496 - ZAO(CBDT), Meerut
056530 - ZAO(CBDT)(Revenue), Merrut
056576 - ZAO(CBDT), Hyderabad
056600 - ZAO(CBDT)(Revenue), Hyderabad
056658 - ZAO(CBDT), Allahabad
056680 - ZAO(CBDT)(Revenue), Allahabad
056737 - ZAO(CBDT), Jalandhar
056750 - ZAO(CBDT)(Revenue), Jalandhar
056815 - ZAO(CBDT), Agra
056830 - ZAO(CBDT)(Revenue), Agra
056892 - ZAO(CBDT), Rohtak (Haryana)
056910 - ZAO(CBDT)(Revenue), Rohtak
056971 - ZAO(CBDT), Kolkata
056990 - ZAO(CBDT)(Revenue), Kolkata
057050 - ZAO(CBDT), Mumbai
057075 - ZAO(CBDT)(Revenue), Mumbai
057127 - ZAO(CBDT), Chennai
057150 - ZAO(CBDT)(Revenue),Chennai
057208 - ZAO(CBDT), Cochin
057240 - ZAO(CBDT)(Revenue), Cochin
057288 - ZAO(CBDT), New Delhi
057315 - ZAO(CBDT)(Revenue), New Delhi
058296 - PAO(DST), New Delhi
058374 - CPAO(Survey of India), Dehradun
058490 - RPAO(Survey of India), Hyderabad
058606 - RPAO(Survey of India), Kolkata
058743 - RPAO(Survey of India), Jaipur
059161 - PAO(DSIR), New Delhi
059241 - PAO Bio-technology)
000996 - National Remote Sensing Centre
060175 - Head Accounts & IFA, VSSC
060256 - Head Accounts & IFA, SHAR
060334 - Head Accounts & IFA, SAC
060412 - PAO(Department of Space), Bangalore
060493 - Head Accounts& IFA,ISRO Satellite Centre
060570 - Accounts Officer-I ISRO Office,New Delhi
060647 - Head Accounts & IFA, PSLV
060700 - Accounts Officers I MCF

060803 - Head Accounts & IFA, LPSC
060880 - Accounts Officer-I, ISTRAC
060990 - Sr. Accounts Officer-II CED
061100 - Sr. Accounts Officer-II ISRO HQ
000357 - Pay & Accounts Office
001717 - Sr. Dy. Accountant General/ Dy. Accountant General
001918 - Director General of Audit, Defence Services
061808 - A.G. ANDHRA PRADESH, HYDERABAD
062044 - A.G.(A&E) JHARKHAND,RANCHI
062123 - AG II (Bihar), Patna
062201 - Pay and Accounts Office- (Audit), Mumbai. O/o The A.G.(A&E)-1 Maharashtra, Mumbai - 400020
062289 - A.G.(A&E), WEST BENGAL, KOLKAYTA
062335 - PAO, O/O AG (A&E), RAJASTHAN, JAIPUR
062376 - Office of the Accountant General (Audit) Delhi
062463 - A.G. (A&E) GUJARAT, RAJKOT
062541 - AG (HP & Chandigarh), Simla
062699 - PAO,AG(A&E),Kerala
062779 - o/o the Accountant General (A&E), Residency Park House Road, Karnataka, Bangalore-560 001
062859 - P.A.O. O/o.A.G.(A&E)I, Madhya Pradesh, Gwalior
062939 - PAO(AUDIT) O/O AG(A&E)-II MAHARASHTRA,NAGPUR
063171 - A.G. (A&E) ORISSA, BHUBNESHWAR
063252 - AG (Punjab), Chandigarh
063335 - A.G.(A&E) Rajasthan, Jaipur
063413 - PAY AND ACCOUNTS OFFICER (IAD), CHENNAI
063576 - A G Uttar Pradesh, Allahabad
063735 - A.G.Gujarat Ahmedabad
063811 - PAO (Defence Audit) Meerut Cantt
063821 - PAO, O/O THE A.G.CHHATTISGARH, RAIPUR
063830 - PAO/A.G. (A&E) Uttarakhand
070965 - A.G. Madhya Pradesh,Gwalior
071229 - A.G. Hariyana,Chandigarh
064815 - PAO LOK SABHA SECRETARIAT
065820 - PAO (Rajya Sabha)
010648 - PAO(Youth Affairs & Sports), New Delhi
011450 - PAO(Women & Child Development),New Delhi
011525 - PAO(WCD),Mumbai
011601 - PAO (WCD) Kolkata
011676 - PAO (WCD),Chennai

071207 - Directorate of A/Cs U.T. Daman & Diu, Daman
071220 - PAO, DIU
000666 - Designated Authority for AIS Pensioners
072539 - PrAO cum PAO(MNRE), New Delhi
073544 - PrAO cum PAO(External Affairs), N. Delhi
075020 - PAO(BSI/ZSI), Kolkata
075126 - PAO(Environment), New Delhi
075501 - PrAO_Cum_PAO(FPI) Delhi
000110 - PAO, IMD, M/o Earth Science, NEW DELHI
000111 - PAO, IMD, M/o Earth Science, KOLKATA
000112 - RPAO, IMD
000113 - PAO, IMD, M/o Earth Science, PUNE
075211 - PAO (Ocean Development) New Delhi
075305 - Sr. AO/Pay & Accounts Officer
075691 - Pr.A.O-cum-PAO, Chemical & Petrochemicals
075800 - PAO Bhopal
084001 - PAO(Election Commission)
086000 - PAO Corporate Affairs, New Delhi
086200 - PAO Corporate Affairs, Mumbai
086400 - PAO Corporate Affairs, Calcutta
086600 - PAO Corporate Affairs, Chennai
088100 - PAO (ALHW), New Delhi
088200 - PAO (Shipping), New Delhi
088300 - PAO (LHLS), Noida
088400 - PAO (Shipping), Mumbai
088500 - PAO (Shipping), Kolkata
089001 - PAO PANCHAYATI RAJ,KRISHI BHAWAN,NEW DELHI
026801 - PAO (Disinvestment)
091001 - PAO-CUM-PR. AO, MIN. OF OVERSEAS INDIAN AFFAIRS, NEW DELHI
092001 - PAO, MINISTRY OF MINORITY AFFAIRS, SHASTRI BAHWAN, NEW DELHI
005865 - PrAO-Cum-PAO (Petroleum),New Delhi
088000 - Pr.A.O.-cum-P.A.O., Shipping, New Delhi
055310 - PAO,CEX & Customs Tuticorin

13.3.2 List of remote PAOs

001753 - RPAO, BSF,JAMMU
001754 - RPAO, BSF, Shillong
001755 - RPAO, CRPF,Jammu

001759 - RPAO, ITBP,Shillong
002178 - PAO, CRPF 1
002179 - PAO, CRPF 2
002180 - PAO, CRPF 3
002181 - PAO, CRPF 4
002182 - PAO, CRPF 5
002183 - PAO, BSF 1
002184 - PAO, BSF 2
002185 - PAO, BSF 3
002186 - PAO, BSF 4
002187 - PAO, BSF 5
003237 - Pay & Accounts Office, SSB, Guwahati
023408 - RPAO(IB), Shillong
023498 - PAO(Assam Rifles), Shillong
028875 - PAO(Doordarshan), Guwahati.
034921 - RPAO(NH),Guwahati
037224 - PAO(GSI) N.E.Region,Shillong
043810 - PAO, CPWD, N.E. Zone, Shillong.
045375 - PAO(Heavy Water Plant), Talcher
050205 - PAO, CENTRAL EXCISE, DIBRUGARH
052512 - PAO(Collectorate of C&CE), Shillong
054432 - PAO(Collec.of Central Excise),Bolpur(WB)
004165 - ZAO, CBDT, Jammu
056339 - ZAO(CBDT), Shillong
056360 - ZAO(CBDT)(Revenue), Shillong
061887 - PAO, INDIAN AUDIT DEPARTMENT, PORT BLAIR
061964 - AG Assam,Mizoram,Arun. Pradesh,Shillong
063017 - Sr.D.A.G.(A&E) Manipur,Imphal
063094 - AG (Nagaland), Kohima
070703 - A.G. (A&E), Assam, Guwahati
071361 - Dir. of A/Cs & Budget, Andaman & Nicobar
085001 - PrPAO Accounts Office,Kavaratti,Lakhsdweep.
004188 - ZAO, CBDT, Guwahati
062621 - AG J&K SRINAGAR
063658 - O/o Sr DAG(A&E), Sikkim, Gangtok
071295 - A.G. MIZORAM
071383 - PAO(Andaman & Nicobar Island Admn.
071405 - PAO(Car Nicobar)
071427 - PAO(Rangat)

13.3.3 List of Tier 1 Cities

Following is the list of Tier 1 Cities which consists of Metro cities, state capitals (excluding Jammu & Kashmir, North Eastern states and Islands).

S. No	Name of the City	No of DDOs
1	New Delhi	992
2	Kolkata	421
3	Mumbai	342
4	Chennai	275
5	Bangalore	209
6	Hyderabad	195
7	Ahmadabad	127
8	Chandigarh	121
9	Jaipur	120
10	Lucknow	106
11	Nagpur	103
12	Patna	102
13	Pune	93
14	Bhubaneshwar	83
15	Bhopal	82
16	Vishakhapatnam	77
17	Kochi	76
18	Ranchi	75
19	Dehradun	72
20	Trivandrum	68
21	Raipur	63
22	Kanpur	53
23	Coimbatore	51
24	Allahabad	49
25	Vadodaraa	44
26	Indore	43
27	Surat	42
28	Shimla	40
29	Ghaziabad	38
30	Rajkot	34
31	Panaji	33
32	Amritsar	32
33	Gwalior	31
34	Agra	29
35	Faridabad	29
36	Noida	25
37	Mysore	24
38	Gandhi Nagar	18
39	Aurangabad	18
40	Gurgaon	16
41	Howrah	6
42	Puri	6
43	Secunderabad	5
44	Silvasa	5
45	Belapur	2
46	Bhayandar	2

S. No	Name of the City	No of DDOs
47	Cochin	2
48	Nava Sheva (Mumbai)	2
49	Tarapur	2
50	Vasai	2
51	Kharagpur	1
52	Mohali	1
	Total DDOs	**4487**

13.3.4 List of Tier 2 Cities

Cities which have fair connectivity options like presence of major Internet Service Providers and NICNET have been categorised as Tier 2 Cities These cities are also the district headquarters. The list of the Tier 2 Cities is as bellow:

S. No	Name of the City	No. of DDOs
1	Jodhpur	56
2	Jabalpur	33
3	Mangalore	33
4	Dhanbad	32
5	Madurai	29
6	Bareilly	28
7	Jalandhar	28
8	Ludhiana	28
9	Varanasi	27
10	Ajmer	26
11	Jamshedpur	24
12	Salem	24
13	Udaipur	24
14	Cuttack	23
15	Trichy	23
16	Hubli	22
17	Vijaywada	22
18	Durgapur	21
19	Daman	19
20	Meerut	19
21	Muzaffarpur	19
22	Bilaspur	18
23	Calicut	18
24	Hazaribagh	18
25	Nasik	18
26	Jalpaiguri	16
27	Bikaner	15
28	Gorakhpur	15
29	Bhagalpur	14
30	Darjeeling	14
31	Patiala	14
32	Jamnagar	13
33	Tirupathi	13
34	Bhavnagar	12

S. No	Name of the City	No. of DDOs
35	Tiruchirapalli	12
36	Hissar	11
37	Karnal	11
38	Panchkula	11
39	Rohtak	11
40	Belgaum	10
41	Bhilai	10
42	Jaisalmer	10
43	Kalyan	10
44	Erode	9
45	Nasik Road	9
46	Panipat	9
47	Sambalpur	9
48	Kottayam	8
49	Almora	7
50	Ambala	7
51	Bokaro	7
52	Kandla	7
53	Kolhapur	7
54	Nellore	7
55	Rourkela	7
56	Solan	7
57	Thrissur	7
58	Ernakulam	6
59	Kozhikode	6
60	Palakkad	6
61	Akola	5
62	Aligarh	5
63	Anand	6
64	Chittorgarh	5
65	Gaya	5
66	Hooghaly	5
67	Marmago	5
68	Alleppey	4
69	Alwar	4
70	Amravati	4
71	Ankleshwar	4
72	Bharuch	4
73	Haridwar	4
74	Kalpakkam	4
75	Madgaon	4
76	Porebandar	4
77	Saharanpur	4
78	Sonepat	4
79	Etawah	3
80	Kutch	3
81	Mandi	3
82	Muzaffarnagarr	3
83	Rishikesh	3
84	Vasco	3
85	Ahmednagar	2

S. No	Name of the City	No. of DDOs
86	Ambala Cantt	2
87	Avadi	2
88	Darbhanga	2
89	Dharwad	2
90	Gautam Buddh Nagar	2
91	Goa	2
92	Hamirpur	2
93	Kancheepuram	2
94	Kurukehetra	2
95	Margoa	2
96	Mathura	2
97	Nainital	2
98	Roorkee	2
99	Satara	2
100	Thanjavur	2
101	Tiruchi	2
102	Ujjain	2
103	Vaishali	2
104	Vellore	2
105	Warangal	2
106	Yamuna Nagar	2
107	Ajanta	1
108	Avadi Chennai	1
109	Biharsharif	1
110	Bolangir	1
111	Dalhousie	2
112	Dharamshala	1
113	Durg	1
114	Dwarka	1
115	Khalgaon	1
116	Laharia Saria	1
117	Merrut	1
118	Mussoorie	1
119	Nalanda	1
120	New Jalpaiguri	1
121	Palghar	1
122	Pinjore	1
123	Rajgir	1
124	Tanjore	1
125	Tiruvarur	1
126	Udupi	1
127	Vallore	1
	Total Locations	1143

13.3.5 List of Tier 3 Cities

Cities and Towns which have limited connectivity options and are located at district headquarters have been classified as Tier 3 Cities. The list of cities is as below:

S. No	Name of the City	No of DDOs
1	Diu	47
2	Moti Daman	42
3	Siliguri	39
4	Murshidabad	21
5	Guntur	20
6	Neemuch	18
7	Nani Daman	17
8	Pondicherry	17
9	Bhuj	16
10	Moradabad	15
11	Tuticorin	15
12	Asansol	14
13	Berhampur	12
14	Cooch Behar	12
15	Barmer	9
16	Bhatinda	9
17	Jadgalpur	9
18	Kullu	9
19	Malda	9
20	Sriganganagar	9
21	East Godavari District	8
22	Koraput	8
23	Paradeep	8
24	Shivpuri	8
25	Tirunelveli	8
26	Ferozpur	7
27	Pithoragarh	7
28	Rajahmundry	7
29	Rampur	7
30	Trichur	7
31	Vapi	7
32	Bahraich	6
33	Bellary	6
34	Dewas	6
35	Haldwani	6
36	Kannur	6
37	Keonjhar	6
38	Mandsaur	6
39	Suratgarh	6
40	Valsad	6
41	Begusarai	5
42	Kakinada	5
43	Kishanganj	5
44	Kollam	5
45	Nadia	5
46	Nanded	5
47	Ropar	5
48	West Godavari District	5
49	Ananthapur	4

50	Angul	4
51	Balasore	4
52	Balurghat	4
53	Barauni	4
54	Burdwan	4
55	Chandrapur	4
56	Cuddalore	4
57	Deoli	4
58	Dhenkanal	4
59	Faizabad	4
60	Ganjam	4
61	Gurdaspur	4
62	Kangra	4
63	Mehsana	4
64	Nagaur	4
65	Pilibhit	4
66	Rae Bareli	4
67	Sitamarhi	4
68	Balrampur	3
69	Bankura	3
70	Barabanki	3
71	Barwaha	3
72	Bhandara	3
73	Bhilwara	3
74	Bolpur	3
75	Chindwara	3
76	Deoghar	3
77	Dindigul	3
78	Faridkot	3
79	Gandhidham	3
80	Ghazipur	3
81	Giridhi	3
82	Gulberga	3
83	Haldia	3
84	Hanumangarh	3
85	Hassan	3
86	Hoshangabad	3
87	Hoshiarpur	3
88	Jalore	3
89	Jhansi	3
90	Kadamtala	3
91	Kalyani	3
92	Khandwa	3
93	Lakhimpur	3
94	Mirzapur	3
95	Motihari	3
96	Mount Abu	3
97	Nadiad	3
98	Nagapattinam	3
99	Nagercoil	3
100	Navasari	3
101	Panchkula	3
102	Pathankot	3
103	Pollachi	3

104	Raigarh	3
105	Rajnandgaon	3
106	Ramanathapuram	3
107	Rangareddy	3
108	Ratlam	3
109	Ratnagiri	3
110	Rewa	3
111	Rewari	3
112	Sagar	3
113	Satna	3
114	Sirohi	3
115	Sitapur	3
116	Srikakulam Distt	3
117	Tharad	3
118	Tiruppur	3
119	Tiruvalla	3
120	Una	3
121	Villupuram	3
122	Virudhnagar	3
123	Abhohar	2
124	Amalapuram	2
125	Amerli	2
126	Anakapali	2
127	Arakkonam	2
128	Badaun	2
129	Balotra	2
130	Banswara	2
131	Baragarh	2
132	Barbil	2
133	Bargarh	2
134	Basantpur	2
135	Bathnaha	2
136	Beawar	2
137	Behrampur	2
138	Betul	2
139	Bhadrak	2
140	Bhawanipatna	2
141	Bhemavaram	2
142	Bhinga	2
143	Bhiwani	2
144	Bijnaur	2
145	Birpur	2
146	Bolani	2
147	Bundi	2
148	Cannanore	2
149	Champaran	2
150	Chandaushi	2
151	Chitradurga	2
152	Chittoor	2
153	Churu	2
154	Cuddapah	2
155	Daltonganj	2
156	Damanjodi	2

157	Damoh	2
158	Dantewara	2
159	Dantiwada	2
160	Davangere	2
161	Dhamtari	2
162	Dhar	2
163	Dhule	2
164	Eluru	2
165	Etah	2
166	Ettumanur	2
167	Falakata	2
168	Farakka	2
169	Farrukhabad	2
170	Forbesganj	2
171	Gadag	2
172	Garhwal	2
173	Godhara	2
174	Gonda	2
175	Gudivada	2
176	Gudur	2
177	Hapur	2
178	Hardoi	2
179	Hosur	2
180	Humma	2
181	Itarsi	2
182	Jagraon	2
183	Jajpur	2
184	Jalgaon	2
185	Jalna	2
186	Jaynagar	2
187	Jhalawar	2
188	Joshimath	2
189	Junagadh	2
190	Kannauj	2
191	Karaikudi	2
192	Karur	2
193	Karwar	2
194	Katihar	2
195	Khajuraho	2
196	Khammam	2
197	Khanna	2
198	Khargone	2
199	Khurda	2
200	Kishangarh	2
201	Korba	2
202	Kotdwar	2
203	Krishnanagar	2
204	Kumbakonam	2
205	Kurnool	2
206	Lakhimpur Kheri	2
207	Lalitpur	2
208	Latur	2
209	Machilipatnam	2

210	Madhopur	2
211	Madhubani	2
212	Makrana	2
213	Malegaon	2
214	Malerkotla	2
215	Mayurbhanj	2
216	Midnapore	2
217	Moga	2
218	Mokamaghat	2
219	Morbi	2
220	Mundali	2
221	Munger	2
222	Nahan	2
223	Nalgonda	2
224	Namakkal	2
225	Nangal	2
226	Nazibabad	2
227	Nilgiris	2
228	Ongole	2
229	Ooty	2
230	Palampur	2
231	Pali	2
232	Pallipuram	2
233	Panjipara	2
234	Parwanoo	2
235	Petlad	2
236	Phagwara	2
237	Phulbani	2
238	Pudukottai	2
239	Purnea	2
240	Purulia	2
241	Raiganj	2
242	Rayagada	2
243	Raygada	2
244	Roodrapur	2
245	Sahajahanpur	2
246	Saharsa	2
247	Sahibganj	2
248	Sambhal	2
249	Sangli	2
250	Sangrur	2
251	Singur	2
252	Sivkasi	2
253	Solapur	2
254	Srinagar	2
255	Sumerpur	2
256	Talchar	2
257	Tanuku	2
258	Theni	2
259	Uttarkashi	2
260	Valmiki Nagar	2
261	Veraval	2
262	Vidisha	2

263	Vijaipur	2
264	Wardha	2
265	Aluva	1
266	24 Paragnas North	1
267	24-Paraganas (South)	1
268	Abdul Hameed Street	1
269	Adilabad	1
270	Adipur	1
271	Adoni	1
272	Ajnala	1
273	Alipurduar	1
274	Alwaye	1
275	Ambikapur	1
276	Andesh Nagar	1
277	Anpara	1
278	Ara	1
279	Araria District	1
280	Aswapuram	1
281	Atrai (Patiram)	1
282	Azamgarh	1
283	Bacheli	1
284	Bagpat	1
285	Balaghat	1
286	Ballia	1
287	Balmikinagar	1
288	Banda	1
289	Baptala	1
290	Barajamda	1
291	Baran	1
292	Barasat	1
293	Barnala	1
294	Barsingsar	1
295	Basti	1
296	Batala	1
297	Beed	1
298	Bellampalli	1
299	Betia	1
300	Bettuah	1
301	Bhadohi	1
302	Bhikiwind	1
303	Bhrhanpur	1
304	Bidar	1
305	Bijapur	1
306	Birbhum	1
307	Bogda	1
308	Bongaigaon	1
309	Boshair	1
310	Budni	1
311	Bulandhshahar	1
312	Buniadpur	1
313	Burnpur	1
314	Buthanpur	1
315	Chaibasa	1

316	Chakur/ Latur	1
317	Chamera	1
318	Chamoli	1
319	Chapra	1
320	Chhattarpur	1
321	Chirawa	1
322	Chitpur	1
323	Coonoor	1
324	Dadri	1
325	Dahod	1
326	Dasuya	1
327	Deoria	1
328	Dera Bassi	1
329	Derbabananak	1
330	Devengre	1
331	Dhori	1
332	Dhrangadhra	1
333	Dinajpur	1
334	Dinhata	1
335	Distt-Nadia	1
336	Doasa	1
337	Elango Nagar	1
338	Fatehabad	1
339	Fatehgarh	1
340	Fatehpur	1
341	Fazilka	1
342	Ferozabad	1
343	Fort Bellary	1
344	Ganganagar	1
345	Gobindgarh	1
346	Godak	1
347	Gomia	1
348	Gondkhari	1
349	Gorakhpur	1
350	Guna	1
351	Guntakal	1
352	Guruvayur	1
353	Gwaldom	1
354	Hathras	1
355	Haveri	1
356	Hazira	1
357	Hindpur	1
358	Hospet	1
359	Humhara	1
360	Hussainganj	1
361	Jagdeo	1
362	Jalaun	1
363	Jaunpur	1
364	Jgadhari	1
365	Jhanor	1
366	Jind	1
367	Junagarh	1
368	Kaiga	1

369	Kaithal	1
370	Kakarpara	1
371	Kakindada	1
372	Kalimpong	1
373	Kalol	1
374	Kapurthala	1
375	Karera Shivpuri	1
376	Karian	1
377	Kariganur	1
378	Karimnagar	1
379	Karma	1
380	Kasargod	1
381	Kasauli	1
382	Kashipur	1
383	Kasimpur	1
384	Kathel	1
385	Katni	1
386	Kawas	1
387	Khamgaon	1
388	Khatima	1
389	Khemkaran	1
390	Kheri	1
391	Khetri Nagar	1
392	Kinnour	1
393	Kolar	1
394	Koratty	1
395	Kothagudem	1
396	Kovilpatti	1
397	Krishangarh	1
398	Krishangiri	2
399	Kudal	1
400	Kudrmukh	1
401	Kumarse	1
402	Kundali	1
403	Kundankulam	1
404	Kunti	1
405	Kushinagar	1
406	Lalpania	1
407	Madanapalli	1
408	Mahabaleshwar	1
409	Mahidananda	1
410	Mainpuri	1
411	Malappuram	1
412	Mancherial	1
413	Mandya	1
414	Mannath Bhanjan	1
415	Mansa	1
416	Mau	1
417	Meghathburu	1
418	Mehboob Nagar	1
419	Mejia	1
420	Miraj	1
421	Mirthi	1

422	Muktsar	1
423	Muvattupuzha	1
424	Nabha	1
425	Nagacoil	1
426	Nakodar	1
427	Nandyal	1
428	Narasaraopet	1
429	Narayanpur	1
430	Narnaul	1
431	Narora	1
432	Naupada	1
433	Nawanshahar	1
434	Naya Nangal	1
435	Nazira	1
436	Neemkathan	1
437	Neyveli	1
438	Nilokheri	1
439	Nizamabad	1
440	North Kanara	1
441	Obra	1
442	Palakol	1
443	Palanpur	1
444	Panampur	1
445	Panchamahal	1
446	Panchet	1
447	Panki	1
448	Parbhani	1
449	Parichha	1
450	Penuguduru	1
451	Phalodi	1
452	Piprakothi	1
453	Pipri	1
454	Polkhar	1
455	Pratapgarh	1
456	Proddatur	1
457	Puttur	1
458	Quilon	1
459	Raichur	1
460	Raigunj	1
461	Raisen	1
462	Rajapalayam	1
463	Rajpura	1
464	Rajsamand	1
465	Ramagundam	1
466	Ramanathapur	1
467	Ramgarh	1
468	Ramgarh Cantt	1
469	Ramgarhwa	1
470	Rampur, Busar	1
471	Ranaghat	1
472	Ranidanga	1
473	Raniganj	1
474	Ratangarh	1

475	Raxaul	1
476	Rekongpeo	1
477	Rengareddy	1
478	Rihandnagar	1
479	Roop Nagar	1
480	Salboni	1
481	Samastipur	1
482	Sasaram	1
483	Sawaimadhopur	1
484	Seemanagara	1
485	Seoni	1
486	Shahdol	1
487	Shajapur	1
488	Shaktinagar	1
489	Shamli	1
490	Sheetalpur	1
491	Shimoga	1
492	Sholapur	1
493	Siddipet	1
494	Sindri	1
495	Sirhind	1
496	Sirsa	1
497	Sirsi	1
498	Sivaganga	1
499	Siwan	1
500	Solbani	1
501	Sriharikota	1
502	Sukanta Park	1
503	Sultanpur	1
504	Sunam	1
505	Sundernagar	1
506	Surangani	1
507	Suri	1
508	Suryapet	1
509	Tadepalligudem	1
510	Tanakpur	1
511	Tanda	1
512	Tarantaran	1
513	Tekanpur	1
514	Tenali	1
515	Thiruvanmiyar	1
516	Thumba	1
517	Tirumanichengalpattu	1
518	Tirur	1
519	Tumkur	1
520	Tuni	1
521	Udham Singh Nagar	1
522	Udyogmondal	1
523	Ukai	1
524	Umargaon	1
525	Unchahar	1
526	Unnao	1
527	Uran	1

528	Us Nagar	1
529	Uttrakhand	1
530	Vellur	1
531	Viarabad	1
532	Vindhyanagar	1
533	West Champaran	1
534	West Singhbhum	1
535	Yavatmal	1
	Total	**1337**

13.3.6 List of Remote Locations:

Cities in North Easters States (Assam, Manipur, Meghalaya, Tripura, Nagaland, Arunachal Pradesh, Mizoram, Sikkim), Jammu & Kashmir, Lakshadweep and Andaman & Nikobar Islands have been classified as remote locations. The list is as below:

S. No	Name of the City	No of DDOs
1	Guwahati	136
2	Port Blair	96
3	Shillong	83
4	Jammu	62
5	Kavaratti	53
6	Srinagar	45
7	Agartala	36
8	Imphal	27
9	Dibrugarh	25
10	Mayabunder	25
11	Silchar	24
12	Gangtok	22
13	Great Nicobar	20
14	Car Nicobar	19
15	Rangat	19
16	Jorhat	17
17	Diglipur	16
18	Itanagar	16
19	Aizawal	15
20	Kohima	14
21	Amini	11
22	Androth	11
23	Dimapur	10
24	Agatti	9
25	Bongaigaon	9
26	Hut Bay	9
27	Kadmath	9
28	Leh	9
29	Kalpeni	8
30	Minicoy	8
31	Tezpur	7
32	Udhampur	7
33	Anantnag	6
34	Baramulla	6
35	Dhubri	6
36	Kiltan	6
37	Wimberligunj	6
38	Chetlat	5
39	Andaman	4
40	Campbell Bay	4
41	Tura	4
42	Bantalab	3
43	Baratang	3
44	Chatham	3
45	Chieswema	3

S. No	Name of the City	No of DDOs
46	Digboi	3
47	Dolly Gunj	3
48	Duliajan	3
49	K.M. Samba	3
50	Kamorta	3
51	Kokrajhar	3
52	Little Andaman	3
53	Poonch	3
54	Prothrapur	3
55	Rajouri	3
56	Salonibari	3
57	South Andaman	3
58	Sunderbani	3
59	Tinsukia	3
60	Tuensang	3
61	Bagafa	2
62	Cachar	2
63	Chandel	2
64	Churachandpur	2
65	Doda	2
66	Joupi	2
67	Kamrup	2
68	Karimganj	2
69	Kathua	2
70	Khatkhati	2
71	Kimin	2
72	Lohitpur	2
73	Mantripokhri	2
74	Maram	2
75	Mohouchin	2
76	Rangia	2
77	Samsai	2
78	Sivasagar	2
79	South Andaman District	2
80	Tawi	2
81	Tejpur	2
82	Teju	2
83	Teliamura	2
84	Thinghat	2
85	Wokha	2
86	Akhnoor	1
87	Alamganj	1
88	Along (Ne)	1
89	Andaman Distt	1
90	Araimile	1
91	Bamdila	1
92	Bandipur	1
93	Bishalgarh	1
94	Bishenpur	1
95	Burnihut	1

S. No	Name of the City	No of DDOs
96	Changlang	1
97	Charduar	1
98	Chassad	1
99	Chirang	1
100	Cooch Behar	1
101	Darrang	1
102	Dhalai	1
103	Dharmangar	1
104	Diphu	1
105	Dirang	1
106	East Sikkim	1
107	Garo Hill	1
108	Golaghat	1
109	Gsaspani	1
110	Gulaghat	1
111	Havelock Island	1
112	Howley	1
113	Imphal West	1
114	Indershwar Nagar	1
115	Jairampur	1
116	Juotipuram	1
117	Kakching	1
118	Kamrup Metro	1
119	Kashmir	1
120	Kethalmambi	1
121	Kishtwar	1
122	Krishnanagar	1
123	Kupwara	1
124	Lakhimpur	1
125	Lekhapani	1
126	Lokra	1
127	Lunglei	1
128	Magaladoi	1
129	Mahidananda	1
130	Manipur	1
131	Maralia	1
132	Medziphema Campus	1
133	Mizoram	1
134	Moreh	1
135	Naharlagun	1
136	Nalbari	1
137	Nazira	1
138	Nonei	1
139	Nowgaon	1
140	Numaligarh	1
141	Pani Sagar	1
142	Parbung	1
143	Paren	1
144	Phek	1

S. No	Name of the City	No of DDOs
145	Port Mout	1
146	Pulwama	1
147	Radhanagar	1
148	Ramban	1
149	Salakati	1
150	Salal Jyotipuram	1
151	Salbagan	1
152	Sangshak	1
153	Satwari Cantt	1
154	Sehlon	1
155	Serchip	1
156	Shajiktampak	1
157	Shangshak	1
158	Shibsagar	1
159	Shokuvi	1
160	Sibsagarh	1
161	Sobansari	1
162	Sonitpur	1
163	Tamenglong	1
164	Tanglutal	1
165	Tawang	1
166	Thoubal	1
167	Udaipur	1
168	Udalguri	1
169	Uri	1
170	West Garo Hills	1
171	Yuksam	1
172	Zunheboto	1
	Total	**1120**

13.4 SLA Template for Data Centre

Section 1: Technology and Performance SLA Criteria

The Implementing Agency shall exhibit the capability to handle the criteria as per the stated metrics below. Only after the listed Technology and Performance criteria are met, the Implementing Agency will be allowed to roll-out the application across the PAOs and DDOs. Once the Pilot phase is over, the Implementing Agency is expected to keep the Technology and Performance levels above the specified level, so as to meet the operations SLA, as defined in this Section. Operations SLA are designed to monitor the performance of the Implementing Agency in delivering the service sought by the CGA. Penalties, unless explicitly mentioned in the remarks section of the particular SLA, would be deducted from the Quarterly Guaranteed Revenue (QGR). If the Implementing Agency performs as per the baseline metrics, then 100% of the QGR will be paid to the Implementing Agency as per Section 2: Terms of payment.

Operations SLA Criteria

SNo	Service Level Parameter	Baseline		Lower Performance		Breach		Basis of Measurement/ Remarks
		Metric	Deduction	Metric	Deduction	Metric	Deduction	
Server Performance based SLAs – The baseline metric mentioned under this category has to be met while delivering baseline metric for application performance as mentioned under the application performance category of this section. Any SLA deviation resulting from additional volumes of transactions over the server beyond the transaction volume baseline metrics would not be considered as a breach.								
1	Concurrent Session connections at Web Server / Application Server							
	Internet users (e.g. Public, etc)	5000	0	2000-4999	-2	< 2000	-5	The measurement would be done in two scales, namely, 1. Simulated – Simulation would be performed at two stages – a. Once prior to deployment at the user acceptance stage using load/stress testing tools b. Periodically during the production phase at non-office hours using simulation tools such as load/stress testing tools. 2. Real-time – The statistics calculated using EMS tools on server performance at any given point of time of a 24 X 7 window. This check would be performed constantly, to identify any
	Intranet users (e.g. PAOs, DDOs, etc)	15000	0	12000-14999	-2	<12000	-5	
2	Concurrent Users at Web Server / Application Server							
	Internet users with <	5000	0	3000-4999	-2	<3000	-5	

SNo	Service Level Parameter	Baseline		Lower Performance		Breach		Basis of Measurement/ Remarks
		Metric	Deduction	Metric	Deduction	Metric	Deduction	
	70% System Utilization (including CPU & Memory)							deviations, and in case of deviations noticed, it shall be escalated immediately to the Chief Technology Officer. The measurement would be on the basis of simultaneous recording by EMS, of a non-availability of service and the performance metric. In case a denial of service is detected while the performance metric is below the baseline, penalties would be levied.
	Intranet users with < 70% System Utilization (including CPU & Memory	10000	0	8000-9999	-2	<8000	-5	
3	Concurrent users at Database Server with < 70% System Utilization (including CPU & memory).	10000	0	8000-9999	-2	<8000	-5	

SNo	Service Level Parameter	Baseline		Lower Performance		Breach		Basis of Measurement/ Remarks
		Metric	Deduction	Metric	Deduction	Metric	Deduction	
Application Performance based SLAs – The baseline metric mentioned under this category has to be met while delivering baseline metric of the server performance as mentioned under the server performance category of this section. Any SLA deviation, resulting from an additional load over the server beyond the server performance baseline metrics would not be considered as a breach. A transaction would be considered as a set of activity involving application server / web server and database server resulting in validation of data at the application / web server and insertion of the validated data into the database at database server. For simulation, the size of data would be considered as 10 fields (a mixture of numeric, alphabet and date) with each field consisting of data of at least 15 bytes in length.								
4	IGFMS Portal page loading time, with a transaction volume of 5000 or more number of transactions performed per minute over the Internet based application software without any deadlocks and contentions taking place over	< 7	0	8-15 sec	-2	>15	-5	The portal page loading time would be monitored on a periodic basis by accessing it from the data centre. The portal page loading time would also be routinely measured over a leased circuit or equivalent at a minimum 128 Kbps bandwidth shared between 2 users. All portal pages would be tested for performance and an average of the total time taken, calculated by dividing the sum total of response times for all pages by the number of pages requested, would be considered for this SLA. It would be the responsibility of the Implementing Agency to ensure that either the size of the file or the time taken to query databases or time taken to perform complex business operations does not affect the response time.

SNo	Service Level Parameter	Baseline		Lower Performance		Breach		Basis of Measurement/ Remarks
		Metric	Deduction	Metric	Deduction	Metric	Deduction	
	application / web server or database server resources and with < 70% System Utilization (including CPU & memory).							
5	Average response time while using Intranet application for PAO, DDO users, with a transaction volume of 7500 or more number of transactions performed per minute	<5 sec	0	6-10 Sec	-2	>10 Sec	-5	Response time at all PAOs, DDOs, for the time window of office working hours, for Intranet based IGFMS application would be monitored using application performance measurement tools (part of EMS). The average response time would be calculated by dividing the total response time, for all requests summed together, by the number of requests made to the application system. It would be the responsibility of the Implementing Agency to ensure that either the size of the file or the time taken to query databases or time taken to perform complex business operations does not affect the response time

SNo	Service Level Parameter	Baseline		Lower Performance		Breach		Basis of Measurement/ Remarks
		Metric	Deduction	Metric	Deduction	Metric	Deduction	
	over the Intranet based application software without any deadlocks and contentions taking place over application / web server or database server resources and with < 70% System Utilization (including CPU & memory).							
6	Time required for generating non-OLAP reports, containing <	< 10 sec	0	11-18 Sec	-3	>18 Sec	9	The simulated queries would be executed on a periodic basis by accessing the reporting application from the data centre and the time thus generated would be used to calculate the SLA.

SNo	Service Level Parameter	Baseline		Lower Performance		Breach		Basis of Measurement/ Remarks
		Metric	Deduction	Metric	Deduction	Metric	Deduction	
	1000 records in the response, from OLTP database and with < 70% System Utilization (including CPU & memory).							

SNo	Service Level Parameter	Baseline		Lower Performance		Breach		Basis of Measurement/ Remarks
		Metric	Deduction	Metric	Deduction	Metric	Deduction	
7	The number of bugs reported within the application software.	< 20	0	21-30	-4	>30	-8	Bugs will be considered as faults located within the application software because of its inability to meet functional, non-functional, technical and operational requirements. Similarly the failure of the application to enforce basic validations over data resulting in capturing of wrong data values or resulting in erroneous performance of the application software would also be considered as bugs. Bugs will be measured on the basis of feedback received at the helpdesk about the application software. The time window used to measuring the bugs would be divided into two sections – 1. Go-Live to first 6 months 2. Every 9 months thereafter till the end of second year after go-live. 3. Every 18 months thereafter till end of the project.
Operational Parameters								

SNo	Service Level Parameter	Baseline		Lower Performance		Breach		Basis of Measurement/ Remarks
		Metric	Deduction	Metric	Deduction	Metric	Deduction	
8	Deployment of patches, hot fixes over COTS solutions (OS, EMS, AV, etc) and virus definition files over anti-virus solutions both at system level as well as network level, within a defined period	Within 1 business day	0	2-5 business days -2	-2	> 5 business days	-5	Measured using version management and patch management tools as well as EMS.
9	Availability of IGFMS Services at the Data Centre (IGFMS Application Software)							The availability of IGFMS services would include both Internet based and Intranet based application software services. Measured using the EMS tool, the non-availability would be considered as non-accessibility of the services by the EMS. Non-availability of any of the services would amount to deviation.

SNo	Service Level Parameter		Baseline		Lower Performance		Breach		Basis of Measurement/ Remarks
			Metric	Deduction	Metric	Deduction	Metric	Deduction	
	Working hours	1st April to 24th March	<= 6 hours per quarter	0	>6 hours per quarter	-2	>=10 hours per quarter	-5	The working hours would be the hours falling between 9 AM to 6 PM from Monday to Saturday. For March the Working hours would be 8 AM to 8 PM, excluding the last working day of the month when it would be 8 AM to 12 AM.
		25th March to 31st March	<= 30 minutes	0	>30 minutes	-10	>=2 hour	Base -20 with an increase of 1% for every hour of downtime beyond 2 hours	
	Non Working Hours		<= 15 hours per quarter	0	0 >15 hours per quarter	-2	2 >=24 hours per quarter	-5	The non-working hours would be the hours falling between today's 6 PM and tomorrow's 9 AM during Weekdays (Monday to Saturday) and Saturday's 6 PM to Monday's 9 PM during Weekends. For the month of March it would be adjusted based upon the designated working hours i.e. all hours not falling within the working hour bracket would be clubbed as non-working hours.
10	Availability of the Security		100	0	97-99.99%	-2	<97%	-5	Measured using EMS in a window of 24x365 days.

SNo	Service Level Parameter	Baseline		Lower Performance		Breach		Basis of Measurement/ Remarks
		Metric	Deduction	Metric	Deduction	Metric	Deduction	
	solution at the Data centre (firewall, IPS, Endpoint data protection, anti-virus, gateway level protection systems, etc)							
11	Adequacy of Training	>70% satisfaction index	0	60-70% satisfaction index	-5	<60% satisfaction index	-10	Satisfaction levels measured through feedback questionnaires circulated to Trainees (To be finalised by O/o CGA and Chief Technology Officer, IGFMS project). Such questionnaires would contain questions on various aspects of the training program and would capture various denominations of Trainee feedback. The deductions would be applicable over the Training Cost quoted by the bidder in the commercial proposal.
12	Average issue resolution time for problems recorded at helpdesk.							Measured through Helpdesk tools and APM

SNo	Service Level Parameter	Baseline		Lower Performance		Breach		Basis of Measurement/ Remarks
		Metric	Deduction	Metric	Deduction	Metric	Deduction	
	Problems related with the Application Software (both Internet and Intranet versions) and any of its module	<4 Hours	0	4-6 Hours	-1	>6 hours	-2	(Application Performance Monitoring) tool.
	Problems related with the Local Infrastructure at DC & DR / BCP.	< 2 business Hours	0	2-5 business hours	-1	>5 business hours	-2	
	Problems related with the Local Infrastructure at PAOs.	< 12 business Hours	0	12-15 business hours	-1	>15 business hours	-2	
	Problems related with the Local Infrastructure at State/ District	< 4 business Hours	0	4-6 Business hours	-1	>6 business hours	-2	

SNo	Service Level Parameter	Baseline		Lower Performance		Breach		Basis of Measurement/ Remarks
		Metric	Deduction	Metric	Deduction	Metric	Deduction	
	PAO/ DDOs.							
	Problems related to user understanding of the IGFMS system.	< 2 business hours	0	2-4 business hours	-1	> 4 business hours	-2	
13	Frequency of reoccurrence of problems of same nature.	Less than 10% of the number of equipments of the category deployed across all locations per quarter	0	More than 10% & less than 15% of the number of equipments of the category deployed across all locations per quarter	-2	More than 15% of the number of equipments of the category deployed across all locations per quarter	-5	The problems would be categorized on the basis the following categories of devices – a. Hardware – Servers, PCs and other related peripheral devices. b. Printers – Dot Matrix. c. LAN – Switches and Routers. d. COTS Software – Anti-Virus, End Point Data Protection, OS, etc. Helpdesk should make provision for giving such reports which would project a location and the number of problems, from the above categories, received in a quarter.

SNo	Service Level Parameter	Baseline		Lower Performance		Breach		Basis of Measurement/ Remarks
		Metric	Deduction	Metric	Deduction	Metric	Deduction	
14	Implementation of CCN (Change control note)	As per agreed timeline	0	Delay of more than 15 working days from agreed timeline	-2	Delay of more than 30 working days from agreed timeline	-5	The deductions would be calculated over the total cost quoted by the Implementing Agency for implementing the CCN. The agreed timelines would be documented as part of the CCN and deviations would be measured from there itself.

The penalties shall be levied only for the reasons attributable to the Implementing Agency. Any risks/issues foreseen by the Implementing Agency shall be brought to the notice of O/o CGA immediately. If no such issues/risks are highlighted by the Implementing Agency, then it is expected that no delays are there in the implementation schedule. However, if the Implementing Agency falters in one or more of the SLA resulting in lower performance or breach, then deduction in the QGR pay-out to the Implementing Agency is calculated as follows:

For baseline performance by Implementing Agency no deduction is made from the QGR. For Lower performance and Breach, deductions in percentages to be made from the QGR are shown in the Table. For example, during a month, if the application was available for 98% of the time and critical faults were resolved in 6 hours time, then a deduction of 8% (5+3) of the QGR is made, and the Implementing Agency will be paid 92%, assuming all other SLA terms are met. The total amount of penalties levied at any quarter would not exceed 25% of the QGR payable to the Implementing Agency for that quarter. However, this does not include penalties which can be levied for those items which are outside the regular QGR payments e.g. implementation of CCN.

The aforementioned SLA parameters shall be measured on a daily/weekly/monthly/quarterly basis (average) as per the individual SLA parameter requirements. However, if the performance of the solution/services is degraded significantly (operating at levels of breach for any SLA for a period of 24 Hrs or more) at any given point in time during the contract and if the immediate measures are not implemented and issues are not rectified to the satisfactory levels of O/o CGA, it will have the right to take appropriate disciplinary action including terminate the contract. It is to be noted that in case the overall penalty applicable for any of the quarters during the contract period touches 25% for three consecutive quarters; then the cap of 25% of QGR over the penalty levied for any quarter would fail to exist, from fourth quarter onwards, resulting in full penalties, as applicable after calculating the breaches, getting levied. In such a scenario O/o CGA may also exercise the right to terminate the contract. Following highlights the definition of "High", "Medium" and "Low" categories as used for O&M/Helpdesk SLAs above.

Note 1 Scheduled maintenance time will be excluded from the computation.

Note 2 Scheduled maintenance time shall not exceed 4 hours in a calendar month

Note 3 Planned Maintenance shall be scheduled between 10 pm and 2 am IST on the intervening night of Second Saturday and Sunday.

Note 4 Scheduled maintenance period(s) shall be planned and published for six months at a time and in the event of any changes to this plan, the same shall be notified at least 3 days in advance of the Schedule.

Note 5 The Helpdesk management system developed and deployed by the Implementing Agency shall be used for monitoring the issue resolution timelines and Implementing Agency shall be responsible for building such functionality into the Helpdesk management solution deployed for IGFMS.

Note 6 Helpdesk tool shall be available 24x365 wherein the users of IGFMS (Internal and External can log the calls through SMS/Portal/email).

Note 7 Business Hours: The hours falling within a working day. Hours: The hours falling within a calendar day.

Section 2: Terms of Payment

1 The adherence to the SLA's would be computed by the Enterprise Management System (EMS) tool implemented by the SI for this purpose. The credits and debits shall be calculated and the total gross amount of QGR would be arrived at after deducting penalties if any

2 Upon reception of the claim by the Chief Technology Officer, IGFMS Project, 75% of the QGR would be paid to the Implementing Agency within 15 working days, subject to the submission of all operational reports. The rest 25% of the QGR would be paid after the evaluation of performance against both the deployment and operational SLA's in respect of that month and after deducting penalties if any. The net QGR will be arrived at after deducting the penalties for lower performance and breaches. The net amount so arrived at would be paid to the System Integrator within 15 working days from the date of receiving a claim by the Chief Technology Officer, CGA IGFMS Project.

13.5 Architecture for a Decentralized IT System

A decentralized computer system, as opposed to a centralized one, is a collection of autonomous computers or computer systems which communicate with one another to perform a common service. Decentralized systems have geographic and organizational diversity. As is the case at the O/o CGA, the option of implementing a decentralized IT solution may also be considered due to the vast geographical expanse of the DDOs and PAOs across the country.

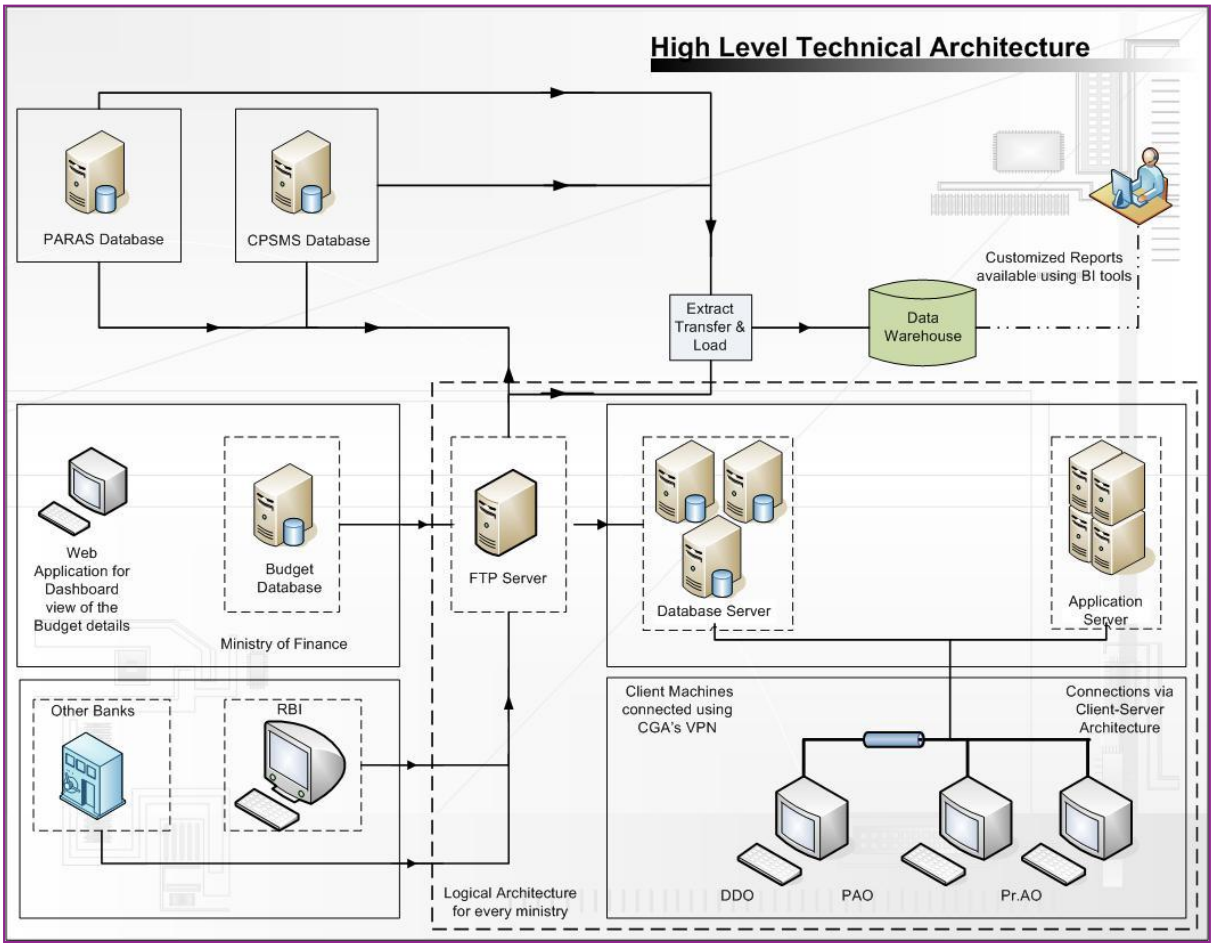
A decentralized solution could have the following common features:

- diverse organizations and organizational procedures,
- diverse computer architectures, both hardware and software,
- diverse terminal types,
- diverse system sizes, from tiny to large, and
- diverse site environments.

The common feature that holds each of these systems together is a message protocol. The parts of these systems are not tightly integrated -- each part is generally quite different from the other. It is "integrated" by having the parts agree to a common but arms-length message protocol.

As the extent of the CGA's IT solution would span across most Civil Ministries, the technical architecture for a decentralized IT solution for the O/o CGA would imply that each Civil Ministry should have its own Integrated Government Financial Management System (IGFMS) application and database servers. To achieve integrity in the IT system and to allow the O/o CGA to obtain a holistic picture of the accounting data, the data from each of these Civil Ministries should be uploaded to a central data-warehouse from which relevant MIS reports can be obtained using Business Intelligence. Thus, though technically the IT solution would be decentralized, it would still achieve the objective of "integrity" and the entire IT system would function as an Integrated Government Financial Management System (IGFMS).

Accordingly, indicative technical solution architecture for the decentralized IT system would appear as depicted below:



The external entities such as RBI and other banks would communicate with the IT system by means of a message protocol system such as FTP. Data from all external entities can be Extracted, Transformed and Loaded to a central data-warehouse for implementing Business Intelligence.

The user could interact with the BI application front-end to perform analysis, run calculations, and report on performance metrics. The application interface includes the BI engine, OLAP (Online Analytical Processing) engine, dashboard and reporting engine, and alerts engine.

For Office of CGA's business functionality, BI technologies would be extremely helpful in providing historical, current and predictive views of business operations. Common

functions of business intelligence technologies such as reporting, online analytical processing, analytics, data mining, process mining, complex event processing, business performance management, benchmarking, text mining and predictive analytics would provide the required slice-and-dice views of the available information to the CGA for analysis purposes.

If implemented correctly, the decentralized system would allow the CGA's organization flexibility for growth of capacity and function. In addition, the decentralized system can be more maintainable since each part can change to anything necessary so long as it continues to support its external interfaces.

There are several technological reasons for building a decentralized system. It is sometimes not feasible to build a centralized system with the required capacity, response-time, availability or security of a distributed system. Typical issues are:

- **Response-time:** If requestors are distributed over a large area, the transit times for requests and replies may be prohibitive. Long haul communication can add a second to response time putting processing and the needed data close to the requestor eliminates such delays.

- **Availability:** Having geographically distributed autonomous sites processing parts of the same application has the effect of error containment -- a failure or disaster is likely to be limited to a single site. In addition, the remaining sites may be able to substitute for a failed node.

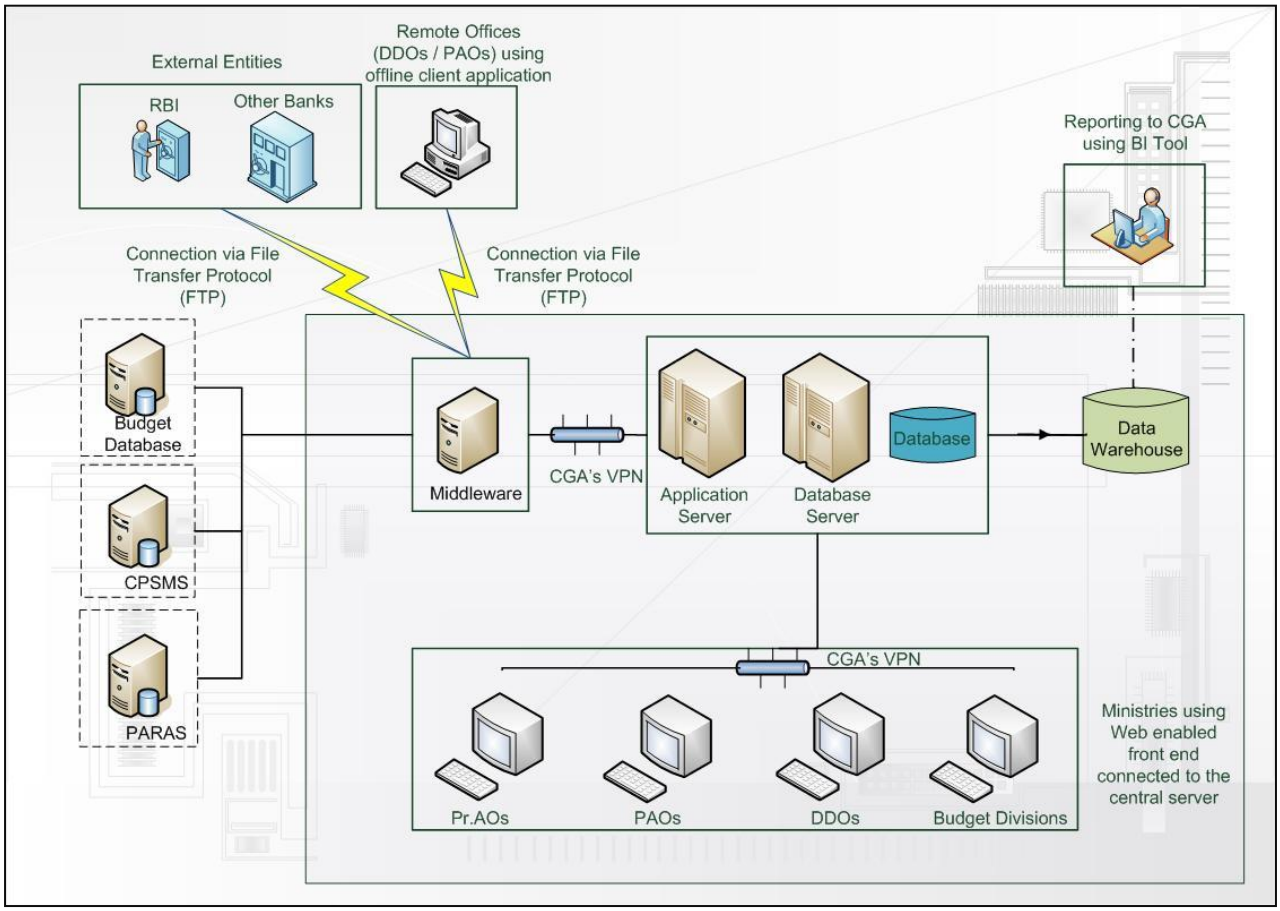
- **Cost:** Decentralization may reduce long-haul communications traffic and hence reduce communications costs. The communications savings may outweigh the extra cost of distributed facilities and staff.

- **Security:** Some organizations feel more secure when they have physical control over the site that stores their data.

A decentralized system is necessarily modular: the autonomous nodes of the computer network communicate with one another via a message protocol. In such a system it is easy to add capacity by adding nodes or by growing a node. If done properly, such change is non-disruptive - changing one service does not interrupt other services so long as the change is upward compatible.

13.6 Architecture for a Hybrid IT System

Indicative technical architecture for a hybrid IT system for the CGA's organization is given below:



To overcome the issues of connectivity for DDOs in remote locations and yet to have all the benefits of the proposed centralized Integrated Government Financial Management System (IGFMS), a hybrid technical architecture for the CGA's organization could also be considered.

As depicted in the hybrid architecture above, the proposed solution would be implemented using a centralized application and database server. Pr. AOs, PAOs, DDOs, and Budget Divisions of the Civil Ministries would connect to the centralized system using a web enabled front end. Thus, wherever network connectivity permits, the DDOs of the respective ministries would be connected to the central server and the accounting data would thus be available for reporting purposes on a real-time basis.

For DDOs in remote locations, where network connectivity is limited and it is not feasible for the DDOs to connect to the central system, an offline application may be developed. The

offline application should allow the day-to-day functioning for DDOs and whenever connectivity is available the offline application would synchronize with the central server.

The hybrid model of the proposed new IT system would thus provide benefits of the centralized approach as has been recommended earlier in this report, and would yet meet the needs of DDOs in remote locations where network connectivity may be limited.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG