Annexure 01

Existing Scope of Work

Employees’ State Insurance Corporation
### Existing Scope of Work

- To deliver medical care and insurance services for Insured Persons (IP) at 1301 Dispensaries, 152 Hospitals, 628 Branch Offices, 59 regional offices and 67 other offices including future expansion if any.

- Operation and Maintenance of Data Centre (DC), Disaster Recovery Centre (DRC) for the deployment of centralized applications

- Operation and Maintenance of various centralized applications along with regular enhancements to functionalities as per changing business needs.

The main data centre for the ESIC application is in ESIC's New Delhi location and the disaster recovery centre is in the Hyderabad location. The users of the ESIC application are spread across all over India. Table lists the number of user's location who are using the ESIC application hosted in the centralized data centre.

<table>
<thead>
<tr>
<th>Location Type</th>
<th>Number of Offices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Centre (DC)</td>
<td>1</td>
</tr>
<tr>
<td>Disaster Recovery Centre (DR)</td>
<td>1</td>
</tr>
<tr>
<td>Head office (HO)</td>
<td>1</td>
</tr>
<tr>
<td>Branch office (BO)</td>
<td>628</td>
</tr>
<tr>
<td>Regional office (RO)/ Sub Regional Offices (SRO)</td>
<td>60</td>
</tr>
<tr>
<td>Hospitals (Hos.)</td>
<td>153</td>
</tr>
<tr>
<td>Dispensaries (DS)</td>
<td>1285</td>
</tr>
<tr>
<td>State Directorate (SD)</td>
<td>29</td>
</tr>
<tr>
<td>Other Offices (OO)</td>
<td>34</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>2192</strong></td>
</tr>
</tbody>
</table>

- State Directorate: is the wing of State administrative machinery that control all the State run hospitals and dispensaries.

- ESIC hospitals/ dispensaries: These are hospitals and dispensaries run by the State and by ESIC.

#### 2.1 Current Solution

Project Panchdeep is divided into five major Modules to achieve the business objectives of ESIC.
**Pehchan:** All services related to issues pertaining to identification, authentication and verification of IPs (Insured Person) are covered under this module.

**Milap:** All services related to provision of networking and bandwidths are covered under this module. There are two components, Bandwidth provider takes care of all issues up to the point of local termination. The local LAN and its power backup is provided by another agency which is part of the implementation team under the supervision of Service Provider. This local agency also does facility management.

**Pashan:** All services related to hardware for data centre, disaster recovery, desktops/PCs/laptops/printers and middleware are covered under this module.

**Dhanwantri:** All services related to the hospitals, dispensaries and diagnostic centres where medical aid that are provided are covered under this module. Issues related to IT support to hospitals, dispensaries and diagnostic centres & Health Insurance are also covered in this module.

**Pragati:** All services of ERP modules related with Finance, Human Resources, Legal, Audit, Annual Performance Appraisal Report, Public Grievance, Right To Information, Vigilance, Training, Project Management, Recruitment, Central Receipt and Issues, Library, Material Management, Campus Management, Health Insurance Module and Document Management System, etc. are covered in this module. All employers and employees related processes through e-forms are part of module Pragati.

**2.1.1 Pehchan**

The solution is based on a centralized web-browser-based with de-centralized transactional capturing with offline capabilities. The solution operates in both, a centralized and de-centralized manner; in a centralized manner, because all data needs to be housed and accessible from a central location and in a de-centralized manner, because collection and processing of data needs to be online regardless of network availability.

This is a Digital solution for capturing data of the insured persons on portable image capture stations. The captured data is stored on central database in Data Centre. The solution is intelligent enough to examine the duplicate registrations. The De-duplication of biometrics is
handled on NEC server and after de-duplication it updates the status on central database and Insurance database.

Insured person verification facilities are provided at all ESIC Locations. A central AFIS (Automated Fingerprint Identification System) is deployed at the central data centre for de-duplication purposes. Full card personalisation and MIS/reporting facilities are deployed.

The core of the whole system is the system central data centre. This data centre houses the database cluster for all of the insured person’s data for the entire country along with the application server cluster and centralised web server cluster (for MIS, Transaction processing and reporting), access/proxy server for protection against intrusions and the backup/file server for management and backup of data.

Card personalisation is performed from the regional office locations which minimises the costs of performing this operation. Insured person’s verification is performed at all ESIC locations. This is a solution of all the components necessary for an integrated system to issue identity card to insured persons for the Employees’ State Insurance Corporation. The salient features are summarized as follows:

- Software design methodology and configuration management based on world-class processes
- Provision of skilled and experienced personnel to execute the project
- A solution that provides client server and web-based support services
- A solution that allows for the implementation of the business requirements for the data collection and card issuing system using the existing core developed system
- A solution that provides for extensive web based management information/reporting
- Provision for de-centralised personalisation of cards
- A solution and system that provides for the issuing of secure cards according to ISO and world standards
- A de-duplication (AFIS) system that provides for world class accuracy and performance

The system consist of the following basic elements: portable data enrolment equipment, AFIS (De-duplication) System, fingerprint verification devices, card personalisation and card issuing system.

The system is made up of the elements as depicted below in System Architecture diagram shown below.
System Architecture

The flow of data is from the data capture, enrolment data of the insured persons, to the central data centre. The data transferred via portable USB storage devices to the nearest regional/branch office that has online connectivity to the data centre. An upload procedure is implemented to branch/regional office to the data centre. Once uploaded, the necessary de-duplication process is activated to ensure that no duplicates are entered into the central database. Once the de-duplication process is finalised the card personalisation is scheduled. All cards then are personalised at this central data centre. Once personalised cards are distributed to the branch office where the insured person is enrolled, the insured person is notified to collect the card. During the first use of the card there is a card activation process. Fingerprint and magnetic stripe reading devices are available at all ESIC locations to capture live fingerprints and read the cards for verification of the insured person's identity. Magnetic stripe card where the insured person's unique number is stored is then used to verify the identity of the insured person by sending this number with a live biometric template to the central database. The result is sent back from the data centre. This is done via a web application.

Software Components

The software components provide the core functionality for the system. The following modules are included with the solution:

- Data Capture Module
- Administration Module
2.1.2 Dhanwantri
ESIC is one of the largest Insurance Corporation in India which provides healthcare facility to Insured Persons. In Project Panchdeep, it is named as ‘Dhanwantri’ which is single application software designed for all hospitals, diagnostic centres, dispensaries and Insurance in the country under ESIC and ESIS.

2.1.2.1 Current Architecture
The following diagram explains the high level architecture:

Dhanwantri can be accessed from thick desktop client and thin web. IIS Server hosts the Web Services and Web Application including business objects and data access objects. Data Access layer is responsible for all data access connecting to MySQL database server.

Dhanwantri is built on a multi-tier architecture that allows the application to run on multiple servers and at various locations. It is designed based on service-oriented architecture (SOA) which helps to achieve higher level of code re-use, allowing applications to bind to services that evolve and improve over time without requiring modification to the applications that consume them. The architecture comprises of loosely coupled services in distributed transaction environment.
2.1.2.2 Service Oriented Architecture - Logical Overview:

The below given diagram depicts the currently Deployed Architecture at Data Centre.

2.1.2.3 Data Centre
Data Centre has mainly three setups – HIS, Insurance and Clinical Data Repository (CDR).

2.1.2.4 HIS Setup:
Total 152 hospitals and 1301 dispensaries are divided into 8 splits. Each split has clustered database servers of 2 nodes and load balanced application servers of 2 nodes. All clustered database servers are connected to a central storage (SAN). Database servers are installed with MySQL Database Server on Solaris/Linux Server; Web Services are deployed on load balanced application servers. Application servers are installed with Hospital Setup.

2.1.2.5 Clinical Data Repository (CDR) Setup:
CDR Database is deployed on clustered database servers with a storage connected to them. Database servers are installed with MySQL Server on Solaris Linux operating system. CDR Web Services are deployed on load balanced application servers. Application servers are installed with IIS.

2.1.2.6 Insurance Setup:
Insurance Database is deployed on clustered database servers with a storage connected to them. Database servers are installed with MySQL database Server on Solaris server operating system.

Insurance Web Services are deployed on load balanced application servers. Application servers are installed with IIS.

2.1.2.7 Hospitals and Dispensaries
Desktop PCs at hospitals and dispensaries are connected to Data Centre though MPLS cloud to run HIS and CDR solutions installed at Data Centre. Smart card reader, biometrics reader, laboratory equipment interface and IP telephony interfaces are implemented at hospitals and dispensaries as required.
2.1.2.8 Laboratory Equipment Interface
- Laboratory Equipment Interface Engine is deployed on a Desktop PC. Interface Engine connects to the laboratory equipment through RS232 and it exchanges data with HIS. Above picture depicts Interface Engine connecting to Laboratory Equipment. Laboratory Equipment Interface Engine is capable of connecting in both Uni-Directional and Bi-Directional.
  - HO/RO/SRO/DO/B0
  - Desktop PCs at HO/RO/SRO/DO/B0 are connected to Data Centre though MPLS cloud to run Insurance solution installed at Data Centre.

2.1.2.9 Insurance Solution
- Insurance solution has all the employers and employer's employee data. Whenever new employee is covered under ESIC, the employee is registered and a TIC (Temporary Identity Card) is issued. Apart from employee, his/her eligible dependents also get registered to avail ESIC coverage.
  - Monthly contribution of all the employees are received from employers and updated in the system.
  - Registered employees (IP) submit their claims (if any) for re-imbursement of their wages after discharging from the hospital. These claims are processed in Insurance solution where the required clinical information is accessed from HIS. Processed claims are advised for payment in ERP.

2.1.2.10 HIS Solution
- Registered employees or their dependents (IP-Insured Person) come to hospitals or dispensaries for treatment. On arrival smart card of the IP is read and
the same is identified and validated in Insurance solution. Validated IPs are provided treatment.

- During treatment IP’s previous clinical data (electronic medical record) is accessed from CDR. At the end of the discharge IP’s clinical data is uploaded to CDR. When an IP goes from one hospital/dispensary to another hospital/dispensary his IP identification and verification is done through Insurance solution which is accessible from HIS setup. Clinical data captured at previous hospital/dispensary is available on CDR which is again accessible from HIS setup. Figure below depicts the flow of an IP visiting hospital to receive payment.

2.1.3 Pragati
A comprehensive ERP Solution is in place to cover the following features under module ‘Pragati’.
- Insurance (Revenue/Benefit)
- Finance & Account
- Human Resources Management Systems
The current ERP is a web-based solution to enable users from various ESIC offices to access the ERP from a Mozilla web browser. The ERP solution is driven by a flexible and configurable workflow engine to ensure it meets all workflow requirements of Pragati. Further, a comprehensive Administration Console help the administrator to manage employee details, department details, Roles, responsibilities, Privileges, Process definitions etc. based on the role assigned. The solution also consist of an employee self-service portal which provide the user with a consistent GUI from which he can perform multiple tasks such as, changing passwords, checking personalized information (PIR), sending messages, receiving corporate notices, participating in groups messages etc.

ERP Solution is hosted on a J2EE compliant Portal Server (Sun Portal & Sun Glassfish Enterprise Server) with the data layer provided by MySQL Enterprise Database. The current ERP solution integrates seamlessly with all other modules on the ESIC solution and across all necessary departments. Similarly all the modules of ERP are integrated with one another based on the rules and regulations of the organization thus eliminating physical movement of information and increasing speed and efficiency of operations.

The solution specifically uses the same / similar forms, registers, & formats so as to enable these organizations to easily transit into an automated environment. The solution incorporate the government rules and procedures so that, it ensures conformity to the stipulated guidelines. The solution ensures update of corresponding files and registers online, thereby eliminating the manual processes.

The ERP Solution has all the above features to decrease the processing time and increasing the operating efficiency.

**Solution Highlights**
- Complete web enable browser based ERP solution
- Seamless integration with internal ERP modules as well other external systems
- Inbuilt configurable rules engine
- Embedded Government of India rules and regulations pertaining to the different modules in the solution
- Flexible and configurable workflow engine to handle complex workflows including multi-level hierarchical workflows
- Integrated work desk to notify and track work-items pending with any particular employee

2.1.3.1 Finance & Accounts

The finance & accounts modules include the complete Workflow of all finance modules starting from the application or initiation of an activity through various approvals, concurrences, and ratifications till the final closure of this particular activity. The accounting system is based on the Government’s Double Entry based Accrual system.

The Financials Accounting system comprises of following core modules – Accounts Payable, Accounts Receivable and General Ledger. The financial accounting system tracks & records the financial transactions arising from different functionalities of the ERP system. The current system includes the following modules:

1. Accounts Payables
   - Bill Processing
   - FVC- General
   - FVC- Interest
   - Cheque Writing
   - Cancel Cheque
   - Replace Cheque

2. Accounts Receivables
   - Receipts

3. General Accounting
   - Chart of Accounts [Budget Architecture]
   - Budget Estimation
   - Budget Allocation
   - Ledger Posting
   - Bank / cash payment & receipts vouchers
   - Journal [Transfer] Entry
   - Bank Credit/Debit Note
   - Cash Book
   - Bank Book
   - Reconciliation
   - Trial Balance
   - Final Accounts [Income & Expenditure Statement, Balance Sheet]
2.1.3.2 Human Resources Management System

The Human Resource Management System are made up of Central modules and Vital Components that are integrated and web enabled. The solution includes the complete Workflow of all these modules starting from the application or initiation of an activity through various approvals, concurrences, and ratifications till the final closure of every particular activity. Each of these modules has different steps / activities through which an application/File moves through. At each step, there is a particular form or a particular field in a form that is entered. This has been taken care in the software.

All the calculations, Formula's, rules & regulations are largely in conformance to Government Rules and Regulations, but are flexible to handle exceptions and changes according to the requirements.

The uniqueness of the solution is that, it is comprehensively integrated to ensure flow of information across modules. E.g. Leave is integrated with Payroll, Promotions, Increments and Pension to integrate the information of non-qualifying leave with these modules. This way all the modules are tightly integrated with one another to allow required information to flow across these modules and thus eliminates redundancy of data.

2.1.3.3 Material Management

The solution includes the complete workflow of all these modules starting from the application or initiation of an activity through various approvals, concurrences, and ratifications till the final closure of a particular activity. The module incorporates similar forms, OMs, registers and other formats that are in use at a Government organization today. This means that the employees have a fast learning curve in learning and using the solution. Each of these modules have a number of different steps /activities through which an application / File moves through. At each step, there is a particular form or a particular field in a form that is entered. This has been taken care in the software. All the calculations, Formulae, rules & regulations are largely in conformance to Central Government Rules and Regulations, but are flexible to handle exceptions and changes according to requirements. Many procedural rules have been incorporated in order to adhere to the regulations of the Indian Government.

Integration with all the departments from which indents originate & the SPCs, allows technical scrutiny by the indenter and approval by the SPC I or SPC II as the case may be. Further, integration of procurement module with the bills & accounts section enable payment & tracking of payments made.

This way all the modules are tightly integrated with one another to allow required information to flow across these modules and thus eliminates redundancy of data.

The Stores & Procurement module automates the Purchase activities starting from raising an indent all the way to making the payment and closing the file.
The following sections give an overview of the features of the modules in current solution.

**Stores & Inventory:**
- Material Inwardly [Goods Receipt Note]
- SDN [Material Issue]
- Material Return
- Material Write-off
- Auctioning
- Fixed Asset Management

**Purchase:**
- Indent
- Process Indent
- PO (Create/Amend/short-close)
- Invoice

It covers medical and non-medical part of material management.

**2.1.3.4 Project Management**
The Project Management module using Primavera enables the tracking of time and materials consumed and follow up on time and material projects and internal projects. Itemization of time and materials for invoicing can be done through this module, while retaining sales prices and cost of items and man hours.

**Registration and Data Entry**
- Create a project
- Create individual sub-projects and link to the main project
- Created of work breakdown structure for the projects
- Allocation of resources to a project

**Project Management**
- Break down the time and materials used on projects and assign individual hours or items to sub-projects for more detailed control of costs and consumables.
- Schedule tasks and allocate resources and capacity to future tasks.

**Accounting**
- The Project Management module is tightly integrated with general ledger functionality, so that dimensions applied to every transaction in a project is in sync.
- Detailed posting profiles are set up, so that transactions are posted to specified ledger accounts depending on pre-set criteria.

**Inquiry and Reporting**

- A report generator enables extended reporting with load and save capabilities.
- A statistic form compares project budgets to consumption over time.
- General ledger integration makes it easy to follow transaction details for a single project or group of projects.

**2.1.3.5 Audit**

Audit modules cover medical and non-medical function of audit. Broadly it covers Internal Audit, External Audit ISO surveillance Audit. All manual business function is governed through this module.

**2.1.3.6 Right to Information**

This module is used by Indian citizens to seek Government Information as mentioned under RTI act of 2005. Whenever ESIC receives any such request from public, the requested information is responded in timely manner. This module is fully automated.

**2.1.3.7 Document Management Systems (DMS)**

The ESIC portal has a robust document management system. This feature is implemented using Alfresco Technologies to capture, store, organize, analyse, create and synthesize information; and making available within and across ESIC users.

Alfresco Document Management captures, shares and retains content, enabling users to version, search and simply build their own content through this tools.

The solution provides Integrated DMS functionality like Check-in, Check-out, Version control, Meta tagging, and Administrative Capabilities. Document processing is provided through a series of workflows included like Document Review, Document Approval, Signature Collection, Issue Tracking, and Customer Routing for Review/Approval. The solution provides enhanced document management site templates that are used right away without further customization:

- Managed Document Library site template
- Divisional Library site template
- Translation Library site template

**2.1.3.8 Central Receipt and Issues (CRI)**
This module covers the daily mail (DAAK) system of ESIC. It includes storing, day to day communication within or outside ESIC, and further passing the mail (DAAK) to respective department for further course of action.

2.1.3.9 Vigilance
This module records investigation actions of the complaints lodged against any ESIC employee. Final inquiry/investigation report can be submitted to respective officials through this module.

2.1.3.10 Campus Management
Campus Management System is one of the modules, which covers all activities related to Colleges run by ESIC Corporation. The Campus Management System has the following high level features:

- Admission Management
- Fee Management
- Attendance Management
- Exam & Mark Management
- Thesis / Dissertation
- Hostel Management

2.1.3.11 Annual Performance Assessment Report (APAR)
APAR Module has been designed to provide an end to end solution for managing the Annual Performance Appraisal of ESIC employees within financial year. It will be initiated at accounting level. Based on performance, rating will be shared to the employees. Employee can appeal to next level if their rating is not satisfactory.

2.1.3.12 Public Grievance
A Grievance is a complaint raised by an Employee, IP or General Public which may be resolved by procedures provided in a Collective agreement, an employment contract or by other mechanisms established by an employer. This module incorporates online provision of settling complaints, grievances by ESIC authorities at Regional Office and Head Office which are received from ESIC Employees (Officers and Staffs), Public and Stakeholders. In addition to these, complaints could also be received and settled from PMO, MPs and Ministries on behalf of employees or public and stakeholders.

2.1.3.13 Legal
Legal Tracking System has been designed to track and manage the court cases internally. It has features to register the case, monitor the proceedings online, manage Advocate registration and payment and extract the report at organization level.
2.1.3.14  Training

Intent of Training module is to govern the training program broadly. It has been provisioned to design the training program, assign the trainer, get the nominations for training, capture the training attendance, collect and upload the training feedback. It also provides reporting features of training program conducted with number of participants.

2.1.3.15  Recruitment

Recruitment module enables the feature of calculating the sanction strength, vacancy calculation, indent creation, job advertisement, and online application form submission, generate offer letter, acceptance of offer letter etc. As of now setting of question paper, evaluation of examination paper etc. are taken care by third party. Once evaluation is done third party submits the marks details to ESIC and further recruitment module takes care to generate the merit list of candidates followed by next recruitment processes.

2.1.3.16  Library

It is fully automated function of ESIC. It caters end to end features of Library management staring from book purchase, issue/return of books, writing off damaged/obsolete books, reporting etc. Currently this module is fully operation in Head Quarter.

2.1.4  Enterprise Intelligence

The current Enterprise Intelligence solution is deployed to meet the analytical and business intelligence requirements of the ESIC. Best in class Business Intelligence Solution is prepared to equip ESIC management team with the analytical tool for enhanced decision-making capabilities. Enterprise Intelligence solution by developing an Enterprise Data Warehouse coupled with an interactive Reporting and Analytical application. The application has help ESIC management team to perform the in depth analysis based on the historical data. The solutions consolidate the data from different business functions and provide a single source of truth to the end users for multi-dimensional analysis along various parameters. Solution design ensures the capability of extending further integration of applications in future. As part of the solution, pre-canned reports and cubes along with GUI based Adhoc reporting capability. Following are the considerations for Enterprise Intelligence solution:

- Modularity
- Flexible and scalable solution architecture.
- Integration - this is one of the key success factors for this solution and features the following:
  - Integrated metadata management
  - Seamless integration with source applications
  - Integration with other applications like exchange server and MS Office.

- Web enablement
• Security as per the user requirements
• Due to non-availability of sufficient data and stabilization period of the transactional applications, it may not be possible to freeze all the Analytical and Statistical requirements immediately after implementation. ETL and analytical framework capable of delivering prioritized analytics earlier and follow an iterative approach to enhance the solution to cater to the ongoing analytical and statistical requirements even post implementation.

At a high level deliverables include the following:
• Deployment of personnel
• Supply of required Software
• Installation and configuration of software tools
• Implementation of Enterprise intelligence solution
• Testing
• Training
• Post implementation support

As part of the solution, data warehouse is built to capture the data for analytical analysis for following key business functional areas:

• Hospital Management System
• Finance
• Insurance
• Inventory
• HR
• Other ERP modules

2.1.4.1 Deliverables:
Current Business Intelligence solution involves following list of deliverables that is tracked and analysed by the ESIC. The list has been finalized during the requirements study Phase of the Project.

The current solution helps in increasing the end user productivity and helps the management team in taking better decisions.

<table>
<thead>
<tr>
<th>Group</th>
<th>Key Performance Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinical</td>
<td>Admissions</td>
</tr>
<tr>
<td></td>
<td>Average Length of Stay</td>
</tr>
<tr>
<td></td>
<td>Discharges</td>
</tr>
<tr>
<td></td>
<td>Occupancy Rate</td>
</tr>
<tr>
<td></td>
<td>Average Daily Census</td>
</tr>
<tr>
<td>Category</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Clinician Load</td>
<td>Average Patient Wait Times</td>
</tr>
<tr>
<td></td>
<td>Outpatient Examination Time</td>
</tr>
<tr>
<td></td>
<td>Patient Satisfaction Count</td>
</tr>
<tr>
<td></td>
<td>Left Without Being Seen Rate</td>
</tr>
<tr>
<td></td>
<td>Mortality Rate</td>
</tr>
<tr>
<td></td>
<td>Overtime Rate</td>
</tr>
<tr>
<td>Physician Load</td>
<td>Predicted Staffing Requirements</td>
</tr>
<tr>
<td></td>
<td>Average Operating Room Turnaround Time</td>
</tr>
<tr>
<td></td>
<td>Operating Room Utilization</td>
</tr>
<tr>
<td></td>
<td>Operation Theatre Utilization Rate</td>
</tr>
<tr>
<td></td>
<td>Radiology Procedure Count</td>
</tr>
<tr>
<td></td>
<td>Laboratory Test Count</td>
</tr>
<tr>
<td></td>
<td>Number of Blood Product Transfused</td>
</tr>
<tr>
<td>Blood Product Wastage Rate</td>
<td>Census Report (ESIC and ESIS Hospital and Dispensaries count State Wise and PAN India)</td>
</tr>
<tr>
<td></td>
<td>Med 6 Report (IP) Monthly and Yearly and combination of number of months</td>
</tr>
<tr>
<td></td>
<td>Med 6 Report (Family) Monthly and Yearly and combination of number of months</td>
</tr>
<tr>
<td></td>
<td>Med 9 Report Monthly and Yearly and combination of number of months</td>
</tr>
<tr>
<td></td>
<td>All regulation Certificate Report: Monthly and Yearly and combination of number of months</td>
</tr>
<tr>
<td>Equipment Utilization Rate</td>
<td>Report Turnaround Time</td>
</tr>
<tr>
<td></td>
<td>Medication Disposal Rate</td>
</tr>
<tr>
<td></td>
<td>Out of Stock Rate</td>
</tr>
<tr>
<td></td>
<td>Average Length of Stay</td>
</tr>
<tr>
<td></td>
<td>Average Daily Census</td>
</tr>
<tr>
<td>Category</td>
<td>Metric</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Bed Turnover Rate</td>
<td>Beds</td>
</tr>
<tr>
<td>Non-Clinical</td>
<td>Total Number of Patients Referred externally</td>
</tr>
<tr>
<td></td>
<td>Most Common Referrals</td>
</tr>
<tr>
<td></td>
<td>Total Number of Delinquent Medical Records</td>
</tr>
<tr>
<td>Material Management</td>
<td>Availability Index</td>
</tr>
<tr>
<td></td>
<td>Safety stock Rate</td>
</tr>
<tr>
<td></td>
<td>Demand Forecasting</td>
</tr>
<tr>
<td></td>
<td>Vendor Performance</td>
</tr>
<tr>
<td></td>
<td>FSN Analysis</td>
</tr>
<tr>
<td>Finance</td>
<td>Medical Benefit Expanses</td>
</tr>
<tr>
<td></td>
<td>Cash Benefit Expanses</td>
</tr>
<tr>
<td></td>
<td>Administrative Cost</td>
</tr>
<tr>
<td></td>
<td>Revenue Generation</td>
</tr>
<tr>
<td></td>
<td>Income Vs Expenditure</td>
</tr>
<tr>
<td></td>
<td>Asset Vs Liability</td>
</tr>
<tr>
<td></td>
<td>Voucher by Finance Report</td>
</tr>
<tr>
<td></td>
<td>Average Expenditure per bed analysis</td>
</tr>
<tr>
<td></td>
<td>Budget Variance Analysis</td>
</tr>
<tr>
<td>Human Resource</td>
<td>Sanctioned posts Vs Vacant</td>
</tr>
<tr>
<td></td>
<td>Employee Grievance</td>
</tr>
<tr>
<td></td>
<td>Average Expenditure per Employee</td>
</tr>
<tr>
<td></td>
<td>Vigilance Status</td>
</tr>
<tr>
<td></td>
<td>Training Expenditure</td>
</tr>
<tr>
<td></td>
<td>Employee Count</td>
</tr>
<tr>
<td></td>
<td>Employee Cost</td>
</tr>
<tr>
<td></td>
<td>Overtime Rate</td>
</tr>
<tr>
<td>Accounts Receivable Rate</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td>Budget Variance Rate</td>
<td></td>
</tr>
<tr>
<td>Expenses</td>
<td></td>
</tr>
<tr>
<td>Current Assets</td>
<td></td>
</tr>
<tr>
<td>Current Liabilities</td>
<td></td>
</tr>
<tr>
<td>Payroll Expense by Department</td>
<td></td>
</tr>
<tr>
<td>Time taken for Requisitions to Reach to Procurement Department</td>
<td></td>
</tr>
<tr>
<td>Time taken for Approved Purchase Order Items Delivered by the Vendor</td>
<td></td>
</tr>
<tr>
<td>End user Request Turnaround Time</td>
<td></td>
</tr>
<tr>
<td>Purchase Order Processing Rate</td>
<td></td>
</tr>
<tr>
<td>Overdue Approved Purchase Order Rate</td>
<td></td>
</tr>
<tr>
<td>Total Number of Zero Stock Days</td>
<td></td>
</tr>
<tr>
<td>Inventory Turnover Rate</td>
<td></td>
</tr>
<tr>
<td>Number of Insured Persons</td>
<td></td>
</tr>
<tr>
<td>Number of Registered Companies</td>
<td></td>
</tr>
<tr>
<td>Number of Pending Claims</td>
<td></td>
</tr>
<tr>
<td>Claims turnover time</td>
<td></td>
</tr>
<tr>
<td>Average Claim Bills</td>
<td></td>
</tr>
<tr>
<td>Days in Inventory</td>
<td></td>
</tr>
<tr>
<td>Insurance</td>
<td></td>
</tr>
<tr>
<td>Determination of Final date of coverage</td>
<td></td>
</tr>
<tr>
<td>Inspection Efficiency</td>
<td></td>
</tr>
<tr>
<td>Survey efficiency</td>
<td></td>
</tr>
<tr>
<td>Defaulters Action</td>
<td></td>
</tr>
<tr>
<td>Efficiency of IR Processing</td>
<td></td>
</tr>
<tr>
<td>Review of Demand Letter</td>
<td></td>
</tr>
<tr>
<td>New Area Implementation</td>
<td></td>
</tr>
<tr>
<td>Benefit Disposal Efficiency</td>
<td></td>
</tr>
<tr>
<td>Benefit Disposal Efficiency (Long Term)</td>
<td></td>
</tr>
<tr>
<td>New Registration Efficiency</td>
<td></td>
</tr>
<tr>
<td>----------------------------</td>
<td></td>
</tr>
<tr>
<td>New Employer registration count</td>
<td></td>
</tr>
<tr>
<td>Total Employer count (Old &amp; New Registration)</td>
<td></td>
</tr>
<tr>
<td>Employer status wise report (Count of status change)</td>
<td></td>
</tr>
<tr>
<td>IP registration report: Gender wise (At HQ) &amp; BO wise (RO/SRO wise)</td>
<td></td>
</tr>
<tr>
<td>Benefit transaction count (PD count details)</td>
<td></td>
</tr>
<tr>
<td>Benefit Pendency report</td>
<td></td>
</tr>
<tr>
<td>Disabled IP report</td>
<td></td>
</tr>
<tr>
<td>Default IP Report</td>
<td></td>
</tr>
<tr>
<td>Monthly Progress Register For Inspection</td>
<td></td>
</tr>
<tr>
<td>Monthly report of Survey</td>
<td></td>
</tr>
<tr>
<td>Monthly AOD Report</td>
<td></td>
</tr>
<tr>
<td>Challan Count &amp; Amount</td>
<td></td>
</tr>
<tr>
<td>Offline &amp; Online Challan Status</td>
<td></td>
</tr>
<tr>
<td>Recovery Report</td>
<td></td>
</tr>
</tbody>
</table>

**Other Deliverables**

- Business Analysis & Requirement Specifications Document
- Deployment of EDW infrastructure
- Information and Data Analysis
- Source Data , Business Requirements , LDM and Reports Mapping
- ETL Development & Testing
- Reporting & Analysis Development & Testing
- Data Mining & Statistical Services
- Metadata
- UAT Criteria / Plan (ESIC Responsibility)
- System & Integration Testing
- Backup & Archiving policies & implementation
- Security Mechanism Implementation

- Operation Maintenance Training
- Final Application Deployment
- Maintenance of the Application
• Service Desk System
• Documentation
  • Requirements Specifications
  • Data Model Design
  • ETL Architecture & Design
  • Reporting Architecture & Design
  • Data Mining & Statistical Designs
  • Operation Maintenance Manual
  • Security Implementation Document

2.1.4.2 BI Process - ESIC Logical Data Model

• Data Management

All the relevant data that is made available by the individual source systems is captured, EDW team not create or correct any source data.

• ETL Process
  • Extracting data from the source system as per mutually agreed Data exchange mechanism.
  • Design & Implementation of ETL Scripts to load data from source system to staging and finally into the enterprise data warehouse.
  • Implementation of Data Quality based on business rules.

• Frequency
  Daily

• Backup
  ETL repository is backed up on daily basis. Any changes in the ETL mapping versions are maintained via version control tool.

• Staging Area
  Staging area is the intermediate area between the source data and the target EDW. Primarily there are two components of the Staging area.
  • Landing / Staging Layer
  • Data Cleansing and transformation layer

Data is extracted from the source system and loaded into in the landing layer of the staging area without applying any transformation rules. The data quality rules captured during the requirement Phase is applied to transform the source data into the quality to data to be loaded into the EDW.

Staging area captures the incremental data on daily basis and not stores any historical data. Staging area is the only point of loading the data into the EDW.
Staging area also holds all the temporary tables required for transforming and loading the data from staging to the EDW.

- **Out of Scope**
  - Address Standardization
  - Data Entry
  - Any manual correction of Erroneous or Rejected records

### 2.1.4.3 Infrastructure
This installation and configuration is done once by Current Service Provider; any change in the Current tools later on or change in the hardware platform or any other requirement that forces installation to be done again is taken as part of Current Service Provider’s change management program.

- **Key Solution Components**
  - MYSQL Enterprise Edition
  - SAS® Enterprise Business Intelligence
  - Pentaho
  - SAS® Data Integration
  - SAS® Analytics
  - R Language

- **Solution Architecture Diagram**
Underlying diagram represents the Current BI architecture.

![BI Architecture Diagram](image)

- **Risk**
As part of any solution, there are certain risk factors,

- **Some of the Risks envisaged are:**
  - Data Quality
• Non Compliance of Critical Fields
• Failure of critical business & referential integrity rules
• Non Standard use of Codes across enterprise
• Network Connectivity
• Active Participation & Involvement of all IT personnel at various locations across the enterprise.
• Readiness of all Infrastructure at Central Data Centre

**Approach/Methodology**

**Key Factors determining the Approach**

The key factors that determine the final solution approach are

• Network Load
• Availability of source system extraction window
• Requirements captured during Requirements Phase
• Performance & Overall Time for execution
• Audit Trail & Security

### 2.1.5 Overall Portal Architecture

The architecture below depicts the Overall Solution Architecture for Panchdeep project. It is a layered technology solution with clear segregation of Healthcare, ERP, Data Analysis, Messaging and Collaboration components of the solution. This solution is based on SUN Stack with Sun Application Server (Glassfish), Sun Process Server forming the middleware layer. SAS constitutes of ETL and Data analysis and Reporting utility. MySQL RDBMS provides persistence layer for structured data. SAS provides the analysis, search & mining capabilities.

The approach of solution stack selection is based on "best-of-breed" components and products in the industry. Advantage of this approach is the ability of the solution architecture to adapt itself to whatever solutions / products are chosen at each layer independent of the other layers. Every piece of ESIC's business requirement has been mapped into one or more components in solution architecture based on the reference architecture.
Overall Technical Architecture

Following table provides a detailed product map for every component described in the above solution architecture. This section comprehensively maps ESIC functional area to corresponding solution technology/ product(s)

<table>
<thead>
<tr>
<th>ESIC Functional area</th>
<th>Solution</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td></td>
<td>Current Service Provider ERP Solution</td>
</tr>
<tr>
<td>HR, Training and ESS</td>
<td></td>
<td>Current Service Provider ERP Solution</td>
</tr>
<tr>
<td>Salary and Compensation, Payroll</td>
<td></td>
<td>Current Service Provider ERP Solution</td>
</tr>
<tr>
<td>Legal</td>
<td></td>
<td>Current Service Provider ERP Solution</td>
</tr>
<tr>
<td>Procurement</td>
<td></td>
<td>Current Service Provider ERP Solution</td>
</tr>
<tr>
<td>Project Management</td>
<td></td>
<td>Current Service Provider ERP Solution</td>
</tr>
<tr>
<td>Library Management system</td>
<td></td>
<td>Current Service Provider ERP Solution</td>
</tr>
<tr>
<td>Medical</td>
<td></td>
<td>Current Service Provider HIS Solution</td>
</tr>
<tr>
<td>Insurance Module</td>
<td></td>
<td>Current Service Provider HIS Solution</td>
</tr>
<tr>
<td>HealthCare Solution</td>
<td></td>
<td>Current Service Provider HIS Solution</td>
</tr>
<tr>
<td>Health Insurance Module, HIM at Hospitals and Dispensaries</td>
<td></td>
<td>Current Service Provider HIS Solution</td>
</tr>
<tr>
<td>Enterprise Intelligence Platform</td>
<td></td>
<td>SAS Solution (ETL,DQ,BI and SA)</td>
</tr>
<tr>
<td>Document Management Solution</td>
<td></td>
<td>Alfresco</td>
</tr>
<tr>
<td>Portal Solution</td>
<td></td>
<td>Sun Portal 7</td>
</tr>
<tr>
<td>SOA Solution</td>
<td></td>
<td>Java CAPS</td>
</tr>
<tr>
<td>Mail Messaging</td>
<td></td>
<td>Sun Messaging Solution</td>
</tr>
</tbody>
</table>
2.1.5.1 Portal Design & Architecture

The current architecture comprises of following broad technology components:

- **Client Layer**: The Client layer contains the devices that interact with Portal.
- **Browser** – This is a traditional Internet browser that initiates requests to the Web Server and displays the results of requests. Users access the portal using internet browsers; the content is personalized for registered users. Content Authors have access to publishing site both internally and through the internet.

- **DMZ Zone Layer**: This is the layer hosting the edge servers, external DNS, SMTP relay services, front-end Web Servers & Presentation Services.

- **Load Balancer** – This is the hardware load balancer that ensures that load is distributed evenly across all of the web server instances.

- **Directory Services** – The Directory services is provided through Sun Directory Server and Open SSO. Sun Directory Server holds the user credentials for all users including the internal authors & content publishers.
- **Web Front End Server** - This is a traditional web server that serves the content or forwards requests to the Application Server. Web Server takes the request and recognizes that the requested resource is on the application server, and, using the Web server plug-in, redirects the request to the Application Servers.

- **Alfresco Content Management Servers Farm** – these servers take care of the following roles: Web Content, Document and Records Management, Content Publishing and Approvals.

- **Application server** – The various custom-built applications is deployed on the application server.

- **Integration server** - The application integration services provide a composite platform optimized for building service-oriented applications that extend and integrate into ESIC’s the custom-built application infrastructure as well as the ERP applications. Java CAPS is used for the same.

- **Mail Server** – The messaging system along with collaboration is a standards-based SMTP/POP/IMAP mail server that offers a full range of mail server functionality. The messaging solution is designed to manage the email needs of any number of individual users and comes complete with a powerful set of integrated tools for managing mail accounts and message formats. It also offers a scalable SMTP, POP3, and IMAP4 mail server complete with LDAP and Active Directory support, an integrated browser-based email client, content filtering, spam filters, extensive security features, and more.

Backup & Restore of Data: The infrastructure use structured back & restores solution to provide resilience to the entire infrastructure.

### 2.1.5.2 ESIC Web Portal

Portal complies with SOA approaches and uses service oriented concepts, leverages Web services extensively and leverages portlets, which consume services or communicate to provide seamless integration of applications.

User interface Services provide the capabilities required to deliver ESIC IT functions and data to end users, meeting the end-user's specific usage preferences. Interaction services provide the portal view of ESIC applications as a simple, unified access point to applications.

A complete ESIC portal solution should provide users with convenient access for day to day functions in a secure manner. Portals provide an extensible framework for interacting with enterprise ESIC applications, content, people, and processes. The Portal provides additional services such as single sign-on, security, document management, web content publishing,
search, personalization, collaboration services, enterprise application integration, support for mobile devices, and site analytics

Apart from integrated single user interface infrastructure for the ESIC IT Solution, Sun Portal along with Alfresco and Java CAPS provide following functionality to the ESIC application users as desired by ESIC, like:

- The portal is based on SOA based model and uses web services extensively
- Seamless integration with the applications such as Hospital management System, ERP application etc.
- Document Management
- Workflow
- Records Management
- Search

- Knowledge Management
- Collaboration services
- Web Content Management
- Versioning and Document Control
- Security services such as Single Sign On

2.1.5.2.1 Sun Java System Portal Server for ESIC

The Sun Portal server provides features like personalization, aggregation, integration with various back-ends out of the box. The Portal server is used for both Intranet and Internet based portals. The SRA is used for accessing the back-end resources of ESIC securely from the portal. The Sun Portal server is deployed both vertically (by adding more portal instances in a server) or horizontally (by having more servers) to achieve scalability.

The Java System Portal Server provides identity-based content delivery, as per ESIC's requirements, which enables enterprises to define portal pages and provide users with access to content specific to organizations, sub-organizations, roles, and even user-defined communities.

The Identity-based capabilities of the Java System Portal Server, asper ESIC's requirements include:

- Web single sign-on (550) for secure login to the portal and all applications accessed through the portal, as well as across multiple portals for portal federation
- Flexible authentication (can support multiple authentication schemes like LDAP, UNIX, NIS, RADIUS and x.509 digital certificates) and authorization services for changing and complex business environments.
- Fine-grained policy rules so that multiple authentication mechanisms is chained together to provide additional flexibility and integration of legacy systems
- Secure SSL based Portal server ensures that we have a security enabled portal.
Delegated admin features to manage Portal server.
There are several Portlets available out of the box, for the most commonly used functionalities like Email, Blog, and RSS/XML.
The Other important features of portal, which match ESIC's requirements:
- Full text search engine with federated search and taxonomy capabilities
- Extensive community features like built-in wikis, blog support, sharing files, group calendaring, and communities
- The Portlets to be deployed on the Sun Portal server is developed via NetBeans and deployed remotely to the Sun Portal server after development.

2.1.5.2.2 Service Oriented Architecture Model:
The Middle tier architecture suggested for the Portal environment is based on well-known open standards based architecture - **Service Oriented Architecture (Aka SOA)**. All business capabilities of the ESIC portal such as Hospital Management, ERP, Mail and messaging solution etc. is wrapped around services layer (or SOA) using Windows Communicate Foundation technologies. These services are consumed by the frontend ESIC portal.

2.1.5.2.3 Web Content Management with Workflow:
ESIC has listed the compliance requirements for the Content Management / workflow requirements in the PASHAN. Filled compliance sheet has been given in the later section of the document. This feature is provided by Alfresco which enable designated ESIC administrators to have content management feature. The static contents which are hosted out of ESIC portal is kept up-to-date with version control. This is an in-built feature of Alfresco Technologies which enable this functionality using workflow based approval process. The centrally controlled auditing, expiration & retention policies, archival, retention and regulatory compliance is implemented based on records management feature of Alfresco Technologies.

2.1.5.2.4 Collaboration features such as discussion forums, wikis and blogs:
Alfresco provides a number of new features while improving the existing collaboration platform by providing built-in abilities for document management and alerting, adding new capabilities like blogs, wikis, and a Web Part for publishing and receiving RSS feeds.

2.1.5.2.5 Personalization and Team Sites:
A major advancement in sun portal is increased personalization of the portal experience. Users can create lists, document libraries, or sub sites under their My Site and customize the viewing of these sites for both their personal and workgroup views. The My Site also provides new Web Parts for organization hierarchies and colleague tracking, including alerts when metadata for your colleagues change, such as their phone number, title, office location, or other information.
2.1.5.2.6 Single Sign On:
Provide the essential elements of comprehensive security management by employing a range of authentication providers, policy management, group management, and permission levels ranging from individual items in list to entire sites.

2.1.5.2.7 Content Management:
The facilities for the creation, publication, and management of content, regardless of whether that content exists in discrete documents or is published as Web pages. Content management scenarios include document management, records management, and Web content management. Alfresco has integrated Web content management capabilities allowing organizations to empower their business users to manage their own Web content. Some of the features include:
- Support for high-fidelity Web sites with consistent branding
- Navigation controls that automatically render site navigation links
- Browser-based Web authoring with a WYSIWYG Web content editor
- Content publishing and deployment with workflows
- Publishing site templates
- Multilingual site support

2.1.5.2.8 Technical Architecture components
A. SAS® Enterprise Data Integration Server (SAS EDI Server):
The SAS Data Integration Server provides the ability to integrate data from the various source systems of ESIC. This address all of the current as well as future integration needs of ESIC. A high-performance data integration platform that reduces the cost and risk of enterprise ETL through increased efficiency and greater convenience when completing daily and ad-hoc ETL tasks and delivers a single version of the truth allowing organizations to set new standards in the quality of information produced for both internal and external consumption.

In general, SAS Data Integration Server provides an ability to integrate data from the following different types of sources:

B. SAS/ACCESS for relational databases (RDBMS)
- DB2 under 05/390, DB2 under VM, DB2 under UNIX or PC
- CA-Open Ingres
- Informix
- ODBC
- OLEDB
- ORACLE
- Oracle RDB
- SYBASE
- MS SQL Server
- Teradata
C. **SAS/ACCESS for non-relational databases and other data sources**
   - SAS/ACCESS Interface to ADABAS
   - SAS/ACCESS Interface to CA-DATACOM/DB
   - SAS/ACCESS Interface to CA-IDMS
   - SAS/ACCESS Interface to IMS-DL/I
   - SAS/ACCESS Interface to PC File Formats
   - SAS/ACCESS Interface to SYSTEM 2000 software

D. **SAS Enterprise Business Intelligence Server (SAS EBI Server):**
   Consist of following:
   - SAS Information Delivery Portal
   - SAS OLAP Server and OLAP Cube Studio
   - SAS Web Report Studio
   - SAS Add in for Microsoft

2.1.6 **Milap**
Task Milap under project Panchdeep connect all locations of ESIC. Task Milap is backbone of all other IT initiatives under Project Panchdeep. The current network backbone is available across all levels 24/7 @365 days a year. The setup is basis of a central on-line Hospital Information system. Task Milap manage and maintain Application, servers, storage, network, security and other components. Underlying network provides connectivity for a portal based enterprise resource application for providing specified functionalities from a centralized Data Centre at ESIC.

2.1.6.1 **Network Architecture**
The current network Architecture for project Panchdeep as mentioned in Milap can be categorized in following areas
   a. Secured Wide Area Network
   b. Local Area Network at ESIC HO, RO, Brach Office, Hospital, Dispensaries, RBO & State Dir.
   c. Data Centre network Architecture.
   d. Call Control or IP-PBX Telephony across all levels of ESIC current network backbone.

Following paragraphs provide details of current network Architecture and Design for each of above mentioned ESIC network subcomponent.

1. **Secured Wide Area Network**
It is current to connect all ESIC locations including Head Office, RO, Branch office, hospitals, dispensaries, RBO & state Dir. with Service provider enabled MPLS based Wide Area network. It is current to use two separate service providers with both providing similar connectivity as per ESIC requirements. Current links from separate service providers can be load balanced as desired by ESIC. The current Wide Area network is based on HUB and SPOKE model with each site having redundant MPLS VPN to Data Center and Disaster Recovery site respectively.

It is current to secure entire ESIC Wide Area Network comprising service provider based MPLS VPN with overlay Site to Site/Any to Any IPSEC tunnels between ESIC Datacentre/DR and ESIC RO, Branch office, hospitals, dispensaries, RBO & state Dir. offices using Triple DES (3DES)/Advance Encryption Standard(AES) encryption standards.

The current wide area network is highly scalable, manageable, and cost effective, and meets government-mandated encryption requirements. Current Network is enabled with end to end Quality of Service configurations for servicing Voice, Video and WEB applications with guaranteed quality.

**Figure 28 — Secured WAN**

**WAN TRAFFIC:**
ESIC is an Portal based platform, where the services and business application accessed via intranet & MPLS WAN Connectivity is provided by Current Service provider through secured redundant network connections. Users from different locations connect to Data Centre through these links.

**NETWORK:**

- Routers in redundancy are positioned at DC & DR
- One router is positioned at all other locations to connect to datacentre
- Core Switches are positioned at a DC& DR in HA mode
- Redundant WAN links is provided by Current Service provider.

**Solution Components**
Current Wide Area Network comprise of Cisco Integrated Services Routers (ISR) at all locations. The ISR Series supports more than 100 WAN interfaces, making it suitable for a wide variety of deployment options.

2. **Local Area Network at ESIC head Quarter, Regional HO's and branch offices including Dispensaries**
The current local Area Network at Regional offices of ESIC comprise of single layer 3 enabled manageable switch and multiple layer 2 switches providing 10/100 base T connectivity to end user Desktop computers and IP Phones. Current switches provide required Power of Ethernet support to connecting IP Phones as per IEEE 802.3af standard. ESIC Branch Office LAN comprise of single layer 2 switch providing 10/100 base T connectivity to End user Desktop Computers and IP Phones.

**Solution Components**
Current local Area Network at Regional Offices comprises of Cisco Catalyst 3750 layer 3 enabled manageable switches. The Cisco Catalyst 3750-E Series provides stackable switches offering multilayer switching, the switch improves LAN operating efficiency by combining ease of use and the highest resiliency available for stackable switches. Cisco catalyst 2960 provides end user connectivity with each switch providing 2410/100 base T connectivity to Desktop computers and IP Phones. The current Cisco Catalyst switches meets all the functional requirements and technical specifications mentioned in ESIC tender document.

3. **Data Center Network Architecture**
The current network architecture for Datacentre and Disaster Recovery site comprise of following components
- a. Core Router
- b. Core Switch
- c. Storage Area Network

4. **Network Security:**
Perimeter Firewall (Internet& Intranet), Server Farm Firewall, Network analysis, Network/Host based IPS and, AAA server, Network admission control and Correlation and Monitoring response system.

**2.1.6.2 Datacentre/Disaster Recovery Center Architecture**
ESIC data center host various mission critical applications which are accessed by users from Internet as well as from WAN locations (Regional office/ Sub Regional offices, Branch office, Hospitals, Dispensaries and State Directorates).
The applications hosted at ESIC datacentre have 3-tier architecture. Users on internet access
the portal/interface servers located in the public zone, users on intranet accessing the application from regional office, branch office, hospitals etc. access the intranet portal servers located at internal DMZ. The critical application servers and database servers are located at internal MZ zone.

Radware application delivery and network security solution at these datacentres provide complete availability, performance and security to these mission critical applications. Highlights

- 2 MPLS links are provisioned at the datacentre working in active-active mode for users accessing the application from intranet
- 2 Internet links of 120 Mbps each are provisioned at the datacentre working in active-active mode for users accessing the application from internet
- Link load balancers are provisioned for both internet and intranet links for even distribution of load and high availability of these links
- Intrusion prevention systems at the internet and intranet perimeters are deployed with SSL descriptors to provide protection from DOS/DDOS, virus worms, Trojans etc. and also from encrypted SSL based attacks
- 2 layers of firewalls are deployed to provide comprehensive security to the ESIC datacentre.
- Additional layer of IPS is provisioned at the internal MZ to protect ESIC's critical servers and services running from vulnerabilities and threats.
- URL filters, antispam servers, network antivirus servers are located at public DMZ. Flow manager switches are deployed to ensure optimum utilization and scalability and performance of these security devices
- Server load balancers are deployed at public, DMZ and internal MZ zones to distribute the load across multiple servers and provide high availability of servers and services
- SSL accelerators are deployed at public, DMZ zones to offload the servers from CPU intensive SSL encryption, decryption and also accelerate the performance of applications. Web application firewall module on these SSL accelerator provide application, service and content based access control
- Global server load balancing capability on the server load balancers ensures seamless redirection of complete user traffic to DR in the event of critical DC failures.

2.1.6.3 Current Solution Components:
- **Hardware:** Servers, Storage, Tape Library
- **System software:** OS, Database, Middleware, Mailing solution
- **Network:** Routers, Switches, FCIP Directors, WAN Accelerators, Link Load Balancers, Flow Control, Server Load Balancers, IP Telephony, Videoconferencing
- **Security:** Firewall, IPS, RIDS, Authentication, Gateway Antivirus & Antispam, SSL Off-loaders
• **Management:** Event Correlation, Log Collection, EMS, NMS
• The ESIC Data Centre site is designed with an understanding that the main services & operations to users is available at the very critical time.

2.1.6.4 Wide Area application acceleration and optimization.

Solution Components

- **Core Router**
  The Core Router is placed at edge of Data center, which is providing connectivity to the backbone network, either on multiple Ch-STM1 or Gigabit Ethernet connectivity. Current network architecture comprise of Cisco 7600 Series router as core router aggregating all overlay Secured VPN (GRE with IPSEC/GET/DMVPN) tunnels between Datacentre and Remote ESIC offices (RO/B0).

**Core Switch:**
ESIC has deployed Cisco catalyst 6509 with supervisor 720 processor module as Datacentre core switch.
The high switching rate, large switch fabric and 10 GigE densities make the 6509 ideal for this layer. Datacentre core is interconnected with both campuses in redundant fashion with layer 3
10GigE links.

2.1.6.5 Tiered Access Control
The current data center security solution offers multiple configuration points for access control lists (ACLs) for simplified ACL management and scalability. The data center aggregation layer is a Catalyst 6500 with a firewall service blade. This allows several filtering points for both client-to-server traffic and server-to-server traffic.

Solution Components
Network Firewall
Cisco ASA 5580 Series adaptive security appliance is a purpose-built solution that combine best-of-breed security and VPN services with the innovative Cisco Adaptive Identification and Mitigation (AIM) architecture. Designed as a core component of the ESIC Network, the Cisco ASA 5580 Series provides proactive threat defense that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity. The result is a powerful multifunction network security appliance family that provides the security breadth and depth for protecting home office, branch office, small and medium-sized business, and enterprise networks while reducing the overall deployment and operations costs and complexities associated with providing this new level of security.

Server Farm protection Firewall
To provide server farm security by segmenting servers in multiple firewall protected zones current architecture uses Cisco Firewall Services module in Core Switch i.e. Cisco catalyst 6509. It is used to place servers in different Layer 2 domains or virtual LANs (VLANs), and to separate those VLANs using firewall module. Efficiency and productivity gains: Virtualized FWSM delivers multiple firewalls on one physical hardware platform. Network administrators can configure, deploy, and manage these functions as if they were separate devices. Using virtualization to reduce the number of physical devices in a network significantly reduces the cost and complexity of managing network infrastructure.

Security Monitoring and co-relation appliance
Cisco Security MARS appliance is currently in use as security co-relation solution to capture events and logs from a wide range of network devices (such as routers and switches), security devices/applications (such as firewalls, network and host intrusion. Cisco Security MARS transforms raw network and security data into intelligence that can be used to subvert valid security incidents and maintain compliance. Cisco Security MARS enables Service Providers to centralize, detect, mitigate, and report on priority threats using the network and security devices already deployed in network infrastructure.

AAA System
Cisco ACS appliance for Windows platform is current AAA system for ESIC network. Cisco Secure Access Control Server (ACS) is an access policy control platform that helps to comply with growing regulatory and corporate requirements. By integrating with other access control systems, it helps improve productivity and contain costs. It supports multiple scenarios
simultaneously, including:
- Device administration: Authenticates administrators, authorizes commands, and provides an audit trail
- Remote Access: Works with VPN and other remote network access devices to enforce access policies
- Network admission control: Communicates with posture and audit servers to enforce admission control policies

It meets all laid down specifications for AAA system in ESIC tender Document.

**Network Admission Control System**
Cisco NAC Appliance is current Network Admission Control System for ESIC network. Cisco NAC is an easily deployed Network Admission Control (NAC) product that allows Network administrators to authenticate, authorize, evaluate, and remediate wired and remote users and their machines prior to allowing users onto the network. It identifies whether networked devices such as desktops, and other corporate assets are compliant with a network's security policies, and it repairs any vulnerabilities before permitting access to the network.

- Device type. Cisco NAC Appliance can enforce security policies on all networked devices, including Windows, Mac, or Linux machines; laptops; desktops; personal digital assistants (PDAs); and corporate assets, such as printers and IP phones.
- Device ownership. Cisco NAC Appliance can apply security policies to systems owned by the corporation, employees, contractors, and guests.
- Device access method. Cisco NAC Appliance applies network admission control to devices connecting through the LAN, WLAN, WAN, or VPN.

**DC Replication Acceleration Device**
The Cisco Wide Area Application Services (WAAS) solution is current acceleration device for DC DR Replication traffic in ESIC network. It is designed to allow ESIC to consolidate their storage, and backup infrastructure into data centers while preserving local application network (LAN)-performance as well as current network and security infrastructure.

**4. Call Control or 1P-PBX Telephony**
Cisco Unified Communication solution is currently to provide integrated telephony solution for IP Phones, gateways over IP architecture using [SIC IP network backbone. The Design Objectives for the architecture is design the highly resilient and available Unified IP communication setup.

- Provide high level of Redundancy and Resiliency to minimize the failure points and risks.
- Provide Remote Branch users with all the same features and functions of the voice services available at the Central/Main Location i.e. built in feature consistency across enterprise.
- Enable central team for operations and maintenance control to minimize operational complexities (Add/Move/Change) and provisioning/new feature rollout challenges.
- Simplifying the dial plan across the ESIC IP Communication setup.
- Cisco proposes a Multi-Site Centralized Call Processing Model to provide telephony services to ESIC across the main and remote branch sites. The current solution includes six redundant 7845 Media Convergence Servers for call processing at the Data Center serving the entire site spread across the WAN MPLS cloud.
Application Access
The network has a comprehensive redundancy and high availability built for end user access. 2 Internet links on DC and DRC have been provisioned to ensure non dependency on an Internet service provider. Radware Link Proofs sitting at the perimeter intelligently decides the best performing and most available ISP link to Direct clients to the Applications hosted in the data center. Two links for each MPLS and SAN connectivity have also been current and Link proof do intelligent WAN/MPLS and SAN connectivity load balancing and automated failover for the same. Also each Regional office/ Sub Regional offices, Branch office, Hospitals, Dispensaries and State Directorates have been current to have two WAN links each from different ISP and a branch level link load balancing solution help these branch locations to access DC resource without having dependency on one service provider/link. In case of any Service Provider or any WAN ling goes down the branch side link load balancer ensure that the user connectivity to DC site is not affected. In case of MPLS and SAN, the traffic does not get Netted and hence it is the Link proof’s intelligent feature of NHR tracking table which ensure that reply traffic is sent via the same link from which the traffic was requested. This ensures there is no delay in the response.

Deploying Link Proof to address ISP links load balancing and High Availability
Link Proof ensures effective inbound and outbound load balancing of all the links and traffic switch over to any available link in case of link failure/router failure using multiple health check algorithm and full path health monitoring to ensure complete link availability. This automated switch over is transparent to the user. Link proof combines the links and provide aggregated throughput. The intelligent inbound load balancing of Link Proof using proximity calculations ensure that users accessing applications from internet get the best link and hence the application response is faster for users to ensure performance. Users accessing applications like www.esic.in is inbound load balanced by Link Proof. Link proof ensure that the users get the application access from the best performing link at that point.

Application Front End
The data centre host various mission critical applications and these applications sit in Public, DMZ and MZ zones on the firewall. Radware's industry leading application front end solution provide server load balancing, application acceleration and automated switchover to available server in case any of the application server is down (due to any reason be it application down issue or hardware issue) using health monitoring module. On top of the above the application response is boosted by offloading SSL from webservers to dedicated application accelerator appliances which do TCP optimization, compression, image reduction to enhance the application response and relieve server from doing CPU intensive SSL Handshake / encryption / decryption.
2.1.6.6 Hardware Architecture Regional Offices

The regional hardware architecture comprises of a windows based IIS server, several workstations, printing facilities and a card personalisation system. The data deployed on the windows server is MSSQL database for storage of regional data and card personalisation data to personalise cards for that region. Provision has been made to store up to 200,000 records of data (insured person data as well as card personalisation data).

All the card personalisation facilities, captured data upload to central database and MIS/Reporting facilities is hosted at the regional server. Connectivity must also be provided to the central database. The regional offices hardware architecture is shown in the figure below.

Figure 31 — Regional Hardware Architecture

2.1.6.7 Mail & Messaging Deployment Architecture

Following diagram illustrates a sample deployment diagram for the Mail and Messaging Infrastructure.
For Mail and Messaging Java Mail messaging system is in use. Some of the features are:

- Java System Messaging Server
- Java System Calendar Server
- Java System Instant Messaging
- Java System Connector for Microsoft Outlook
- Convergence

The messaging system along with collaboration is a standards-based SMTP/POP/IMAP mail server that offers a full range of mail server functionality. The messaging solution is designed to manage the email needs of any number of individual users and comes complete with a powerful set of integrated tools for managing mail accounts and message formats. It also offers a scalable SMTP, POP3, and IMAP4 mail server complete with LDAP and Active Directory support, an integrated browser-based email client, content filtering, spam filters, extensive security features, and more.

2.1.7 Pashan
2.1.7.1 Data Center

2.1.7.1.1 Datacentre Indicative Architecture

2.1.7.1.2 Physical infrastructure

Location of the Data center facility
The location identified for the Data center is open from two sides and it is a three-floor building.

Data center Area
The current data center area is located on ground and first floor. Walls are not exposed to the direct sunlight. The structural floor and ceiling is separated by 13 ft. (min).
Data center building meets the point load and distributed load requirement of the equipment's (Servers racks, Fire suppression cylinders, Main electrical panel, and Air Handling unit). Required load bearing capacity in building is ensured by ESIC.
It is also advisable that the floor above the Data Center is free from any water sources. And
there is no source of air contamination around the Datacentres or from the adjacent building.
The location identified for the data center is free from sources of EMI, industrial pollution, and
vibration. The building has good infrastructure support like power, chilling plant and redundant
source in case of prolonged outage of the data center infrastructure. The building also has
established security resources that take care of miscreant’s attack or vandalism.

2.1.7.1.3 Design Considerations
The application portal caters the IT services for ESIC project. A centralized infrastructure setup
is deployed at Delhi data centre to host the application. All the users connect to this data center
through ESIC network. A DR site is also at Hyderabad in high availability.
Centralized architecture, Consolidation, Security, Reliability and Availability are the most
important parameters in data center facility design. Factors like redundancy, simplicity,
flexibility and manageability are given importance for Operation and maintenance of the Data
Centre & DR Site.
Data center at the ESIC has:

- Multi-Service capability
- High Availability for production environment
- Scalability
- Reliability
- Security
- Flexibility
- Manageability
- Application Response time / Performance
- Cost Effectiveness

Data center has the provision to house current and future requirements..
Access: The access is adequate from the loading dock, and other support area entrances. It has
appropriate door sizes and negotiable corners, ramps and smooth floor surfaces inside the
facility. The access pathway to the Data center is 3' wide with the extension of the boundary
wall of the data center. Workstations area is separate for easy movement of the equipment's
into the Datacentre. In addition, it is important that proper access is provided in support areas
to allow for service or replacement of UPS, chillers and other large items.
The current data center facility have provision of Single door of dimension 2100 mm x 1200 mm
for equipment like Air conditioning units, electrical panel etc into the data center. The door is
kept closed and is not be used for regular access of data center facility.
Walls/Partitions: rigid floor-to-ceiling perimeter walls/partitions having 1-hour
fireproof rating.
Internal Partitions: Partitions inside data center built to the false ceiling height for
the same zone. Rigid floor-to-ceiling perimeter walls/partitions.
Wall Finishing: Internal walls are finished smoothly with emulsion paint.
Finishing of light colour is for the illumination of data center.
Doors: Double doors of dimension 1800 mm x 2100 mm with provision for peep
through glass of 4" x 10". The door is 1-hour fire rated and with secure bolted hinge. Provision for remote door release is available for the electric door locks.

**Thermal Insulator:** Thermal insulator is laid on the structural floor to prevent heat gain inside the data center. It also helps to save energy and to minimize the running cost of the air-conditioning. The junctions between the insulator and fixtures are watertight and airtight.

2.1.7.1.4 Room Layout and Planning

The current Data center is able to accommodate diverse hardware designs and requirements. The hardware areas is planned in such a fashion as to allow for seamless adaptation to the changing needs.

2.1.7.1.5 Power Sub System

**Primary Power Distribution (GRID):**

The Power subsystem is a very vital element for the Un-interrupted operation of the Data Center.

**Design Considerations:**

The primary power distribution for the Servers, Telco Equipment's, Fire Detection/suppression system, building access control, CCTV housed in the data Center is from the dedicated UPS.

**Raw Power Lighting Distribution Boards**

The LDB's for raw power lighting and Emergency lighting are located in the corridor in the x wing and labelled as LDBX. Raw power lighting distribution is drawn from LDB. Circuits are available in the current data center area. For additional circuit Requirement, spare MCB's in the LDBY is made use for DC expansions.

Emergency lighting distribution for the data center area and the access path is from ELDZ.

2.1.7.1.6 Lighting

**Normal Lighting**

Evenly distributed lighting of 500 LUX illumination is deployed for the datacentre. The distribution of lights with floor is aligned with equipment layouts so as to avoid shadowy areas caused by tall equipment, cabinets or racks. The lighting, sectional controlled by switches, gets switched off when they are not required.

3x18 W. Mirror Optics low glare light fittings is provide to achieve desired illumination level.

**Emergency Lighting**

The lighting inside data center is connected to raw power supply from LDB9 and LDB1D and 40% of them is connected to the emergency lighting distribution circuit at ELD. The emergency lights are located at the NOC area, mains control panel areas and passages leading to the main entrance and emergency exit.

2.1.7.1.7 Wiring

All the servers racks are individually wired through 3 core 4 sq.mm FRLS PVC copper conductor cable.

Panic push button is provided at suitable location to cut off the supply in case of emergency.
Main LT Panel
The panels are designed with electrical draw out circuit breaker and MCCB integrated with genet. All the feeders are provided with necessary safety relay and KWH meter for power consumed by the individual feeder. The panels have supply from two sources, so that the supply could be made available within 2/3 minute in case of failure of mechanical equipment with safety device. Maintenance work on this panel can be carried out without interruption of supply.
Main LT panel distributes raw power to the Data center facilities. The main LT panel is suitable for 3-Ph, 4-wire power distribution. The Main LT panel feeds power to the UPS input panel, Precision Air Conditioning Panel, and lighting circuits of the data center.

Earthing:
Earth pits location for the current data center is in front of the DC building at a distance of approximately 3 metres. A Dedicated ground wire is provided for the Computer equipment in the data center.

Un-Interruptible Power Supply
An Uninterruptible Power Supply (UPS) is installed to carry: n 100% of the computer hardware load for a period at least long enough to transfer the equipment to an alternate utility feed or back-up generator. On-line UPS that runs continuously is used as opposed to an off-line unit. The on-line UPS filters, conditions, and regulates the power. Battery back-up is capable of maintaining the critical load of the room for a minimum of 30 minutes during a power failure to allow for the transfer of power to an alternate feed or generator.

Earthing
Earthing is done to the under structure system in the access floor in the datacentre. The under structure system is properly connected to the building earth. For personnel safety and protection of equipment from damages and electromagnetic interference, a separated and insulated ground wire is provided for the computer equipment so as to achieve maximum 2 Volts between earth and neutral.

2.1.7.1.8 Air Conditioning System
Precision ACs is provided in the data center. The units are Independent and are neither utilized for, nor associated with the overall Building Unit. Floor insulation is carried out using arm flex make insulation of 20 mm thickness. This is required in order to prevent sweating in the floor below. The equipment placement in the racks is such that the cool air intake is from the front and hot air exhaust is from the rear/top of the racks.
Total Calculated Capacity of the Air conditioning equipment provided for the server room is 32 Tonnes. The equipment load is assumed 100 kW considering the full capacity of data center. It is deployed to provide x precision Air Conditioning unit of 8 Tonnes each, with one redundant unit of 8 TR capacity. Three units is located alternatively one opposite side in the data center area. The three units on each side operate in times sequentially mode. Two units on either side operate based on the population of the equipment rack in the data center and the other units are standby units. This provides 100% redundancy. As the equipment load increases, the cooling need also increases. With the maximum equipment load in the data center room the
calculated cooling capacity required is 32TR. During maximum equipment load units operate in time sequential mode and one unit act as a redundant unit. Air distribution method in the data center is usually through the Floor discharge method. The units discharge the air below the access floor and distributed through the air grilles or perforated floor panels. The heat dissipate vents of most computer equipment are designed to suit such distribution as it is efficient in air circulation.

2.1.7.1.9 Building Management System
BMS is very key element and ensure the controlled environment in DC. BMS provides central monitoring facility that all the subsystems & BMS are working in Tandem.

2.5.11 Fire Detection System
Fire Detection system is a First Hand safety Tool to detect the fire if present and raise an Alarm so as to initiate action.

The Detection system uses the following components and devices:
- **Ionization Smoke Detector**: Used for sensing smokes from non-smouldering fires (Thin Smokes) such as arising from combustion of Paper / Cotton / plastics.
- **Photo Electric Smoke Detector**: Used for sensing smokes from smouldering fires (Thick smokes) such as arising from combustion of rubber / PVC cables etc.
- **Heat Detectors**: Used for sensing the change in the temperature of the hazard, thus signalling a fire condition.
- **Manual Call Points**: Used for Manual Signal to the system of a fire condition.
- **Manual Abort**: Only inhibit discharge of suppression system when operated
- **Manual Release Station**: Manually discharges the suppression system when in conjunction with Fire alarm panel.
- **Isolator Modules**: Used for Segregating 2 separate zones in a given detection loop.
- **Relay Output Device (Control Modules)**: Used to Address as well as drive a NC Contact.
- **Hooter**: Used for generating an Audio Alarm in case of a fire situation at output 86-90dBA.
- **Fire Alarm Panel (FAP)**: control unit with modules to integrate with various building facilities.

Conventional Fire Detection System
In this type of detection system all the detectors are connected in series to a Main Fire Alarm Panel.

Analog addressable System
Unlike conventional alarm methods, these systems monitor and control the capabilities of each alarm initiating and signalling device through microprocessors and system software. In effect, each intelligent fire alarm system is a small computer overseeing and operating a series of input and output devices.

2.1.7.1.10 Fire Suppression System
For Mission Critical DATA Centres, Fire Detection is not the complete solution for Fire Protection. In case of a fire presence immediate action has to be initiated so as to avoid the impetus of a potential Fire Hazard and most important to maintain Business Continuity.
Fire Protection follows the empirical formula:

\[
\text{DETECTION} + \text{SUPPRESSION} = \text{PROTECTION}
\]

The areas that are provided for FM-200 gas based fire protection (Individual Flooding) are as below:

- Above the false ceiling
- Room void
- Below the false floor
- The gas is flooded in all the three voids in the area under consideration.

**Features of a Suppression Agent:**

- Quick acting.
- Reliable.
- High Shelf Life.
- Time tested and approved by Authority.
- Clean and safe for equipment.
- People safe.
- Environment friendly.
- Versatile enough to take care of all Classes of Fire.
- Long-term availability.
- Space efficient.
- No collateral damage to assets, which the system is meant to protect.

2.1.7.11 **Access Control System**

**Design Assumptions**

Security locking system is provided at the entrance of the data center. Electric door lock of the main entrance is capable of manual operation under all conditions.

- Burglar alarm is provided at the emergency exit.
- 24-hour security services to the premises
- Maintain updated lists of personnel who has been authorized to enter the datacentre
- Maintain logs/records for visitors
- Visitors or service personnel are well identified and escorted in the data center
- Permission for staying in data center is granted on job basis only.
- Backup power is provided for locking control system, security system, fire detection and suppression system.

The Access Control System control and monitor the access of the personnel entering the Data center area. Only authorized personnel with relevant access level are allowed to enter the Data center area. Access Control is computerized control over entry to any area that can be secured with a lock and key. Entry is only allowed to authorized people at authorized times. Control of who is allowed to come and go is easily maintained.

2.1.7.12 **Magnetic Card Reader**

The current Magnetic card reader installed is used for the current datacentre with magnetic swipe control, each person possess an ID card, which permit access to protected areas at authorized times. The card access system is linked to a microcomputer based system controller,
which allows or denies access. If an ID card is lost or stolen, or if a controller can be reprogrammed quickly and easily. The system access control has report capability. The system provides reports of all card activity, including whether access was granted or denied, and why

2.1.7.1.13 Biometrics
The second or higher levels of access control can be achieved using the Biometric devices - Thumb Reader is installed at DC and DR Locations
Note: During the emergence situation the response time of the biometrics devices is consideration for speed of Exist.

2.1.7.1.14 Closed Circuit Television (Surveillance System)
Design considerations
CCTV system exists with camera installed at Data center Main door and at entrance and exits doors of the building.
One colour camera is located at the data center main entrance. The monitor is located in the security room. It is monitored round the clock by the security personnel.
The current system to be checked to accommodate two additional camera for the current data center area.
System description:
The purpose of a Closed Circuit Television (CCTV) System is to ensure effective surveillance of an area and also to create a record of post event analysis. The system can also be effectively used for continuous on-line monitoring of events, if dedicated manpower is available and application demands. A CCTV System also acts as an effective deterrent for fraud and when used effectively helps detect the culprit.
The key components of the systems are as follows:

- Colour Indoor camera: located at strategic areas to capture video images.
- Multiplexer: accept signal from multiple cameras.
- Monitor: Is high resolution, min. 500 TV Lines, specially used for CCTV applications.

A CCTV System can provide on line display of video images on a monitor and records the images. The system is configured using CCD Cameras, Lenses, Multiplexer & a time-lapse recorder. Cameras at strategic locations using appropriate lens help to watch different areas. The video images from the cameras can be viewed using high resolution monitor through a multiplexer unit. A time-lapse recorder is connected to the multiplexer unit to tape all the events seen by all the cameras simultaneously on a standard 3Hr tape.
The Multiplexer unit records all the cameras at rapid succession of full-scale image. The system updates images every 0.64 seconds by employing video motion detection technology, Due to such high switching speed, chances of missing any incident are extremely remote. The resolution of the picture is very high as the recording is done as a full screen image.

2.1.7.1.15 Telco/ LAN Wiring
Design Considerations
Copper and fibre cables are used for horizontal cabling for servers to network connections. Gigabit Plenum UTP cable for laying in the data center Consider MMF for fibre cable laying in the data center.

2.1.7.1.16 Local Area Network Design for Data Center
The Local Area Network setup for Data center has been designed in accordance with the Structured Cabling guidelines for Data and Voice connectivity. The High Bandwidth Data connectivity has been provided to the Servers in the Server Farm and the NOC area. The voice connectivity also has been provided in the Server Farm area and the NOC area in the Data center for the intercommunication purpose. The WAN links are assumed to be available in the current communication room. All the components used in the LAN setup are Giga speed and Fibre.

Rack sizing and nos. of Networking Racks in Server room.
Each of the Networking Rack is of 42U height and floor standing open rack
Server racks
Rack sizing and nos. of Server Racks in Server room
Each of the server rack is of 42U height. Server rack of 600 x 1000 mm is provided in the server farm

2.1.7.1.17 Video Conferencing
Polycom CMA5000 used for Video Conferencing with Polycom VSX-7000
Key Features
It is end point agnostic and supports Video endpoints from other OEM’s.
Scheduling- Scheduling or ad-hoc calling for video, audio, Web and data conferences Ability to schedule conferences, book rooms and invite participants.
Management - Manages on-site and remote video systems, including statistics, directories, booking and software updates Intuitive web-based interface. Supports management of network and video equipment from multiple vendors Manages calls made on multiple protocols
Scheduling And Booking- SYSTEM BOOKING Book system and meeting room simultaneously Book recurring meetings and video resources Create, password protect, edit or delete booked conferences Add web or data conference to meetings Add/remove participants from reservation or connect/disconnect participants during conferences Connect conferences ad-hoc or pre-schedule connection Reserve resources for dial-in participants (telephone or video on ISDN or IP v.4 or IP v.6) Schedule point-to-point conferences or bridged meetings Lock conference, preventing new participants from joining. Invite participants by e-mail Customize meeting names
2.1.7.1.18 Desktop Virtualization

N-computing, the leading provider of desktop virtualization software and hardware, drastically lowers desktop computing costs, improves manageability, and reduces both energy consumption and e-waste. The N-Computing solution is based on a simple fact: today's computers are so powerful that the vast majority of applications only use a small fraction of the computer's capacity. N-Computing's virtualization software and hardware tap this unused capacity so that it can be simultaneously shared by multiple users spreading out the cost of the computer and typically providing four times the number of seats for the same money.

The N-Computing virtualization software works with standard Windows and Linux computers, and each user's monitor, keyboard, and mouse connect to the shared computer through a small and highly reliable N-Computing access device. The device itself has no CPU, memory, or moving parts so it is easy to deploy and maintain. The N-Computing solution does not have hidden costs and is supported by a global network that is committed to customer satisfaction.

Please refer to Product details on further details on N-Computing. For the solution current by Current Service provider, the overall Desktops for the solutions have been distributed as shown below. Desktops have been split Windows desktops, Linux Desktop sand N-Computing based
workstations.

### 2.1.7.1.19 EMS
ESIC is setting up an Enterprise Management infrastructure to enhance their application and infrastructure performance. They are looking to build this with tools which value add the current services provided. The tools current should easily integrate with the current ITIL processes and should provide a robust and automated workflow. ESIC is looking for an Enterprise Management Solution to manage current and current solution for managing the complete Network Infrastructure Server Infrastructure, real-time business views, Performance management and Service Desk Management.

Current Service provider has provided the following requirements:

- A scalable solution with Modular Architecture
- Central Monitoring and Management of ESIC Network infrastructure
- Graphical views of various entities like IP Segments, Critical Routers & Switches etc.
- Real-Time Topology Views
- Support for IP based Protocols
- Support SNMP & RMON communication standards
- Real-Time and Historical Data analysis
- Ability to receive alarms from third-party tools
- Ability to receive data from any SNMP Compatible device and element management tools
- Provision for future enhancements in a modular structure
Logical Diagram for IT Management in ESIC

Figure 25 — EMS
**Server Management** is deployed centrally at Datacenter and monitor Servers. The solution deploys intelligent agents for managing various servers, hardware, operating systems, web servers and databases. Agents are deployed using RPC DCE for secured communication protocol between the managed server and the management server. Database Management for Oracle/SQL is deployed to manage the oracle /SQL databases. As part of the solution, OS, Oracle/SQL, Web server SPI are deployed on managed servers. This server in high availability mode. Hence 2 servers is deployed in the central location using MS-cluster server.

**Network Management**

| Network Management | Management software for Networks | - Link availability of network elements  
|                    |                               |  
|                    |                               | - Discovery of Network  
|                    |                               | - Real Time Bandwidth Utilization  
|                    |                               | - Topology creation  

**HP Network Node Manager**
Network Management software is deployed to manage ESIC network devices. This monitor using SNMP communication between the managed node and the management station. Software is configured to discover & monitor 5500 Network Devices in a distributed architecture. Master server is installed at a central location. All devices in central location & around are monitored by this master server. NNM run in MS-CS mode (master server — collector server) mode. And have 1 Collector in sub locations or intermediate site. Every Collector server is licensed with adequate node monitoring capacity. This server replicated to Network Manager Server in DR location using MS-cluster server.

Performance Management

<table>
<thead>
<tr>
<th>Performance Management software</th>
<th>Infrastructure Management Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Capacity Planning</td>
</tr>
<tr>
<td></td>
<td>Historical Trending reports</td>
</tr>
<tr>
<td></td>
<td>Predictive reports of Network and server</td>
</tr>
</tbody>
</table>

HP Performance Insight

Performance Manager is deployed to collect performance data from agents and SPI's developed on each managed node and network devices. Many out of box reports are available for each type of application being managed. Performance Management is deployed for Network Infrastructure performance and capacity planning. Performance server have 3 pollers station servers in sub locations or intermediate site. This server id not included in the High availability

Desktop Management

<table>
<thead>
<tr>
<th>Desktop Management</th>
<th>Desktop Software</th>
<th>Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Software distribution</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Asset Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Patch Management</td>
<td></td>
</tr>
</tbody>
</table>

Desktop Management for Desktops is deployed to provide the following functionality:

- Software Delivery (User Self Service)
- Inventory Manager (Asset)
- Usage Manager
- Patch Manager

Desktop Management is integrated with Directory service for defining a policy for OU based software entitlement. Agents is centrally deployed using active directory, however all desktops
have to be configured for prerequisites prior to deploying the agents.

**Integrated Solution**
Following are the integrations involved in the solution:-

- Performance Management with Network Management
- Network Management with Server Management
- Server Management with Service Desk Management for automatic ticket logging
- Desktop Management with Service Desk Management for maintaining assets in CMDB

**2.1.7.2 End User Location – New Requirement**
Minimum Technical Requirements Specifications –Hardware

**11.2.7.2.1 Indicative LAN Diagram**

Connectivity at HO, RO, ESIC Hospitals, SD, State Govt. Hospitals and Model Hospitals
Note: Annexure 02 to 06 contain details of Desktop, Printer/Scanner/Photocopy, Desktop UPS, Wireless Access Point, Router - BO & Dispensaries, WAN Switch, Router, Network Switch, LAN Switch, Router – BO & Dispensaries, VOIP Phones (A. Basic IP Phone, B. Advanced End Point Video Phones)

2.1.8 Security Architecture

2.1.8.1 Software Security Architecture
This section describes the security features included in the current architecture.
• **Feature 1 - External Firewall:** When the internet connectivity becomes the bottleneck in the overall solution the suggested architecture does support adding additional ISP Link to provide more bandwidth. The additional can be driven by the same Firewall and Web Proxy Server - which is scale-up architecture or additional set of Firewall and Web Proxy Server (Web Proxy Server) - which is scale-out architecture.

• **Feature 2 - Proxy Server:** The Presentation tier is also very scalable. By adding more servers into the farm makes the presentation tier to scale out the load or by adding more processing power or memory makes the presentation tier to scaled-up.

• **Feature 3 – Open SSO Server Authentication & Authorization:** The ESIC portal is protected with – Open SSO Server based Forms authentication and authorization. Open SSO Access Manager Authentication and authorization allows only authorized users are able to login and access the designated section/subsection of the portal based on their profile. All the users access the applications only after user authentication and authorization. Access Manager Authentication and authorization also offers content personalization functionality.

• **Feature 4 - Internal Firewall & DMZ Zone:** Connections from the internal and the external network to the DMZ are permitted, but connections from the DMZ are only permitted to the external network which protects all the internal information stored in the database, business logic components, etc. Hosts in the DMZ may not connect to the internal network.

• **Feature 5 – Authentication & Authorization:** The extranet portal & Intranet portal are protected with Open SSO Federated Access Manager backed by Sun Directory based Authentication and Authorization. Standards based Authentication and Authorization allows only authorized users are able to login and access the designated section/subsection of the portal based on their profile. All the users access the applications only after user authentication
and authorization.

**Feature 6 – Sun Directory: Server** and Access manager provides the means to manage the identities and relationships that make up your organization's network. Integrated with Identity Management, provides functionality needed to centrally configure and administer system, user, and application settings. With Open SSO, you can simplify user and computer management, enable single sign-on (SSO) access to your network resources, and help enhance the privacy and security of stored information and communications.

**Key Security Features of Open SSO and Sun Directory Server are:**
Sun Open SSO Enterprise is used to address the three primary issues associated with balancing risk and reach.

1. **Access Management**
2. **Federation**
3. **Secure Web Services**

**Highlights**
Single, comprehensive solution that solves single sign-on (SSO) challenges for internal applications, internal Web services, SaaS applications, partner services, affiliate services, business process outsourcing, third-party hosted portals, and more. First integrated solution for managing SSO, authorization, and personalization in Web, federated, and Web services environments. Fast, lightweight federation enables identity providers and service providers to connect in minutes.

- 100% Pure Java TM for ease of deployment on the broadest range of operating systems
- Simplest solution in the market to configure and deploy, with no installer necessary

**2.1.8.2 Basic Open SSO Enterprise Architecture**
A list of the components that comprise the architecture are:

**Sun Open SSO Enterprise**
Instances of Open SSO Enterprise provide the core functionality. Each instance is configured with its own embedded configuration data store. Configuration data includes information about services, administrative users, realms, policies, and more. User data is accessed through a single load balancer deployed in front of two instances of Sun Java System Directory Server.

**Distributed Authentication User Interface**
The Distributed Authentication User Interface is a component of Open SSO Enterprise that provides a thin presentation layer for user authentication.

**Process Rights Management**
In the Solaris software, administrative tasks that previously required super user rights are now protected by process rights management. Process rights management uses privileges to restrict processes at the command, user, role, or system level. A privilege is a discrete right that a process requires for performing an operation. The system restricts processes to only those
privileges that are required to perform the current task. Therefore, fewer root processes are vulnerable to exploitation. As installed, the Software Express releases and the Solaris release are completely compatible with previous releases of the Solaris Operating System in terms of the privileges enhancements. Unmodified programs that run as root run with all privileges.

Policy Control and Management
Sun Java System Federated Access Manager is Sun's commercial version of the Open SSO project, and an identity and access management solution to extend security for Web and Java applications to federated environments and Web services security -- with a single product.

• First and most complete identity-based solution for managing authentication and authorization in web, Java, federated, and Web Services environments
• Scalable to millions of users

Key Features
• Web SSO Enables users to sign on once and get access to all the resources to which they are entitled
• Provides centralized control over application security
• Protects applications by using policy agents to enforce rules- and roles-based authorizations
• Pre-integrated with ESSO solutions for rapid, efficient access, advanced password reset and secure password management
• Federation Extends core authentication and authorization services with partners via standards-based security assertions (including SAML and ID-FF)
• Creates a seamless, simple sign-on experience
• Simplifies the process of managing federated partners with robust web-based administrative tools
• Works seamlessly with Sun Java System Federation Manager to extend authentication and authorization capabilities across service provider partners who have deployed basic access management capabilities
• Identity Web Services Provides tools and functionality needed to secure Web Services
• Creates Trusted Authorities that allow Web Service providers and consumers to exchange secure messages
• Integrates with Java developer tools to build identity-based security directly into applications and services
• Ease of Integration - As a founding member of the Liberty Alliance, Sun has helped create and deliver interoperable standards and guidelines for federated identity management

Rights Management Services:
In Solaris 10 the project.max-locked-memory and zone.max-locked-memory resource controls can be used to limit the memory consumption of processes that are assigned the PRIV PROC LOCK MEMORY privilege. This privilege allows a process to lock pages in physical memory.
If you assign the PRIV_PROC_LOCK_MEMORY privilege to a rights profile, you can give the processes that have this privilege the ability to lock all memory. As a safeguard, set a resource control to prevent the user of the privilege from locking all memory. For privileged processes that run in a non-global zone, set the zone.maxlocked-memory resource control. For privileged processes that run on a system, create a project and set the project. Max-locked-memory resource control.

Metro stack has XACL support. It provides:
Role-based access control
Mandatory access control
Discretionary access control

PERMIS: PERMIS is a sophisticated policy based authorisation system that implements an enhanced version of the NIST standard RBAC model Sun Microsystems implementation of the OASIS Open Extensible Access Control

Mark-up Language (XACML) Standard. The implementation is written in the Java programming language. XACML, is an approved OASIS Open standard, is an XML-based language for access control. XACML describes both an access control policy language and a request/response language. The policy language is used to express access control policies (who can do what when). The request/response language expresses queries about whether a particular access is allowed (requests):01 and describes answers to those queries (responses). XACML contributes to the simplification and cost reduction of developing and deploying secure web services or any application that requires secure access control. The Sun project provides complete support for all the mandatory features of XACML as well as a number of optional features. Specifically, there is full support for parsing both policy and request/response documents, determining applicability of policies, and evaluating requests against policies. All of the standards attributes, types, functions, and combining algorithms are supported, and there are APIs for adding new functionality as needed. There are also APIs for writing new retrieval mechanisms used for finding things like policies and attributes.

File Integrity and Secure Execution
System administrators can detect possible attacks on their systems by monitoring for changes to file information. In the Solaris 10 OS, binaries are digitally signed, so administrators can track changes easily, and all patches or enhancements are embedded with digital signatures, eliminating the false positives associated with upgrading or patching file integrity-checking software.

The Solaris 10 OS also introduces the Basic Audit and Reporting Tool (BART), a file integrity-checking application for data files and customer applications. The BART utility allows a customer to create snapshots of their own data, applications and critical system files and periodically scan for changes to these files. Additionally, the Solaris Fingerprint Database project, hosted by Sun on the Sun Solve Web site, provides digital fingerprints for all files shipped in the Solaris OS, spanning many previous generations of the operating system. The Solaris Fingerprint Database offers free online verification utilities that allow you to check the integrity of Solaris files on any current system to ensure that no hacker has modified critical system files. Used individually or together, these file integrity tools provide powerful, flexible ways to monitor for changes to your operating system platform.
based operating systems, applications and users often need administrative access to perform their jobs. However, most implementations offer just one level of higher privilege: root or super user. This means that any user or application given root access has the ability to make major changes to the operating system—and is typically the target of hacking attempts. The Solaris 10 OS offers unique User Rights Management (also known as role-based access control, or RBAC) and Process Rights Management (also known as privileges). Together, User and Process Rights Management technologies reduce risks by granting users and applications only the minimum capabilities needed to perform their duties. Unlike other solutions on the market, no application changes are required to take advantage of these security enhancements. Solaris also offers protection against 'buffer overflow' attacks as well as an extensive audit trail that can be exported into common XML format for further analysis.

**Network Service Protection**
The Solaris 10 OS ships with Solaris IP Filter firewall software preinstalled. This integrated firewall can reduce the number of network services that are exposed to attack and provides protection against maliciously crafted networking packets. Starting in Solaris 10 8/07, the IP Filter firewall can also filter traffic flowing between Solaris Containers when it is configured in the Global Zone. In addition, TCP Wrappers are integrated into the Solaris 10 OS, limiting access to service based allowed domains. Solaris also provides protection against attack through its Secure by Default networking configuration. When configured in this manner, a Solaris 10 system retains a usable GUI interface, can browse the Web, send Email and do other outbound communications. Only the Solaris Secure Shell encrypted remote access method is allowed for inbound communication.

**Cryptographic Services and Encrypted Communication**
For high-performance, system-wide cryptographic routines, the Solaris Cryptographic Framework add a standards-based, common API that provides a single point of administration and uniform access to both software and hardware-accelerated, cryptographic functions. The pluggable Solaris Cryptographic Framework can balance loads across accelerators, increasing encrypted network traffic throughput, and it is available to applications written to use Public Key Cryptography Standards (PKCS) #11, Sun Java Enterprise System, NSS, Open SSL, and Java Cryptographic Extension software. Starting with Solaris 10 8/07, the Solaris Key Management Framework is introduced to assist in managing digital certificates. The Key Management framework provides a single set of administrative commands for digital certificate creation requests, manipulation and loading across the most common formats. Solaris also provides protection against theft of all material by encrypting communications using the IP sec/IKE and Solaris Secure Shell protocols. Solaris IP sec /IKE complies with industry standards to provide encryption of data between two or more systems over the network without any application modification at all.

The Solaris Secure Shell protocol is a specific set of utilities that have been modified to allow for encrypted remote access and file transfer between two systems.

**Flexible Enterprise Authentication**
The Solaris 10 OS delivers a number of flexible authentication features. At the foundation of Solaris is support for Pluggable Authentication Mechanism (PAM), which make it possible to
add authentication services to Solaris dynamically. Sun and third party vendors provide many PAM modules and customers can create their own to meet specific security needs. The Solaris Kerberos Service delivers Kerberos-enabled remote applications such as rsh, rcp, telnet, Solaris Secure Shell, and NFS file sharing. Kerberos-based protocols allow for enterprise single sign-on (SSO), authorization and encrypted communication. Lightweight Directory Access Protocol (LDAP) client-side authentication one interoperability enhancements enable enterprise-wide, secure, standards-based authentication to your servers and applications, All Solaris User and Process Right: management information can also be stored centrally in through the LDAP-based directory server, allowing for centralized management of users and security role definitions. Local passwords have strong password encryption options, including MD5 and Blowfish, as well as account lockout, password history and complexity checking, and a banned passwords list. By providing strong password encryption, systems are less subject to successful password cracking should a password file ever be lost or stolen.

**Repeatable Security Hardening and Monitoring**

New features in the Solaris 10 OS make it easier than ever to minimize and harden a system. The Reduced Networking Meta cluster install option creates a minimized Solaris OS image, ready for administrators to add functionality and services in direct support of their system's purpose. As mentioned previously, Solaris 10 now includes a Secure by Default networking configuration that disables many unused network services, while configuring all other services for local system-only communications. The freely available Solaris Security Toolkit assists in the process of installing and maintaining a minimized and hardened operating system security configuration. The Toolkit also includes an audit mechanism to compare a running system configuration against a site-specified hardening profile. In this way, the Toolkit can be used to both verify and enforce compliance with an organization's OS security standards.

**Mandatory Access Control and Labelling**

If your system requirements include privacy, increased accountability, and reduced risk of security violations, then Solaris Trusted Extensions is for you. As a standard part of Solaris, true multi-level security is available for the first time in a commercial grade operating system that runs all your current applications and is supported on over hundreds of x64/x86 and SPARC platforms. Mandatory Access Control is enforced in Trusted Extensions by the use of User and Process Rights Management as well as Solaris Containers, which have an information sensitive label applied to them. Customers can quickly configure new labels, which protect files, networks, applications and users against inappropriate access, without writing complex, error prone security policy files.

**2.1.8.3 Infrastructure Security Solution**

Security is designed to provide highly secured environment and to protect & secure mission critical data.
- Firewall in HA mode is used for parametric security device
- IPS in HA are positioned to secure traffic up to layer 7
- All the traffic pass through Anti-Virus server to check for any virus attack malicious content.
• The mail traffic pass through Anti-Spam server to protect from mail virus and spams.
• LDAP authentication is current for centralized authentication.
• Identity management manage the identities of users.
• From the security perspective the traffic at datacentre is divided into different security zones at firewall and at core switches using VLAN.

Network and Application Security
Network security is ensured by positioning Radware DefensePro-1020 in the network. Defence Pro blocks all malicious traffic entering the Datacentre and affecting the network and application resources. High volume DOS attacks, Mass propagating worms and virus, scanning attempts are mitigated and the perimeter of the network itself. ESIC network has a multi-layered security built to provide comprehensive security to Application Infrastructure. The first level scanning and mitigation is done at Perimeter and more specific Application level malicious traffic scanning and mitigation is done at the second layer. DefensePro-1020 fronting the Servers at all the Zones blocks critical worms, Virus, Backdoors, Trojans, SYN flood, protocol anomalies, server cracking, DOS/DDOS and evasion techniques which can adversely affect the availability and performance of Applications hosted. It also detects and blocks the SSL attacks.

Deploying Defence Pro at the Network Perimeter & MZ zone
Defence Pro can be used to protect network from attacks launched within SSL traffic by deploying an AppXcel SSL Accelerator in conjunct with Defence Pro.

DefensePro Advantages:
• Scalable Up to 3-Gigabit Speed Security Switching
  Inline, high capacity, dedicated security switching with String Match' engine accelerator delivering 3-Gigabit application security performance.
• High-Port Density
  DefensePro provides the highest port density in the industry with up to 11segments protection in a single box, enabling high capacity scanning across multiple network segments with a single device.
• Complete Application Security
  DefensePro performs bi-directional, State full, deep packet inspection and accelerated signature matching to immediately block hidden worms, viruses, Trojans and intrusions. Providing multi-Gigabit speed protection for over 2,000attack signatures with 24x7 security updates, DefensePro ensures continuous application security.
• Real-Time DoS/DDoS and SYN Attack Protection
  Offering multi-Gigabit Denial of Service/DDoS protection, and advanced SYN flood protection for known and unknown SYN floods, safeguarding networks against Denial of Service attacks.
• Adaptive Behaviour-based Protection
  • DefensePro uses adaptive behavioural analysis capability to provide zero day protection from Denial of Service attacks without any human intervention. The automated, self-learning mechanism proactively scans network traffic for anomalous traffic patterns; when it detects an attack, it characterizes the attacks specific behaviour, establishes filter criteria and executes the appropriate countermeasure. A Close Feedback mechanism dynamically changes the filtering criteria according to the ongoing development of the attack, accurately mitigating the damage
caused by these highly sophisticated attacks.

- **End-to-End Traffic Shaping and Optimization**
  Dynamic traffic shaping ensures the continuity of mission critical applications by controlling end-to-end bandwidth to guarantee Service Levels. By dynamically controlling bandwidth, DefensePro proactively isolates attack impact, preventing spread to users and applications while ensuring complete continuity of all unaffected and secure mission critical applications.

- **P2P Traffic Control**
  Controlling the bandwidth usage of P2P applications enables alignment of bandwidth use with business priorities and eliminates temporary and expensive link capacity upgrades. In addition, it reduces the propagation of worms and viruses via P2P applications.

- **Security Update Service**
  The Security Update Service (SUS) delivers automated weekly and emergency attack signature filters for subscribers, ensuring up-to-date protection against current and emergent application vulnerabilities.

- **Centralized Security Management**
  Configware Insite enables a centralized set-up, configuration and attack signature updating across multiple DefensePro devices from one central console for unified management of application security.

### Security Flow Management Antivirus and Antispam Flow Control Manager

Deep emphasis has been given in building security inside the network. While Intrusion prevention systems have patched all vulnerable points sufficient focus has been made for State full inspection and access control using multiple layers of Firewalls. At the same time more specific content level scanning products like Antispam, Antivirus URL filters are positioned at appropriate points to ensure content level scanning, blocking and access.

In this secure infrastructure Radware's Content Inspection Director (CID) ensure high availability of all security devices in the network like URL filters, Antivirus, Antispam Filters and proxy servers. Also they ensure even distribution of traffic across these solutions. Antispam and Antivirus to optimize performance. A critical functionality of provision user level scan policies is also provided by CID. Radware's CID takes the ownership of managing flow of traffic for each user/group across security devices for scanning before it is delivered to the destination.

Deploying Content Inspection Director the flow of traffic to the security devices and to ensure high availability & accelerated performance Content Inspection Director simultaneously load balance Antivirus Gateways &Proxy/Cache servers. Content Inspection Director act as CENTRALIZED station for SECURITY POLICY ENFORCEMENT, it have policies on Source/Destination, IP subnet URL, Content etc to redirect on required traffic for scanning, files like gif, jpg, mpg that can never have any malicious content is send directly without overloading the security appliances, this way CID enhances the performance of these devices by manifold.

CID with FLOW-CONTROL dynamically load-balance the traffic first to Antivirus servers/Anti spam & then to Cache/Proxy servers. ID perform pre-screening of traffic & Files like jpg, mp3, Avi etc that are not reported to have any virus or malicious contents is forwarded directly to Internet. These files are 50% of the Internet Bandwidth & thus by bypassing these traffic AV
server performance increases.

**Content Inspection Director Advantages:**

1. The Content Inspection Director solution ensures any vendor Security device working in ACTIVE-Active mode as FARM/Cluster as AV/Content Inspection dynamic load balancing to make them Active-Active (in a very unique way, different technology like TREND for Antivirus/Antispam etc.
2. CID with FLOW-CONTROL dynamically load-balance the traffic first to Antivirus servers/Anti-spam and then to Cache/Proxy servers.
3. CID performs pre-screening of traffic & Files like jog, mp3, Avietc that are not reported to have any virus or malicious contents is forwarded directly to Internet. These files are 50% of the Internet Bandwidth & thus by bypassing these traffic AV server performance increases by as high as 500%.
4. Scalable solution and always remains as the part of your network, it’s never a dead box.
5. Central management, reporting and control by our management tool called APSoluteInsite. All other management features like CLI, SSH, Telnet etc can be done.

**DMZ (De Militarized Zone)**

- De Militarized Zone is created at HA internet firewalls
- The traffic passes through different security checks —
  - Firewalls
  - IPS
  - Anti-Virus & Antispam Servers
- After proper scanning this traffic is sent for authentication in secured zone

**Authentication Zone**
• Authentication zone is created as a separated zone on secured layer of core switch behind firewall.
• All the traffic has to pass through authentication servers before entering secured militarized zone.
• LDAP servers are used for authentication of traffic.
• LDAP servers are configured as primary & secondary server to provide high availability.
• Traffic is allowed to access application only once it is authenticated.

**Management Zone**

Technical Proposal — Current Service provider Solution

• The zone caters to the management of ESIC IT Infrastructure
• CS-Mars do the logging and event correlation
• EMS & NMS suite are positioned here
This is most secured zone, only trusted traffic can enter this zone.
Internet users have to pass through firewall & IPS defense before getting access to this zone.
Core application servers are places in MZ zone
Main Database server farm is placed here with connectivity option to fiber channel.
Centralized storage is also a part of this zone.
SAN is configured in HA mode.
Centralized backup library & backup is also placed in this zone.
All the packets is scanned, filtered & authenticated before forwarding to application servers in secured Militarized zone.

EMC CLARIION CX4 Series Storage Solution:
The Clarion CX4 series delivers midrange storage with the fourth-generation CLARIION CX storage platform. The unique combination of flexible, scalable hardware design and advanced software capabilities enables EMC CLARION CX4 series systems to meet the growing and diverse needs of today's midsize and large enterprises.

The Value of the Current Solution
The Clariion CX4 series offers new levels of capacity and performance, making it a superior solution for various types of applications - from databases and email/messaging backup-to-disk, video streaming, and replication, to large-file applications such as seismic data analysis and genome sequencing. Time, Resources, Risk, and Cost - An investment in this EMC solution reduces the resources required to manage your information assets. EMC’s investment in Research and Development and System Integration ensure that the solutions you implement work as expected right from the start. Your investment in EMC enterprise storage solutions delivers rapid return on investment.

ESIC has CX4-480 with 6GB cache to start with, CX4-480 can seamlessly upgrade to the highest model available in CX4 family i.e.CX4-960 with 32GB of total cache.

Architecture

SAN Storage Array
- EMC Clarion CX4-480 SAN Storage with 42 TB of total usable space of which 18 TB is on 4500GB 15K RPM 4Gbps Fiber channel disk drives for all applications and databases including mail and 10TB of usable space on 1TB STA-II for biometric application & data. An additional 14 TB has been configured for one clone and 2 snapshots
- EMC Clariion CX4 has dual Active-Active Storage Controllers, 6 GB of total cache
- It has redundant Power supplies, FANs, Hot swappable Disk Drives.
- The Front End ports are combination of FC and iSCSI for higher scalability and flexibility for optimal usage of SAN array. Currently it is configured with 4FC and 4iSCSI ports.
- Mirror View/ Asynchronous software for remote replication and Snap View has been
configured. Replicating SQL logs and file data.

- For iSCSI connectivity, CX4-120 has got 4 iSCSI ports, which can be connected to any LAN switch dual path from each SP. The server connecting through iSCSI must have NIC which has iSCSI initiator installed on it.

**SAN Switches**

- EMC DS5300 Connectrix SAN Switch has been proposed with 80 universal ports (48-ports base with 32-port incremental) for SAN connectivity at the primary site with a switch level redundancy. At the DR side a similar set of switches have been offered but with 48 ports. This is because the number of servers with san connectivity at the DR site is lower.

**EMC Networker Backup software**

For backup EMC networker backup software has been provided and be used to automate the backup process and backups taken on tape library as per the backup schedule and policy. EMC Networker backup and recovery software centralizes, automates, and accelerates data protection across your IT environment. Networker has set multiple world records for fastest backup and recovery performance, and continues to be the fastest backup application in the market today. IT departments can leverage Networker to unify all application, tape- and disk-based backup and recovery solutions, including next generation technologies such as source and target based data de-duplication, Continuous Data Protection, and Data Protection Management for different levels of information protection through common application control and management.

### 2.2 Overall Service Deliverables

The following section details the various deliverables for managing the different technology domains within ESIC solution.

#### 11.3.1 Server Management

It covers all Intel and RISC (HP UNIX and IBM AIX) Servers in the Data Center, Disaster recovery centre and other offices.

**Current Service provider delivers the following:**

**24*7 Monitoring of Critical Parameters, not limited to.**

- System Availability
- Critical Services Availability
- Disk Space

- Memory Utilization
  - CPU Utilization
  - Critical errors in the system logs, as applicable
  - I/O Utilization

**Incident & Problem Management:**

- Orderly start-up and shutdown of servers
• Co-ordinate with vendors in case of problems arising due to hardware failures or otherwise, in which case the involvement of the vendor or principals is required
• Reinstallation of OS, arising due to incidents of OS crashes or problems where a reinstallation is required
• Trends on the incidents / problems
• Recommend on the possible solution! Workaround to address the probable causes of failure.

**System Administration Tasks:**
• Creating and managing domains
• Creating and managing volumes
• Assign Protocol addresses
• Manage Multiple interfaces and IP Addresses
• Manage Clusters
• Manage Access rights & Folders

**User Management Services:**
• Creation of new users and deletion of existing users on request.
  • Create and maintain users groups
  • Create and maintain users profiles
  • Create login and logon scripts
  • Assigning and Maintaining user access rights as per policies
  • Assign and maintain space usage restriction
  • Configuring and maintaining print servers and print queues

**Regular housekeeping tasks:**
• Install software, patches, updates and service packs on the servers
• Monitor CPU, disk, memory and I/O parameters
• Verify logs in event logger and periodically clean up log files
• Schedule and optimize the services running on the server
• Ensure all critical services are running on the server

Maintain list of all system files, root directories and volumes
• Take back up of the file systems
• OS performance tuning

**Release Management:**
Follow the Release Management Process and deploy OS patches and Security Patches. The Release Process would follow a Plan, Test and Roll-out strategy as defined in the Change and Release Management Process
• Maintain the Complete Configuration Information of the Servers
• Assist ESIC to define standard naming convention policies

**Security Administration Tasks:**
Security management — Configuring Account policy, Access rights, Password control
• Load latest anti-virus updates on the server, manually if central server failed to update
• Monitor access and security restrictions on the Production Servers
• Restricted access to Business Applications
• Hardening of the Operating Systems as per baseline agreed upon.
• Security Audit for Unauthorized User access to the Production Systems
• Log File Analysis for abnormalities in Security Log of Production Systems
• Periodic Intrusion Detection over vulnerable ports in the servers

ESIC deliver the following:
Definitions of access rights and necessary approvals for the changes in the same
• Necessary Approvals for Changes
• Defined policies as agreed upon mutually
• Space usage restriction definitions

11.3.2 Backup and Restore Management
Scope & Deliverables
This service covers all the designated servers which is identified for backup and has a policy defined for the same and deployed at ESIC locations (DC, DRC, Hospitals, offices etc).

Current Service provider delivers the following:
• Ensure daily backup of all critical data
• Labelling of backup media and log maintenance as per the policy
• Periodic monitoring by Operations Manager to ensure that all tapes have data and can be restored successfully.
• Review backup logs to verify successful completion of backup
• Notification to ESIC team on any backup failures
 • Perform restoration drill as per the schedule and sign off with ESIC
 • Current Service provider adheres to the backup strategy for ESIC, based on the business requirements, after the approval for ESIC.
 • Tapes, cartridges and related paper documentation are stored in accordance with ESIC's requirements and the business continuity and business resumption plans.
 • Current Service provider provides routine backup and recovery of data with respect to the IT Infrastructure so as not to adversely impact scheduled operations and to maximize availability of the Services, including by performing regular backups of all designated servers.

11.3.3 Mail and Messaging Management Services
Scope & Deliverables
It involves managing the existing mail messaging system.

Current Service provider delivers the following:
24*7 Monitoring of Critical Parameters, not limited to:
• Mail Queue Length
• Mail Services Status
• SMTP Gateway Status
• Mail Server Disk Management
• Mail DB Size

Incident & Problem Management
• Tracking and Co-ordination of all incidents / problems till resolution.
• Trends on mail and messaging incidents / problems

User Administration Services
• New Id Creation for Mails / Web Access
• ID Transfer / Re-certification / Rename / Deletion
• Client Setup
• Enabling Web access of mailbox
• SMTP Access
• Password Resets
• Mailbox Quota Management

System Administration Tasks
• Creation / Deletion / Change of Site / OU / Domain
• Fragmentation Check for Mailbox/ Mail Folders
• Compacting / Cleaning of the DBs
• Schedule Replication between Sites

Security Administration Tasks
• Permissions for Shared Mail folders
• Access Control on the Gateway systems
• Content filter setup at the Anti-spam systems
• SMTP Dot forwarding, as applicable

Capacity & Availability Management
• Analysis of the Usage of the Mail and Web Application over a period of time and recommendations to ESIC to consolidate, restructure, divestiture, realign the setup so that the existing setup is used efficiently.
• Analysis of the performance of the application over a period and recommendations for upgrade / migration to latest technologies
• Reporting on the usage of the application by the users and recommend necessary action
• Reporting on the SPAM control effectiveness

Anti-Spam Management (once it is setup)
• Anti-SPAM Filters setup, configuration and monitoring
• Periodic updation of the signature files for latest controls
• Enable on-demand filters for file extension, Manage Exclusions
• Recommend industry best practices for Spam Control

11.3.4 Security Management Services
Scope
The service caters to the overall security setup of ESIC. The service caters to management of the individual devices at the perimeter layer and also the management of the Critical servers
and databases from a security aspect. ISO 27001 latest standards are followed for DC and DRC. The devices covered are

- Firewall Servers
- IDS/IPS, as applicable
- Antivirus Servers
- Anti-Spam System
- Perimeter Routers
- Critical Business Servers

**Current Service provider delivers the following:**

**24x7 Proactive Monitoring:**
- Availability of Firewall / IDS / Critical Systems / Perimeter Network Devices / Monitoring for the security device health, performance, availability, capacity/ Monitor Logs of the devices mentioned in scope
- Escalate Firewall / IDS alerts due to policy violations

**Policy Deployment / Hardening**
- Understanding the ESIC’s firewall / IDS setup and fine tuning the firewall policy after getting policy sign-off from ESIC
- Suggest new policies
- Make policy changes
- Implement global policies.
- Patch updation and signature pattern updation required for firewall LIDS
- Password Policy Enforcement
- Server and Database hardening, as applicable
- Application of Security patches for OS / DB and other Applications
- Rigorous Change Management with respect changes to the Firewall and IDS

**Security Incident Response**
- Respond promptly and quickly once the alert is validated and a threat is identified
- Notify the key resources in ESIC on the threat or the Intrusion
- Fault & Recovery Management
- Corrective actions

**Trend Based Consulting**
- Threat Assessment
- Ongoing advice on any proposed changes in the internal network based on security implications.

**Management Tasks**
- Management of any NAT, Port Changes, Policy Changes
- Daily Backup of the Firewall /IDS Policy database & the objects

**Password Management**
- Assist in building a structured password policy for the OS, DB and the Applications
• Implement the password policy (as applicable) using the native tools of the servers

Central Antivirus Server
• Managing the Central Antivirus Server(s), if applicable
• Discovering Desktops and Servers on the Antivirus console
• Maintaining the configurations of all desktops reporting to their respective primary and secondary servers
• Updation of Virus definition files
• Scheduling virus definition updates from the Master server to primary and secondary servers

Regular Management Tasks
• Managing the servers and desktops from the centralized Antivirus console
• Scheduling and performing Antivirus sweep scans across all assets
• Taking precautionary actions in terms of definition file updates and interim solutions released during the high alert situations
• Troubleshooting virus related incidents
• Escalation and coordination with principles for problem resolution

Notification to ESIC
• Alerting and notifying the users in ESIC about new viruses and its impact
• Sending Newsletters on the latest trends and vulnerabilities relevant to ESIC Setup

ESIC deliver the following:
Necessary Approvals for Changes

11.3.5 Storage Management Services
Scope
The service caters to the SAN / TLD and other storage boxes located in the ESIC Datacenter.
Current Service provider delivers the following:

24X7 Pro-active Monitoring
• CPU Utilization
• Uptime Statistics
• Volume Usage Statistics
• Snapshot Usage Statistics
• CRC errors, as applicable for network based storage devices.
• Tape Errors & Auto loader errors
• Error log of Tape Libraries (as reported in the backup software)

Fault/Incident/Activity Management
• Performing online storage tuning.
  • Assigning and initializing online storage volumes as required.

• Managing the archiving of inactive files and reporting on online storage directories for review by Operations and DBA team
• Conducting routine monitoring using Software tools to measure the efficiency of online
storage access and taking corrective action as needed (including performance adjustments to Equipment and Software, or file placement as required to maximize service).

**Storage Administration Tasks**
- Configure Port setting
- Configure Port zoning
- Add, delete and modify RAID configuration
- Add, delete and modify file system configuration

**Security Management Tasks**
- Configuration of Volume with relevant user rights and permissions after a complete change management cycle
- Management and Audit of the usage of the volumes by the assigned users

**Storage Performance Management**
- Based on 11/0 pattern statistics & performance data Current Service provider monitor, manage & control online storage & make necessary changes in overall storage architecture in conjunction with ESIC to meet the Service Levels. Current Service provider configure & allocate the required storage capacity to the end users based on the approved change requests for configuring / reconfiguring storage volumes

**Catalogue Management**
Current Service providers monitor (using Tools) & maintain the catalogue information based on:

- Storage allocation
- Storage utilization
- User directories & files
- Access pattern & history (helps in managing archiving of inactive file)

**Administration**
Monitoring user directories for file inactivity and reporting monthly.
Monitoring and maintaining file directories and catalogues.
3 Providing online storage compaction as needed and as possible within production processing schedules.
- Providing data migration/archive management.

**Backup Storage Media Management**
Current Service providers use the management console through terminal services or web to access the storage server to verify the status and quality of the tapes.
The media retention policy be jointly developed in consultation with ESIC teams, Current Service provider team and the application team. Current Service provider adheres to the defined policies.
- Current Service provider use the Reporting capabilities of the existing Storage management server to generate relevant reports like media quality report, usage report, capacity reports etc.
11.3.6 Network Management Services

Scope
Management of all Network devices (routers, links, switches, load balancers, lan extenders etc.) within the ESIC environment.

Current Service provider delivers the following:

24X7 Proactive Monitoring:
24*7 Monitoring of the Critical Parameters, not limited to..
- Availability
- Bandwidth Utilization
- Errors
- CPU Utilization
- Packet Drops
- Interface Status

- 24*7 monitoring of the availability of the Network Services like
  - DNS Services
  - DHCP Services
  - WINS Services

Incident & Problem Management
- Tracking and Co-ordination of all incidents / problems till resolution
- Identification of probable causes of failures in the WAN environment
- Analyze Impact of associated systems, which can affect the WAN, availability
- Defining methodologies / workaround to address the probable causes of failures in case of incident or emergency
- Recommend on the possible solution / workaround to address the probable causes of failure
- Performing router, switch, and modem reconfiguration Coordinating with the vendors for the WAN uptime

Configuration Management
- Maintain connectivity maps of the WAN environment, detailing the connectivity and type of communication medium deployed
- Recording changes in the documents maintained on-site
- Maintaining protocol address registers and record changes, additions or deletions of sites.
- Monitor and control configuration aspects like IP address, subnet mask
- Maintain a repository of the IOS images standardized for the WAN environment

Configuration Backup & Recovery Drills
- Backup configuration files periodically or otherwise as and when changes are affected.
- Conducting drills based on defined redundancies and disaster recovery

Capacity & Availability Management
- Usage and Bandwidth Analysis. Recommendations to ESIC for upgrades, consolidation
• Analyze traffic and identify opportunities for setting QOS for the business services
• Analyze use of the Network services like DHCP and WINS and recommend consolidation, distribution of the services

### Accounting Services
Creating new users (Administrative and Privileged) and managing them

### Administration Services
- Administrations for Network authentication servers.
- Maintaining and administering network elements and devices on the NMS
- Configuration of new routers on the network
- Setup DNS and DHCP Servers
- Setup new domains in DNS, Secondary servers, replication for DNS
- Setup new WINS servers

### LAN Incident Management
- Provide End to End Support for all the Switches
- Ensuring the active ports are working properly. In case of a failure provide a workaround by immediately activating other Port and subsequently get the hardware repaired / replaced.
- Resolve any loose connections between the LAN Switches and the routers/ Desktops
- Restart Switches in case of any Hung State

### LAN Configuration Management
Configure Ports for a Manageable Switch
Configure VLAN for a Manageable Switch (if possible)

#### 11.3.7 Database Management Services

**Scope**
It covers all the DB (SQL) assets and technologies covered for ESIC.

**Current Service provider delivers the following:**

**24*7 Monitoring of all the Critical Parameters, not limited to.**
- Availability
- Disk Utilization
- Buffer Cache utilization.
  - Table space, segment etc..
- Memory / I/O / CPU Utilizations for the RDBMS
- Disk Free Space
  - Alert Logs for errors
- Lock Requests/sec and Lock Timeouts/sec

Monitor system performance and recommend actions for improving the system: Analyze the result of the Daily monitoring procedures and suggest if any changes are required to improve...
the performance of the Database / System / Applications.

**Incident & Problem Management**
- Coordination with the vendor / principal, for patch codes, bug fixes, upgrades on a need / no need basis and also for any technical escalation i.e. the Database software, and OS vendors and Storage Principals.
- Be a bridge between Application Owner and database software vendor and application software vendor: Understand the user requirement and conduct discussions with the application owner and vendor to provide solutions of best strategy to enhance the current system.
- Check and respond to all database related calls in the Service Desktop and follow up for the closure of the activities and update the call status.

**DB Backup**
Manage the backup strategy of the databases & assisting for proper restoration and recovery of the databases and overlying applications along with the Application Team.
- Restoration of database, archive log
- Database recovery with minimal downtime by using the right backups available. Recovery depends of efficiency of backup strategy as planned in consultation with ESIC.

**House Keeping Tasks**
- Regular de-fragmentation activities for better space management and performance
- Perform table-loading jobs

**Administration Tasks**
- Perform Database object creation / modification activities through import utility. The Database Administrator implements any change in the Database.
- Assist users in accessing and using the information: Assisting users in connecting to the Database through the applications. Handle database configuration problems.

**Security Management**
- Grant and revoke database access:
  - Understand and Implement Database Security in view of the requirements for Business Functionality.
- Securing Database access through system Database Roles and privileges as per Oracle security guidelines.

**Trend Based Consulting**
- Involvement in implementation for database availability, performance and automation
- Setup baselines for application databases: Implementing the Set up standards for database disk layout, backup strategy, maintenance activity and security guidelines for databases before going live and capture the exceptions.

**11.3.8 Application Monitoring Services**
Application Monitoring in [SIC is divided into 2 sets.
- Monitoring of ERP
- Monitoring of HIMS

**Current Service provider delivers the following:**
Performance Monitoring and Administration
• Monitoring availability of the server and services deployed
• Monitor alert notifications, checking for impending problems, triggering appropriate actions
• Monitor client connection and transaction status
• Monitor and collect DB performance statistics
• Monitor threshold values for key parameters such as response time, memory usage, file system usage
• Monitor middleware resource use ex. connection pooling etc
• Monitor message flows and queues
• Monitor Server response time
• Monitor and report on health of applications
• Monitor and check the application log
• Monitor application locks and release them
• Startup and Shutdown of web / application server instances
• Support to known errors and problems

Other Administration
• Vendor Management
• Escalating calls as per the escalation matrix
• Coordinating with escalation team to close calls
• Update knowledge base on closure of a call
• Log calls based on the monitoring alerts
• Trouble shooting Application server product related issues

11.3.9 Software Distribution / Patch Management Services

Scope
The objective of these services is to maintain standard and updated software deployment as per set policies. Ensure any non-solicited software not deployed. Provide first level diagnostic for all standard software. Provide other application software support as per guidelines set.

Current Service provider delivers the following:

List of Deliverables
• Install the software as per the corporate guidelines
• Setup standard installation and configuration document for all applications
• Ensure all the standard software are updated with latest patches and service pack
• Install, upgrade and update patches & service packs after proper authorization.
• Use Automated / Manual systems to update / upgrade / rollout patches / new software
• Maintain uniformity of software versions across enterprise
• Maintain software inventory
• Games or unauthorized software cannot be installed without written consent of authorized Solutions & Technology Team member.
• Software Inventory & License Management
  • Maintain version details of all the software in use
  • Track vendor details and escalation details

Give timely information on:
- New patches, upgrade option availability.
  - Security Patch Management
- Download and testing
- Roll out planning & sign off
- User intimation & patch deployment
- Have roll-back plan in the event of a failure

Other Application Software Support:
- Carry out installations, upgrade of non-standard applications as per the guidelines given by Applications Team
- Escalate any application related problem to application owner/administrator
- Provide first level support including diagnosis and troubleshooting
- Track incidents relating to application failure incidents, problems and resolution.
- Track system performance pre/post software/patch distribution

End User Support Services
Scope
Covers all the end users, their desktops and peripherals in DC, DR, RO, BO, hospitals, dispensaries, state directorate

Current Service provider delivers the following:

Central Service Desk
Call Logging
- Receive calls/incidents, service requests, queries, change requests from ESIC End Users and the ESIC IT Department through one of the agreed modes for communication
- Log Tickets in the Service Desk Tool on behalf of users calling Central Service Desk over phone
- Log Tickets with the correct category, severity, problem description, user information
- First Level Support

Call Routing
- Route the calls to the appropriate support team (within Current Service provider)
- Route calls to the vendors in case of issues pertaining to vendors
- Route Service Requests to the appropriate teams (like User Mgmt Group, Server-Mgmt Group, and Mail Mgmt Group etc.

Escalation
- Escalate issues / tickets which are going beyond the Service Levels
- Escalate issues pertaining to vendors' non-performance or delays
- Escalate issues pertaining to users non-availability or non-cooperation
- Escalate customer complaints to the appropriate management staff for further action
- Track all the issues and send status updates on the progress
Customer Notification
Notify the users on the ticket with information on who is working on the ticket and the status of the ticket
Notify the users on any outage in the Data Centres, which may cause unavailability of a service for the end users.

Reporting & Documentation
- Provide periodic updates on the status of the tickets to the end users
  Prepare MIS for the Tickets
- Extract agreed and ad-hoc reports from the Service Desk tool and send it to the concerned groups / upload in the reporting portal
- Maintain up-to-date information on the customer contacts, vendor contacts, management contacts, SLA matrix, Severity and categorization matrix

Technical Support Services
Provide Technical Support Tasks
- Assistance to users for accessing applications
- Providing them FAQs based on the call trends
- Troubleshoot desktop operating system problems
- Troubleshoot desktop application problems
- Install/configure desktop O/S, applications and all associated peripherals
- Configure & update Antivirus software
- Patch management for desktops - ensure critical patches are updated on schedule

Providing immediate notification to ESIC of system outages on critical systems, and providing progress updates in accordance with the Procedures Manual.

Print Management
- Restart Print Queues in case of a 'Hung' State
- Resolve all Hardware and Paper Jam Issues with respect to Printers
- Configure Print Queues for Servers / Users / Groups
- Provide appropriate rights and permissions for accessing printers
- Proactively Notify Admin of ESIC on Procurement for Paper
- Coordinate with Hardware support teams and resolve any hardware failures in the printers
- Resolve any issues for the print service due to virus in the network

11.3.10 IP PBX Management Services
Scope and deliverables
It involves managing devices like IP PBX.
Current Service provider delivers the following:
- IP PBX Operations Management
- Creation of voice ports, voice mail box and assign telephone extension to users. Maintain user extension lists and facilitates shifting of user by transferring extension within office.
- Maintain voice tag block in the wiring closet.
- Telephone links and voice circuits management.
- Coordinate with service providers in the event of a failure.
- Coordinate test activities to get the links up and working.
- Vendor Management with the respective vendors.
- Track maintenance schedule with support provider.

**Hardware Break fix Support**

**Objective:**
To provide hardware break fix support for all infrastructures installed at the ESIC Data center and the Disaster Recovery center and all ESIC locations. This service is provided on a 24x7 window.

**Logistics Management (Spares Management):**
- Simple Connect Call Centre at Current Service provider GSM to manage the entire logistics in the project. Hardware issues to be directed by Centralized Help Desk to Simple Connect.
- Spares at Strategic locations in order to cover the entire geographic spread of ESIC.
- Spare stocking based on: Failure Pattern/ Install Base/ TAT from Principals/ Spare transit time.
- Back to back support from OEM for TAC Support and Spare replenishment.

**11.3.11 Go-live Support Service Delivery Process**

Current Service provider would adopt the ITIL standards on Service Support and Service Delivery for the IT Services to ESIC. The integration of Service Support functions for day-to-day operations is shown below and some of the key processes have been detailed.

**Introduction**

The Service Desk handles a range of services, acting as a SPOC for all the services. It not only handles Incidents, Problems and queries, but also provides an interface for other activities such as change requests, maintenance contracts, software licenses, Service Level Management, Configuration Management, and Availability Management etc.

**Current Service provider’s Deliverables**
- Receive incidents, service requests, queries, change requests from end users at DC, DR, Hospital, dispensaries, RO, Branch Office, RBO, State Directorates, through the agreed modes of communication (E.g. Phone, email, web etc)
- Record incidents / service requests / change requests / queries in the service management tool on behalf of users reaching service desk through agreed modes of communication (E.g. Phone, email etc)
- Classify the incidents / service requests / change requests as per the defined categories (technical domains)
  / Prioritize incidents / service requests / change requests as per urgency and impact.
- Allocate the incidents / service requests / change request to the appropriate staff (Eg. Desktop or Network engineers)
- Monitor, track and update the progress status of all incidents and service requests
- Escalate incidents / service requests which are going beyond the agreed Service Levels
- Escalate issues pertaining to user’s non-availability or non-cooperation
- Record customer complaints and inform the concerned management staff for appropriate actions
- Logging and tracking incidents / service request that require resolution from suppliers
- Escalate issues pertaining to suppliers non-performance or delays
- Notify the users with progress status of all queries, incidents, service requests, change requests and complaints.
- Notify the users on any planned maintenance or unplanned outage in the Data Center which may cause unavailability of a service for the end users
- Generate the required MIS
- Maintain up-to-date information on the customer contacts, supplier contacts, management contacts, SLA matrix, Severity and categorization matrix
- Maintain all the documents (contracts, AMC and warranty information) up-to-date a central repository

**KPIs/ Critical Success Factors:**
- Percentage of calls answered within the agreed timelines
- Percentage of abandoned calls
- Percentage of Incidents that are correctly classified and prioritized
- Notification to users on status, resolution, planned maintenance and outages
- 3 Timely escalation on SLA violation and complaints

### 11.4 Current Operating Hours

<table>
<thead>
<tr>
<th>Infrastructure Details</th>
<th>Operating Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized Service Desk</td>
<td>24 x 7 x 365 or 366</td>
</tr>
<tr>
<td>DC &amp; DR</td>
<td>24 x 7 x 365 or 366</td>
</tr>
<tr>
<td>Hospitals</td>
<td>24 x 7 x 365 or 366</td>
</tr>
<tr>
<td>HO, RO, BO, State Directory</td>
<td>12 x 7 x 365 – (9 AM – 9 PM)</td>
</tr>
<tr>
<td>Dispensary</td>
<td>12 x 7 x 365 – (7AM – 7 PM)</td>
</tr>
</tbody>
</table>