

## Contents

1. Overview .....	3
2. Definitions and Acronyms .....	3
3. Introduction to SOW .....	4
4. Service Locations & Environment .....	4
5. HSE First.....	4
6. Current IT & ERP Service Organogram .....	6
7. Infrastructure details .....	6
8. FMS – Facility Management Service Snapshot... Error! Bookmark not defined.	
9. IT Service KPI .....	8
10. IT Service Catalog .....	9
11. IT Service Details .....	10
12. ITSM Process Details .....	38
13. Resources and Skills Requirement.....	43
14. Reports Review .....	49
15. Performance review .....	50
16. Escalation Management .....	51
17. Compliance and Audit .....	52
18. Asset and Inventory Management .....	52
19. Service Desk.....	52
20. Vendor Management.....	54
21. Transition/Onboard Plan .....	54
22. Specific clarifications to be noted with respect to this RFPError! Bookmark not defined.	
23. Annexures .....	55

## 1. Overview

India's largest City Gas Distribution Company

Gujarat Gas Limited (GGL) is India's largest City Gas Distribution (CGD) Company in terms of sales volume operating in 44 districts in 6 states of Gujarat, Maharashtra, Rajasthan, Haryana, Punjab & Madhya Pradesh and 1 Union territory of Dadra & Nagar Haveli.

GGL continues to hold the leadership position in CGD industry in terms of size and scale of operation. The Company has a successful track record of providing uninterrupted services for over 3 decades through a network of more than 42,000 kms. of Natural Gas pipeline, distributing approx. 9.47 mmcmd of Natural Gas. The Company operates over 825 CNG stations and has connected more than 22.27 lakh households, over 15,588 commercial customers and more than 4,429 industrial customers.

GGL has won Downstream Project of the Year – India award for Natural Gas Distribution for Cleaner & Greener cities & villages and ESG Initiative of the Year - India award for Small Steps for Social, Environmental Cause, Giant leaps for Social & Environment by Asian Power in the year 2024. GGL has also won the following awards and accolades during FY 2023 - 24 :

- Recognized as the 'World' s Most Trustworthy Companies 2023' by Newsweek and Statista amongst the listed firms in Energy and Utilities category
- Listed in Dun & Bradstreet' s flagship publication 'India' s Top 500 Value Creators 2023' in Gas Processing, Transmission and Marketing category
- Won 'IEI Industrial Excellence Award 2023' for the commendable performance in the category of Engineering, Manufacturing and Processing
- Received 'Supply Chain Champion Award' in Oil & Gas industry category by ISCM (India Supply Chain Management) in 9th edition of its annual rankings
- Conferred with the prestigious 'SKOCH ESG Award 2023' in City Gas Distribution (CGD) Project
- Ranked amongst the 'TOP 150 Wealth Creators' by Dalal Street Investment Journal

The company has successfully commissioned the country' s first pilot project of blending green hydrogen with Piped Natural Gas for the domestic customers on collaboration with NTPC. GGL is committed to reach out to every possible natural gas user in its expanded GAs. The size and scale of the combined entity gives it the ability to achieve efficiencies and effectively manage the transformational changes in the sector. This major gain in productivity would benefit all the key stakeholders i.e. Customers and Shareholders.

GGL is strategically aligned to energize India's Natural Gas vision.

\* Data as on 31st December 2024

## 2. Definitions and Acronyms

These are the definitions and acronyms used in this SOW. They are group and project specific acronyms.

Term or Acronym	Definition
FMS Vendor / Contractor	GGL IT & ERP Infrastructure Facility Management Contractor
BCP	Business Continuity Planning
DR	IT Disaster Recovery
GGL / Company / Owner	Gujarat Gas Ltd.
SDL	Service Desk lead
SOW	Scope of Work
HSE	Health Safety and Environment
Top Management / VIP users	GGL Executive team members, Directors & Above
Other Users	All Users apart from Top Management
KPI	Key performance Indicators
KRA	Key Result Areas
EU	End User or customer who is directly consuming the service
NPD	Non-Performance Deduction
FMS Team	Includes Locations Engineers, Core Infra Engineers and Lead
Engineer	Interchangeably used as FMS Engineer or Local Engineer or Core Engineer
Local Engineer	Resident Engineer at Site

### 3. Introduction to SOW

This Scope of Work (SOW) defines the scope of work to be accomplished and the tasks to be performed by GGL IT Infrastructure Facility Management Services Provider (here in after referred as FMS Vendor / Service Provider) for Gujarat Gas Limited (here in after referred as GGL / Company).

FMS Vendor will provide the required resources and expertise to support the GGL IT Infrastructure at various locations that includes Registered Office (Gandhinagar), Corporate Office (Ahmedabad), Geographical Area Head offices and its satellite locations and Other offices i.e. Warehouses etc. (list enclosed). The Scope of the service includes management and support of defined IT services within GGL. The SOW lists down the various services that need to be provided by FMS Vendor and lists down the roles and responsibilities of GGL and FMS Vendor in the execution of these services. GGL expects FMS Vendor to begin work by establishing an overall service delivery in scope, to be followed by detailed roles and responsibility. Prior to the execution of service delivery, the framework and activities will be jointly approved.

GGL lays utmost importance on Safety (HSE) and Quality and expects the similar focus from FMS Vendor in terms of safety and Quality of Services to be provided. GGL Safety guidelines and IT policy procedures provides independent assurance that work to confirm the defined processes are operating within the parameters and policies defined for the engagement.

This SOW defines the scope of work to be accomplished by FMS Vendor and specific responsibilities for various activities/task spanned to be performed and completed by FMS Vendor with inputs from and/or participation of GGL. It will be the responsibility of FMS Vendor team to ensure end to end delivery of IT Service defined in this SOW, subject to various terms, conditions and SLA's specified in this SOW.

This SOW Framework has to comply as per ITIL (IT Infrastructure Library) standard minimum version 3.0 and as applicable from time to time. All the services and process are defined by GGL IT team as per ITIL best practices. FMS Vendor needs to follow these Service Delivery process for all the defined business services of GGL.

### 4. Service Locations & Environment

All existing states where operations are, have been listed below:

- a. Gujarat
- b. Maharashtra
- c. Punjab
- d. Haryana
- e. Delhi
- f. Madhya Pradesh
- g. Rajasthan
- h. Dadra Nagar Haveli

GGL is planning to expand its business PAN India in other states. Bidder to support in these states.

NOTE: Consider growth of 5% every year in terms of IT & ERP Infrastructure, Employees and Business Locations from point of view of Scaling and Aligning FMS Team for SLA compliance

### 5. HSE First

At GGL always HSE is first. GGL believes that every employee OR contractor has the right to work safely at GGL and go home safely without any injury OR illness.

**GGL's TARGET IS 0 (ZERO) INJURY DURING WORK.**

FMS Vendor has to go through detailed HSE training before starting services. During this training all policy procedures and compliance requirement would be shared with FMS Vendor.

**PLEASE NOTE THAT WORKING ON EQUIPMENTS AND MACHINERIES IN GGL PREMISES REQUIRE SEPARATE SAFETY PASSPORT. WITHOUT THIS, NOBODY IS AUTHORIZED AND ALLOWED TO WORK.**

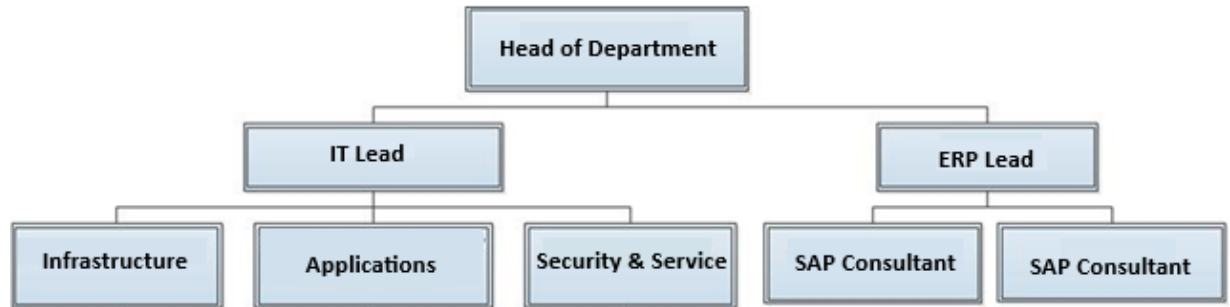
After thorough training of HSE all the FMS VENDOR service staff would be provided safety passport.

**PLEASE MAKE NOTE THAT INDEPENDENT SERVICE DELIVERY TO EUs ONLY WILL BE ALLOWED IF AN ENGINEER IS HAVING SAFETY PASSPORT.**

Any physical access to the premises OR logical access to the IT & ERP equipment or system will be strictly dependent on Safety Passport. Without safety passport access will not be given.

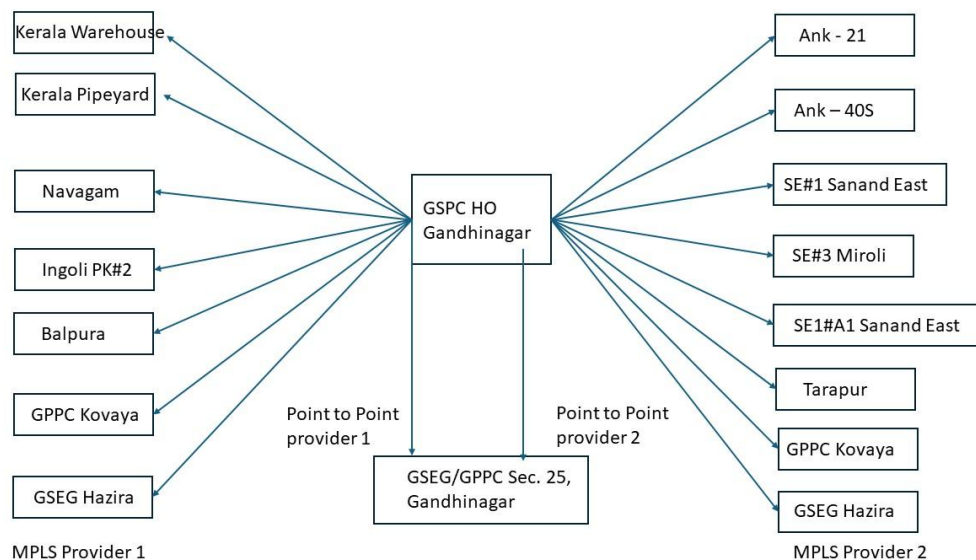
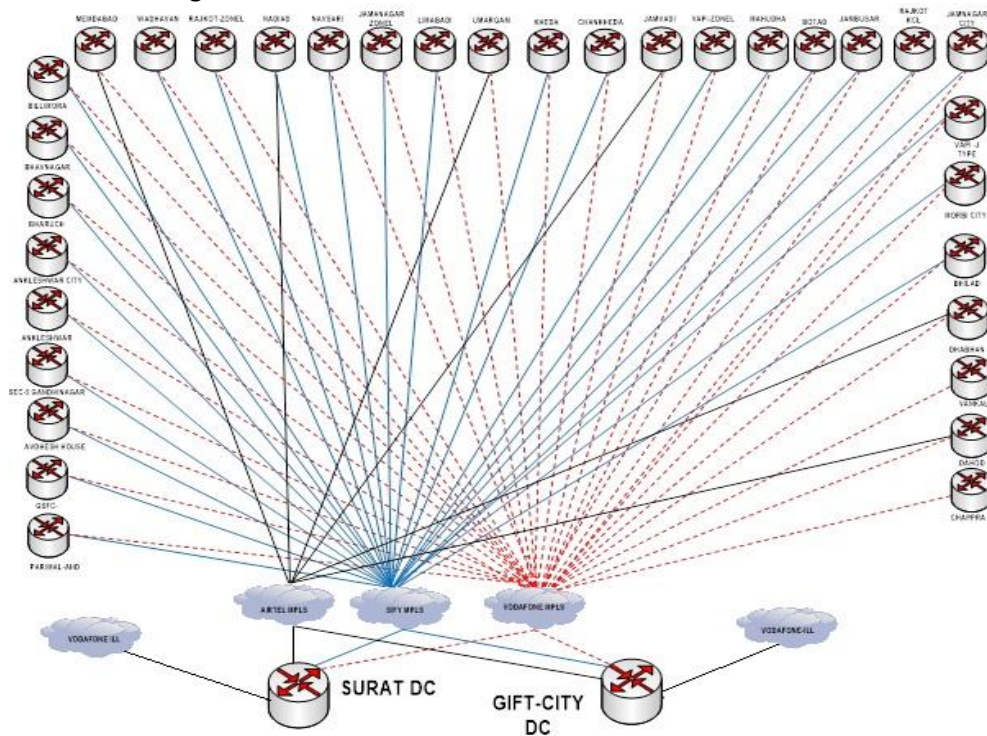
**All FMS Vendor team will ensure compliance to basic Personal Protective Equipment's (PPE) – Helmet (Where ever applicable), Shoes, Gloves while working in the field at their own cost.**

## 6. Current IT & ERP Service Organogram



## 7. Infrastructure details

### a. Current WAN Diagram



## b. End-Users IT &amp; ERP Assets

Asset-Type	Corporate	Zone-1	Zone-2	Zone-3	Zone-4	Zone-5	Zone-6	GSPC/ GSEG/ GPPC	Grand Total
Desktop/Laptop	253	362	421	213	373	47	115	338	2122
Peripherals	341	399	535	287	537	119	165	1	2384
Monitor	195	348	501	209	349	43	85	118	1848
Network / Biometric	141	138	228	62	102	14	33	161	879
Printer (Managed / Unmanaged) / Scanner	44	95	60	33	62	9	21	105	429
Server/ Workstation	102	17	89	5	9	2	4	105	333
UPS	19	32	11	20	27	2	7	13	131
VC/TV/CCTV+NVR	28	14	23	8	12	3	5	116	209
Virtual	138		54					31	223
<b>Total</b>	<b>1261</b>	<b>1405</b>	<b>1922</b>	<b>837</b>	<b>1471</b>	<b>239</b>	<b>435</b>	<b>988</b>	<b>8558</b>

- Above numbers are indicative, actual details shall be shared during project transition phase.

**8. FMS**

As part of Facility Management scope, FMS Vendor is expected to manage end-to-end service delivery of the below IT & ERP services at GGL. A detailed explanation of these IT & ERP services can be referred in Section-11 - IT Service Details. All GGL IT & ERP the services are divided into two categories i.e. DCS Primary Services that are required to be managed directly under this RFP and EUS Primary services that will be managed under separate RFP however any support, interfacing and coordination required with EUS Primary services shall be covered under scope of this RFP

## a. Primary DCS Services

- i. Server Virtualization Service
- ii. Desktop Virtualization Service
- iii. Wintel Service
- iv. Directory Service
- v. Messaging Service
- vi. UNIX/AIX Service
- vii. SAP BASIS Support Service
- viii. Backup/DLO Service
- ix. Storage Service
- x. Network Service
- xi. Data Connectivity Service
- xii. Internet Service
- xiii. Network Security Service
- xiv. Video Communication Service
- xv. End-Point Security/Anti-Virus
- xvi. DC Infra Mgmt. Service
- xvii. DC facility Mgmt. Service
- xviii. UPS service
- xix. Security Event and Incident Monitoring
- xx. Vulnerability Assessment & Penetration Testing (VAPT) and Mitigation

## b. Primary EUS Services

Following Services are not directly managed under this RFP, however the bidder will need to extend support, interface or coordinate for below services to comply as per SLA requirement

- i. End User Computing
- ii. End-Point Security/Anti-Virus
- iii. IT Assets Management Service (End-User)



- iv. Endpoint Encryption Service
- v. BMC ITSM Platform Management
- vi. Patching Services - End-user/Core Infrastructure

To deliver the above IT & ERP services FMS Vendor is expected to follow the below defined GGL ITSM process.

- a. Incident Management
- b. Change Management
- c. Problem Management
- d. Service Request Management
- e. Knowledge Management
- f. Availability Management
- g. Capacity Management
- h. Patch Management
- i. MIS Reports/Dashboards
- j. BCP/DR
- k. Vendor Management
- l. Backup Management
- m. Security Compliance
- n. Documentation
- o. Audit Compliance
- p. Project Support
- q. Asset & Configuration Management

A detailed mapping of each IT & ERP Services against ITSM processes are as per Section – 10 IT Service Catalog. GGL uses BMC ITSM tool sets to automate ITSM processes and monitor IT & ERP Services. BMC ITSM Tool is subject to change in future.

GGL ITSM processes are aligned with ISO 20000 and ISO 27001 standards.

## 9. IT Service KPI

Below are the high-level Key Performance Indicators for the FMS Contract.

- a. Adherence and improvement to the below KPIs should be the strategic objective of the engagement. Hence the below KPI should be measured, reported and reviewed monthly.

KPI in Current Support Model			
Sr	KPI	How to Measure	Minimum Acceptable Target (Monthly)
1	% of Customer Satisfaction Index 4 or above	Total number of Customer Satisfaction Feedback having rating more than 4 out of 5 based on the feedback for minimum 10% of the calls logged in the system.	90%
2	Business Service Uptime SLA Compliance	Averaging Compliance of Individual services in scope (excluding planned downtime)	100%
3	SLA Compliance for response time	(Total number of calls responded within SLA / Total number of calls registered) %	100%
4	SLA Compliance for resolution time	(Total number of Calls Resolved within SLA / Total number of Calls registered) %	100%
5	HSE Compliance	No major non-compliance	100%
6	Asset and Inventory Management Compliance	Accuracy of physical assets vs. reported in the Financial Records for Cor-Infrastructure	100%
7	Capacity Management Compliance	Capacity Utilization should be less than 80%	95%

8	Business Continuity Compliance – IT & ERP DR	Adherence to BCP Plan, DR Testing , Data Replication and, Documentation	100%
9	Security Compliance	Business hours lost due to Security Incident to be zero	100%
10	Incident Resolution by use of KEDB	Number of KEDB used to resolved the Incident	30%
11	Remote Support Compliance	% of calls closed via remote support should be minimum 60%	100%
12	Change Management Compliance	All the approved changes to be implemented Successfully	100%
13	Incident Management Quality Compliance	Number of repeated Incident less than 2% from the reference period	100%
14	Backup Compliance	Adherence to GGL Policy and procedure for Backup and restoration for devices under scope. Backup Success rate should be 99%	100%
15	Patch Management	All critical Operational and Security patches must be implemented within agreed timelines	100%
16	Vendor Management	Timely coordination with all 3 <sup>rd</sup> party vendors to ensure zero calls breach on account of coordination/liasoning	100%
17	Service Improvement Plan	At least 5 SIP initiatives in an year to improve overall ITSM process	100%

- b. The KPI's where penalty deduction are applicable are explicitly marked (Refer section ITSM Process Details), however from performance monitoring perspective the KPI's are based on the ITSM standard and as applicable to GGL from time to time (including the ones shared above).

SLA, Response/Resolution time (Turn-Around Time or TAT) for various categories of service requests e.g. TAT for new mail ID / domain ID creation, providing access to File Server share, providing internet access, creation of ID for online attendance system, new software installation request, toner/cartridge change etc. are already covered as part of IT Service request Management Process (ITSM Procedures)

## 10. IT Service Catalog

IT service Catalogue is a representation of IT & ERP services and the expected ITSM processes to be followed for each of the services. Most of the ITSM processes are automated.

Legend- ✓ (Responsible), x (Not-Responsible)

S. No	ITSM Processes A-Automated P-Partially Automated	A-Incident Management	A-Change Management	A-Problem Management	A-Service Request Management	A-Availability Management	P-Capacity Management	A-Patch Management	P-BCP/DR Management	P-Vendor Management	A-Backup Management	P-Security Compliance	P-Documentation	P-Audit Compliance	P-Project Support	A-Asset & Configuration Management
	<b>IT Services</b>															
1	Server Virtualization Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	Desktop Virtualization Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3	Wintel Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓



4	Directory Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5	Messaging Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6	UNIX/AIX Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
7	SAP BASIS Support Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
8	Backup/DLO Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
9	Storage Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
10	Network Infra Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
11	Data Connectivity Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
12	Internet Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
13	Network Security Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
14	Video Communication Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
15	End-Point Security/Anti-Virus	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
16	Data Centre Infrastructure Management Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	X	✓	✓	✓	✓	✓
17	Data Centre facility Management Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	X	✓	✓	✓	✓	✓
18	UPS Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	X	✓	✓	✓	✓	✓
19	IT Assets Management Service (Core Infrastructure)	✓	✓	✓	✓	✓	✓	✓	X	✓	✓	✓	✓	✓	✓	✓
20	Security Event and Incident Monitoring	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
21	Vulnerability Assessment & Penetration Testing (VAPT) and Mitigation (to be carried out internally)	✓	✓	✓	✓	X	✓	✓	X	✓	✓	✓	✓	✓	✓	✓

Note: GGL gets a 3<sup>rd</sup> party annual VAPT assessment carried out under a separate contract

#### 11. IT Service Details

FMS Vendor must deliver (Drive / Support) following IT & ERP Service as a part of Service Delivery

Please refer to [www.gujaratgas.com](http://www.gujaratgas.com) (contact us) for locations details like state, pin code etc.

The following service are divided into two categories i.e. DCS Primary Services that are required to be driven directly under this RFP and EUS Primary services for which only support needs to be provided under this RFP

	S. No	Service	Drive / Support	Description	Infrastructure	Days /Wk	Business Hr Support	Non-Business Hours
	1	End User Computing Services	Support	This service covers support to end users for PCs, laptops, mobile devices, printer, VC, Software installation and Application access across all GGL Sites	Desktop Laptop Printer Mobile Standard end user applications	6	onsite	VIP User Support

	S. No	Service	Drive / Support	Description	Infrastructure	Days /Wk	Business Hr Support	Non-Business Hours
<b>End User Service</b>	2	Desktop Virtualization Service	Drive	This service covers fine tuning of applications, installation of hardware / software image of thin clients	Thin Client Hardware Software	6	onsite	Need basis-Onsite Support
	3	Server Virtualization Service	Drive	This service manages and supports Virtualized platform for using VMware Virtualization Technology. 77 instances of virtual servers.	90% of the Wintel environment is virtualized Sphere & ESX 4.x, 5.x, 6.x,7.x  Hp SimpliVity Hardware , DELL FX2 Hardware , HP blade servers compatible Vmware platform	6	Onsite	Need basis-Onsite Support
<b>Server Services</b>	4	Wintel Service	Drive	This service provides Support and Management of all Microsoft Windows servers deployed within GGL.	Windows Server 2003,2008,2010,2012,2016,2019	6	Onsite	Need basis-Onsite Support
	5	Directory Service	Drive	This service covers support and management of Active Directory Structures in GGL Domain and subdomains.	Active directory 2012 R2 and above	6	Onsite	Need basis-Onsite Support
	6	Messaging Service	Drive	This service provides Management and support of IT & ERP Communication Infrastructure in GGL	Microsoft Exchange 2016 in HA, M365, Cisco WebEx , JabberActive Sync Service-Android, Windows, iOS. Symantec-Enterprise Vault ver 12.x and above	6	Onsite	Need basis-Onsite Support
	7	Linux / AIX/ UNIX Management Service	Drive	This service provide support and Management of AIX/ UNIX Environment	AIX 7 Onwards HP UX 11i.Ver 3	6	Onsite	Need basis-Onsite Support
	8	SAP BASIS Support Service	Drive	This service provide support and Management of SAP Environments	SAP ECC, SAP CRM, SAP BW, SAP EP, SAP GRC, SAP Gateway, SAP Syclo, SAP Mobile Application, SAP PO	6	Onsite	Need basis-Onsite Support
	9	Backup /DLO Service	Drive	This service manages and supports the data backup of GGL IT & ERP environment.  The Scope includes Data and configuration backup of GGL business	VERITAS Net backup Server 8.1 and above Dell Tape Library LTO 6 NEO Tape library LTO 7 HP 4100 VTL Disk based Appliance Data replication to DR Site DELL/Fujitsu DFS Storage	6	Onsite	Need basis-Onsite Support
<b>Data Backup and Storage Services</b>								

BID No.:

	S. No	Service	Drive / Support	Description	Infrastructure	Days /Wk	Business Hr Support	Non-Business Hours
				services and infrastructure and data backup from selected end user system.	<b>EU Side</b> Data backup of laptops using DLO Data backup of desktops to external media / central servers during transition or replacements			
	10	Storage Management Service	Drive	This service manages and supports the centralized storage facilities for all GGL data storage requirements.	EMC Storage DELL INC PowerEdge Netapp	6	Onsite	Need basis-Onsite Support
<b>Network Services</b>	11	Network Infra Service	Drive	This Service manages and supports Network devices/Hardware deployed across GGL location	Routers Switches-L2,L3,SAN Wireless equipment Access point WAN Optimization Load Balancer Voice Gateway	6	Onsite	Need basis-Onsite Support
	12	Data Connectivity Service	Drive	This service manages and supports LAN WAN, SAN WLAN, VPN Network across GGL location	MPLS Link. RF Link. OFC Link. LAN and OFC Cabling Data-Centre Cabling Equipment's supporting this Services IT Equipment cabling within Racks. VPN	6	Onsite	Need basis-Onsite Support
	13	Internet Service	Drive	This Service manages and supports Internet facility across GGL location and to Internet facing applications.	Internet link. Proxy device.	6	Onsite	Need basis-Onsite Support
<b>Cyber Security</b>	14	Network Security Service	Drive	This service secures GGL outer periphery from external attacks as well as hardening of internal network and guest access Management.	Firewall IPS ACS Proxy device.	6	Onsite/Offsite	Need basis-Onsite Support
<b>VC Services</b>	15	Video Communication Service	Drive	This services covers support of Video Communications Infrastructure in GGL.	Polycom & Cisco -VC equipment End-Point devices Peripherals and accessories Audi/Video setups in meeting rooms.	6	Onsite	Need basis



	S. No	Service	Drive / Support	Description	Infrastructure	Days /Wk	Business Hr Support	Non-Business Hours
Cyber Security	16	Antivirus Service	Support	This service covers support of Antivirus server and clients installed on all IT & ERP Infrastructures in GGL.	Trend Micro XDR patch updating / client installation on PC, Device control, DLP	6	Onsite	Need basis-Onsite Support
	17	Data Center Infrastructure Management Service	Drive	This Service manages and supports Server Infrastructure deployed within Data Centre at GGL	Servers-Blade Servers, Standalone Servers	7	Onsite	Need basis-Onsite Support
Datacenter Services	18	Data Centre Facility Management Service	Drive	This service manages and supports all safety & security devices deployed within Data Centre at GGL.	Access Control system UPS system - APC Symmetra, HVAC system - APC In Row RD Fire/Smoke detection & prevention system Water detection system Rodent prevention system	7	Onsite (07:00A M to 10:00PM ) Remote (10:00P M to 07:00AM )	Need basis-Onsite Support
	19	Ups Service	Drive	In this service the FMS engineer has to visit all GGL location and inspect the UPS deploy at office and do first hand diagnostic, check battery health and incase observe any battery issue report same to GGL Service owner and get ticket raised with UPS Battery ARC Vendor	UPS deployed across GGL office to provide backup power to IT & ERP equipment's	7	Onsite/remotely	Need basis-Onsite Support
Utilities	20	IT Assets Management Service	Support	FMS vendor has to ensure that all IT & ERP Assets are Tagged, Documented, Tracked and stores properly at designated GGL locations/premises for IT & ERP Inventory	All IT & ERP Core-Infrastructure Physical & Software Assets. Currently BMC Suite is being used for same	6	Onsite/remotely	Need basis-Onsite Support
Asset Management	21	Security Event and Incident Monitoring	Drive	FMS vendor to ensure that all Security Alerts/Events from all IT & ERP Assets are Captured, Analyzed, Normalized and Stored in safe custody	All IT & ERP Assets that are OR going to be connected to GGL IT & ERP Infrastructure	8	Onsite/remotely	Need basis-Onsite Support
Cyber Security								



	S. No	Service	Drive / Support	Description	Infrastructure	Days /Wk	Business Hr Support	Non-Business Hours
Cyber Security	22	Vulnerability Assessment & Penetration Testing (VAPT) and Mitigation	Drive	FMS vendor to ensure that all IT & ERP assets are assessed from point of view of inherent weaknesses or loopholes in terms of Software or Hardware	All Active IT & ERP Assets that are OR going to be connected to GGL IT & ERP Infrastructure	6	Onsite/remotely	Need basis-Onsite Support
	23	Endpoint Encryption Service	Support	FMS Vendor to ensure that all the laptops (PC's) data is secured with the appropriate encryption	All the approved end user PC's have encryption installed, configured and tracked properly and licenses are managed accordingly in the Encryption solution and console	6	Onsite/remotely	Need basis-Onsite Support
	24	BMC ITSM Platform Management	Support	FMS Vendor to ensure that the GGL ITSM platform is kept up to date and working alongwith Coordination with the OEM for tool upgrade, patch update, customization	The ITSM platform (currently Old and New Hardware Tool) has updated user, asset and service catalogue in the existing ITSM System	6	Onsite/remotely	Need basis-Onsite Support
	25	Endpoint/Server Patch Management	Support	FMS Vendor to ensure that the GGL Systems (PC, Servers, Network) are regularly updated with the operational, security, performance patches as per GGL Policy	The BCM client management to be used for the ITSM platform (currently BMC) selection, rolling out and pushing of the patches to the endpoints	6	Onsite/remotely	Need basis-Onsite Support

## a. Server Virtualization Service

**Responsibility matrix** legend Responsible-R, Co-ordinate-C

S No	Server Virtualization Service	FMS Vendor	GGL
1	Monitoring VMware Server Performance and ensure High Availability of VmWare Service, M365 / Cloud Support	R	C
2	Monitoring Events and alerts in BMC, Motadata and Nagios tool and responding to the alerts with proper actions and closure	R	C
3	To ensure all the VMware configuration data are backed up	R	C
4	VMware Cluster management	R	C
5	VM Installation, P to V, troubleshooting, root cause analysis, fixing the root causes .Resolving VMware issues	R	C
6	Escalating Incidents, problems to OEM, Vendors for resolving, coordination with OEM. fault analysis for any VDI Performance issue and have performance tuning of VMware Server	R	C
8	Daily VMware Service Health Check-up as per schedule	R	C
9	To ensure to have BCP/DR test as per BCP Plan scheduled by GGL, BCP/DR to be activated as an when needed post GGL approval	R	C
10	Ensure all ITSM process (Incident, Problem, Change Management) are followed for Server Virtualization Service	R	C

## b. Desktop Virtualization Service

**Responsibility Matrix** legend Responsible-R, Co-ordinate-C

Sr no	Desktop Virtualization Service	FMS Vendor	GGL
1.	Monitoring Virtualized Desktop Service Performance and ensure High Availability of VDI Service, M365 / Cloud Support	R	C
2.	Ensuring High Availability of VDI Service, fault analysis for Service improvement plan to overcome any performance issues.	R	C
3.	Ensure all Thin Clients are updated with latest patch release available.	R	C
4.	Preparing Image of VDI Version deployed within GGL and storing in Central location for Installation of Windows version approved by GGL	R	CC
5.	VMware Service Health Check-up as per schedule, updation of all latest patches /Firmware available in all Thin client images.	R	C
6.	To troubleshoot, do root cause analysis, and provide fixes to the problem reported in VDI Service	R	C
7.	Coordination with OEM, Escalating Incidents, problems to OEM, Vendors for resolving	R	C
8.	Allocation of Thin Clients as per User list provided by GGL	R	C
9.	Ensure all ITSM process (Incident, Problem, Change Management) are followed for Desktop Virtualization Service	R	C

## c. Wintel Service

**Responsibility matrix**      **legend Responsible-R, Co-ordinate-C**

S No	Wintel Service	FMS Vendor	GGL
1	Monitoring Uptime of Windows Servers including critical Operating System parameters like CPU, Memory, Hard Disk, Network etc.	R	C
2	Monitoring events and alerts generated via Monitoring tool (BMC, Motadata and any new tool GGL procure during contract period) and taking appropriate actions against the alerts/events, Validate the alerts for False-Positives. Taking corrective preventive action against error logs in System application, Security.	R	C
3	Monitoring System, Application, and Security logs, analyzing for their criticality & suggesting for corrections. Responding to System event Alerts of servers for hardware, software.	R	C
4	Managing Disk space, memory, processor and other critical resources directly affecting performance of the applications.	R	C
5	Regular Shutdown and Start-up of Servers as per the Scheduled prepared by GGL IT & ERP team.	R	C
6	Periodic Checking of Operating System and Hardware , allocation of Server resources (RAM, Hard Disk space, Processor) as per GGL requirement.	R	C
7	Server Builds (Build Images of the Servers to ensure quick restoration )	R	C
8	OS Installation, Configuration, Troubleshooting, Fault analysis, Root cause analysis, fixing the root causes	R	C
9	Installation of Software Packages approved by GGL IT & ERP team.	R	C
10	Help in creating SOPs, Suggesting correction / modification in existing SOPs.	R	C
11	MIS reports as per GGL IT & ERP Requirements	R	C
12	To ensure all VAPT/Audit point are closed on time (max 45 days). Regular Vulnerability Assessment and patching vulnerabilities.	R	C
13	Escalation of issues and problems to Vendor, coordination till IT & ERP gets resolved for hardware / software.	R	C
14	To ensure to have BCP/DR test as per BCP Plan scheduled by GGL , BCP/DR to be activated as an when needed post GGL approval	R	C
15	Checking and corrective preventive action on abnormalities.	R	C
16	To ensure all Wintel Server are having latest Antivirus patch, if not coordinate with Antivirus Server owner to get the same deployed.	R	C
17	To create and maintain system start-up and shutdown sequence to avoid any Service corruption	R	C

## d. Directory Service

**Responsibility matrix**      **legend Responsible-R, Co-ordinate-C**

Sr no	Directory Service	FMS Vendor	GGL
1	Monitor and ensure Directory services are up and running and ensure High availability of services and M365 / Cloud Support	R	C
2	Create and Manage Directory Structures, Create/Modify/Delete Users and User properties/groups/Network shares	R	C
3	Create login and logon Scripts.	R	C



4	Management & Administration of DNS, DHCP, NFS, NIS, DFS roots, Group policy, Configuration of Access Control using NTFS permissions, access rights modifications	R	C
5	Assign and maintain space usage restriction. Check AD Health by AD Tools, Resolving potential Errors found in Health tools	R	C
6	Restore server operating system in the event of a crash. Resolve server problems like system 'hang', hard disk crash, etc. Escalation of issues and problems to Vendor, coordination till IT & ERP gets resolved for Active Directory	R	C
7	To ensure end to end operational work such as new file system creation, Managing File, Directory level permissions Configuration of Account Policy, Access Rights & Password control, Resetting Password reset requests, configuring print servers	R	C
8	Creation of DNS entries, zones, hosts, services. Monitoring DNS/DHCP Service Performance by tools. Ensuring DNS / DHCP Services uptime	R	C
9	Monitoring IP Scopes for the DHCP Scopes, Escalating if IP Scopes are full or reaching limit. Resolving DNS/DHCP Issues related to configuration. Monitoring Hosts which take IPS from DHCP.	R	C
10	Creation, testing, implementing different Group Security Policies as and when required by GGL IT & ERP .refer to GGL IT & ERP SOPs and performing operation of Active Directory Domain Admin. Ensuring IP distribution as per the GGL IT & ERP Policy.	R	C
11	AD Installation, Configuration, Troubleshooting, Fault Analysis, Root Cause Analysis, Fixing the root causes	R	C
12	Monitoring events and alerts generated via Monitoring tool (BMC, Motadata & any new tool GGL procure during contract period) and taking appropriate actions against the alerts/events, Validate the alerts for False-Positives. Taking corrective preventive action against error logs in System application, Security.	R	C
13	Periodic Schedule Maintenance Activity & AD Tuning and reconciliation of AD data with HR data	R	C
14	Ensure to have BCP/DR test as per BCP Plan scheduled by GGL , BCP/DR to be activated as an when needed post GGL approval	R	C
15	Backup of DNS / DHCP configuration	R	C
16	Escalating incidents and problems to OEM, Vendor, other DNS Administrators / Network Admin for resolving DNS / DHCP Issues	R	C
17	To ensure all VAPT/Audit point are closed on time (max 45 days). Regular Vulnerability Assessment and patching vulnerabilities. AD Security loop holes scanning and fixing in coordination with Security Team.	R	C

## e. Messaging Service

**Responsibility matrix**      legend Responsible-R, Co-ordinate-C

S.No	Messaging Service	FMS Vendor	GGL
1	Monitor and ensure High Availability of Communication Services - Exchange Server, Enterprise Vault, Active Sync, cisco jabber, M365 / Cloud Support	R	C
2	To ensure that Email communication is happening with internal and with external domains	R	C
3	Email Blocking, Enabling as per the requirement of GGL IT&ERP	R	C

S.No	Messaging Service	FMS Vendor	GGL
4	24*7 monitoring of the Critical Parameters for the Servers like. Monitoring Mail Application for availability. <ul style="list-style-type: none"> <li>• Mail Queue Length</li> <li>• Mail Services Status</li> <li>• SMTP Gateway Status</li> <li>• Mail Server Disk Management</li> <li>• DB Cache size</li> <li>• Memory/Pages/Sec</li> <li>• MTA Messages /Sec</li> </ul>	R	C
5	Ensuring configuration and availability of Email services on end user Mobile handsets, and other devices mentioned in Scope	R	C
6	<b>Email Security Tasks</b> <ul style="list-style-type: none"> <li>• Provide Permissions for Shared Mail folders</li> <li>• Provide Access Control on the Gateway systems</li> <li>• Provide Content filter setup at the Anti-spam systems</li> <li>• Provide SMTP Dot forwarding.</li> <li>• Orderly startup and shutdown of Mail Application Services.</li> <li>• Taking Backup of the Exchange server as per customer's policy.</li> <li>• Restore Mail Databases in the event of a Server crash.</li> </ul>	R	C
7	<b>Anti-Spam Management:</b> <ul style="list-style-type: none"> <li>• Releasing Quarantined mail upon customer request</li> <li>• Analyzing the kind of spam mail that entered network</li> <li>• Modifying/creating filters to arrest the spam.</li> <li>• Analyzing why a genuine mail got quarantined/blocked</li> <li>• Creating/Modifying filters, sub-filters, policies and sub-policies.</li> <li>• Setting/modifying attachment scanning filters.</li> <li>• Creating/modifying compressed file settings.</li> <li>• Configuring/Modifying Spam filter's MTA Connection settings</li> <li>• Setting/Modifying Exception handling settings.</li> <li>• Setting/Modifying schedule update settings.</li> <li>• Performing Virus/Engine/Spam Engine filter updating.</li> <li>• Setting/Modifying SMTP routing settings.</li> <li>• Adding/Deleting trusted IP's/domains or Un-trusted IP's/domains.</li> <li>• Blocking/Allowing specific mail ID's.</li> <li>• Managing Spam filter logs.</li> <li>• Creating/Deleting/Modifying address groups.</li> <li>• Defining/Modifying/Deleting filter action settings.</li> <li>• Enabling disabling Filters.</li> <li>• Defining/Modifying/Creating Incoming/outgoing policies.</li> <li>• Monthly policy back up of Spam filter application.</li> <li>• Trouble-shooting as and when required,</li> <li>• Updating the necessary Virus/Spam engine updates</li> </ul>	R	C
8	<b>Messaging Support activity</b> <ul style="list-style-type: none"> <li>• Create/Modify/Delete Mail boxes, Mail box stores, DLs.</li> <li>• Transfer/Re-certify/Rename/Delete ID.</li> <li>• Add/Delete/Modify Mailboxes, Distributions and Contacts.</li> </ul>		C

S.No	Messaging Service	FMS Vendor	GGL
	<ul style="list-style-type: none"> <li>• Configure/Manage Connectons/Connections Documents.</li> <li>• Configure/Manage ACLs.</li> <li>• Directory and Replication Management.</li> <li>• Configure/Manage Calendaring and Scheduling.</li> <li>• Install/Configure Exchange Web Access.</li> <li>• Maintain Work Flow.</li> <li>• Manage Message Queues.</li> <li>• Manage replication services.</li> <li>• Perform periodic Mail Performance Tuning as per customer policy.</li> <li>• Adhere to checklists for mail maintenance as provided.</li> <li>• Perform Client Setup.</li> <li>• Enable web access of mailbox.</li> <li>• Provide SMTP Access.</li> <li>• Perform Password Resets.</li> <li>• Perform Mailbox Quota Management.</li> <li>• Perform Creation/Deletion/Change of Site/OU/Domain.</li> <li>• Perform Fragmentation Check for Mailbox/Mail Folders.</li> <li>• Perform Compacting/Cleaning of the DBs.</li> <li>• Schedule Replication between Sites.</li> <li>• Configure client access to POP, IMAP and HTTP services.</li> <li>• Configure client access to SMTP services.</li> <li>• Configure Message Store Quotas.</li> <li>• Configure Message Store Partitions.</li> <li>• Installation, troubleshooting, fault analysis, root cause analysis, fixing the root causes.</li> <li>• Escalating Incidents, problems to OEM, Vendors for resolving Exchange issues.</li> <li>• Performance tuning of Exchange Service</li> </ul>	R	
9	Ensure Email Archival-User Archive, Compliance Archive, are done as per defined GGL policy.	R	C
10	Ensure to have BCP/DR test as per BCP Plan scheduled by GGL , BCP/DR to be activated as an when needed post GGL approval	R	C

## f. Linux / AIX / HP UNIX Service

**Responsibility matrix**      legend Responsible-R, Co-ordinate-C

Sr no	Linux / AIX / HP UNIX Service	FMS Vendor	GGL
1	Monitoring Uptime of Linux / AIX / Unix Servers including critical Operating System parameters like CPU, Memory, Hard Disk, Network etc.	R	C
2	End-to-end management of AIX Operating system based IBM servers and blade infrastructure	R	C
3	Install Operating systems in DB, App and other servers, Setup OS clustering for DB and other server. Server Builds (Build Images of the Servers to ensure quick restoration )	R	C
4	Monitoring events and responding according to category. Validate the alerts for False-Positives. Fine tune and monitor the OS for warnings and errors and resolve issues proactively	R	C

Sr no	Linux / AIX / HP UNIX Service	FMS Vendor	GGL
5	Managing Disk space, memory, processor and other critical resources directly affecting performance of the applications. React to critical system problems / alerts / warning as they occur	R	C
6	Monitoring System, Application, and Security logs, analyzing for their criticality & suggesting for corrections. OS Spool, Batch Job, OS alerts management and administration	R	C
7	Record keeping of hardware / software inventory, backup register, DR plan, periodic checklist etc. and regular update	R	C
8	Proactively research and identify OS patches and upgrades required to maintain system health.	R	C
9	Create sandboxes and prepare server instances as and when required.	R	C
10	Overall daily management of the SAP Infrastructure environment to ensure service level metrics are maintained	R	C
11	Participate in Internal and External Audits and implement recommendations	R	C

## g. SAP BASIS Support Service

**Responsibility matrix**      legend Responsible-R, Co-ordinate-C

S No	SAP BASIS Support Service	FMS Vendor	GGL
1	Monitoring uptime of SAP Services including SAP ECC, SAP BW, SAP Gateway, SAP CRM, SAP GRC, SAP PO, SAP BO and other SAP environments deployed at GGL. SAP Production and Project Landscape management. Maintain inventory of the system landscape, SAP Data Migration	R	C
2	Transport System configuration, transport deployment to QA ,Production and Production Landscapes	R	C
3	Monitor SAP Database, Index optimization, Reorganization, Space management, DB performance tuning and monitoring.	R	C
4	SAP User Management – User Creation, Role Assignment, Password reset, User and Password parameter management, SOD Checking using GRC system	R	C
5	SAP Events monitoring using Early-Watch-Alerts (EWA) and System Log Monitoring, Tune SAP / DB parameters as per events	R	C
6	Background Job Management, Update Management, Lock Management, Landscape Connectivity, Spool Management, Email / SMS/ WhatsApp message monitoring.	R	C
7	Periodically scan updates available, Support pack upgrade, SAP Enhancement Pack Upgrade (with support from GGL team), Kernel Upgrade in accordance with OS and DB	R	C
9	Create sandbox copies, QA update using system copy	R	C
10	High Availability Management (HA and ERS), Disaster Recovery site log sync, Backup monitoring and troubleshooting	R	C
10	Overall daily management of the SAP environment to ensure service level metrics are maintained	R	C
11	Participate in Internal and External Audits and implement recommendations	R	C
12	Record keeping of all SAP system related checks and above health parameters	R	C

S No	SAP BASIS Support Service	FMS Vendor	GGL
13	SAP Data Migration during upgrades as required by business	R	C

## h. Backup/DLO Service

**Responsibility matrix** legend Responsible-R, Co-ordinate-C

S No	Backup/DLO Service	FMS Vendor	GGL
1	Monitor and ensure High Availability of Backup and DLO Service for Data Management	R	C
2	To provide Support during implementation of Disk Backup Solution. Ensure all Tape based Backup Solution are supported and managed on day to day basis for smooth Operation	R	C
3	Ensure Backup is done for the Wintel and SAP Servers, end user data, Business/Business data based as per GGL policy, all Images of Thin client to be backed up per defined Schedule.	R	C
4	To report the backup failure instances, troubleshoot the issue reported, wherever required involve OEM/Vendor resolving backup failure instances.	R	C
5	Ensure all End user data are properly backed into DLO and troubleshoot if any issue reported with end user data backup in DLO.	R	C
6	Ensure all the backup restoration request is completed on time with no data loss.	R	C
7	Backup media to be stored in Fire Proof Safe & Bank lockers	R	C
8	Period Backup restoration test as per Restoration policy	R	C
9	BCP test per schedule provided by GGL, during Disaster situation activate BCP/DR whenever required post GGL go ahead	R	C
10	Backup media disposal as and when required per Asset Disposal policy	R	C
11	Maintain log sheet on backup taken and have updated Documentation and report of backups taken.	R	C
12	Monitor and reporting on External Storage Media Handling	R	C
13	Perform External Storage Media mounts, Initialize new External Storage Media.	R	C
14	To follow daily health check list and test data restoration by retrieving a randomly selected data and verify the data with application Owner.	R	C
15	To ensure Backup infrastructure is managed end to end	R	C
16	Conduct restoration drills with sample backed up data on a quarterly basis to confirm data integrity and submit report.	R	C

## i. Storage Service

**Responsibility matrix** legend Responsible-R, Co-ordinate-C

S No	Storage Service	FMS Vendor	GGL
1	Monitor and ensure High Availability of Storage devices, Data replication of Business data across GGL	R	C
2	Monitoring SAN and NAS box for critical parameter such as CPU Utilization, Memory Utilization, Volume availability, Volume Free, Uptime Statistics	R	C

S No	Storage Service	FMS Vendor	GGL
3	Storage Administration - Checking SAN, IP SAN and NAS, Checking CIFS, NFS utilization of IPSAN and NAS, Creation of LUN on storage & mapping it to servers. Checking Logical Unit utilization on SAN	R	C
4	Keep track of Asset Inventory, Configuration changes	R	C
5	Create Snap mirrors for replication to DR site as and when required.	R	C
6	Snapshot / Flash copy / Volume copy administration	R	C
7	Perform Disc Quota and Rights/Permission administration. Disk space monitoring, providing space from SAN. Configure Port setting & port zoning.	R	C
8	Add, delete and modify RAID configuration. Add, delete and modify file system configuration. Perform physical disk management.	R	C
9	Install, Configure, and manage (Storage and SAN switches)	R	C
10	Create and map LUNs/Volumes to different servers. Monitor disk space , Perform capacity planning for disc/volumes.	R	C
11	Configure and allocate the required storage capacity to the end users	R	C
12	Gateway ID creation/modification/ deletion.	R	C
13	Coordinating with Principal Vendor for escalated support	R	C
14	Ensure proper storage and handling of media to prevent data loss.	R	C
15	Conduct restoration drills with sample backed up data on a quarterly basis to confirm data integrity and submit report.	R	C
16	Maintain log sheets of backups taken. Check-list/logs generation & upkeep.	R	C
17	Back up policies & replication monitoring between Surat & Ahmedabad & near DR.	R	C
18	Storage Patch Management, Coordinate with vendor to update firmware/hardware patches. Tracking of Patch/IOS versions	R	C
20	Ensure to have BCP/DR test as per BCP Plan scheduled by GGL , BCP/DR to be activated as an when needed post GGL approval	R	C

## j. Network Infra Service

**Responsibility matrix**      legend Responsible-R, Co-ordinate-C

S No	Network infra Service	FMS Vendor	GGL
1	Maintain, manage and ensure availability of the GGL Network infrastructure Components	R	C
2	Monitoring Network Equipment's Hardware Failures, Interface status as per GGL Policy	R	C
3	Monitoring Network Equipment's operation LAN + WAN & recording important parameters (Device availability, CPU, Memory utilization, Packet Drops, Loop back status, Hardware Failures, Interface status) as per policy.	R	C
4	Checking and reviewing Network Equipment system logs, escalating in time if anything found abnormal. Pursuing and following up till resolution.	R	C
5	Liaise with Vendors / OEM in case of failures and provide necessary support to resolve network problems.	R	C



S No	Network infra Service	FMS Vendor	GGL
	Service desk lead to coordinate with ISP/Service provider incase network team is not getting any response.		
6	Record keeping and network documentation as per GGL Policies and procedures	R	C
7	Ensure the Backup of configuration for all network equipment's as per GGL Policy and change Management requirement.	R	C
8	Preparing MIS, trends, analysis reports related to Network.	R	C
9	Providing solution (existing as well as new) for GGL Network initiatives.	R	C
10	Breakdown & preventive maintenance of Network equipment's in coordination with OEM and AMC/Warranty vendors.	R	C
11	Provide network trouble-shooting that includes problem identification, its diagnosis and escalation to the respective support vendor.	R	C
12	BCP Planning for Network Services/Devices		R
13	Documentation of BCP/DR Scenarios, SOP. Performing BCP-DR as per schedule, documenting test results. Improvement plan / Lessons learnt per BCP observations to be deployed.	R	C
14	Configuration Managements of all Network devices, Documenting and version control of the configurations.	R	C
15	Monitor and control configuration aspects like IP address, subnet mask, DNS settings	R	C
16	Monitoring existing IOS & patch installed and managing new IOS upgrades/ Patch Management as per GGL Policy.	R	C
17	Hardening of Network Devices as per GGL policy	R	C
18	Creating new users (Administrative and Privileged) and managing them	R	C
19	Store and document the above configuration and change details in the form of reports.	R	C
20	Project support for network domain.	C	R
21	End to End configuration, Hardware, monitoring & management for network devices for existing as well as new initiatives.	R	C
22	Create dashboard and reports for the Service	R	C
23	Vendor needs to face internal / external and VA PT audit and implement / Deploy the observations and Noncompliance as part of Audit closures actions.	R	C
24	Vendor needs to follow ITIL practices.	R	C
25	Continuous service Improvements must be provided to improve network environment for technical updates and Improvements.	R	C
26	GGL is using Cisco LMS and Entity (Remedy) for Monitoring of network services	R	C
27	Vendor needs to configure all devices and understand NMS tool for day to day operations and changes in configuration for devices, backend Tool Vendor support would be provided to team if first level they are not able to provide the fix.	R	C
28	Vendor need to provide daily dashboards / MIS Reports, continuous improvement to be done for these reports.	R	C



## k. Data Connectivity Service

**Responsibility matrix** legend Responsible-R, Co-ordinate-C

S No	Data Connectivity Service	FMS Vendor	GGL
1	Maintain, manage, monitor and ensure availability of the GGL network services including LAN,WAN, SAN, WLAN ,VPN	R	C
2	Monitoring Network services operation & recording important parameters (Device availability, CPU, Memory utilization, Link Uptime, Bandwidth Utilization, Packet Drops, Loop back status, Hardware Failures, Interface status) as per policy.	R	C
3	Checking and reviewing Network Equipment system logs, escalating in time if anything found abnormal. Pursuing and following up till resolution.	R	C
4	Carryout bandwidth monitoring, usage monitoring and its analysis and suggesting upgrades / downgrades	R	C
5	Liaise with Service providers in case of failures and provide necessary support to resolve network problems. Service desk lead to coordinate with ISP/Service provider incase network team is not getting any response.	R	C
6	Record keeping and network documentation as per policy and procedures.	R	C
7	Provide resolutions for all network related issues.	R	C
8	Ensure the Backup of configuration for all network services as per GGL Policy and change requirement.	R	C
9	Preparing MIS, trends, analysis reports related to Network services and suggesting improvements around this.	R	C
10	WiFi Access Point support – troubleshooting Wireless network issues, incidents, problems and providing timely resolution.	R	C
11	Supporting WiFi Configuration to end users, Configuring, creating registering new WiFi users in WiFi controller.	R	C
12	FMS team to provide Project support for GGL projects and Own network services.	C	R
13	Providing solution (existing as well as new) for GGL requirements of all network devices	R	C
14	Breakdown & preventive maintenance of Network equipment's in coordination with OEM and AMC/Warranty vendors.	R	C
15	Provide network trouble-shooting that includes problem identification, its diagnosis and escalation to the respective support vendor.	R	C
16	Vendor to update and get necessary approval for all changes (hardware and configuration) required to be done in GGL network architecture.	R	C
17	BCP-DR Performing as per schedule, documenting test results.	R	C
18	Documentation of BCP/DR Scenarios, SOP. Performing BCP-DR as per schedule, documenting test results. Improvement plan/Lessons learnt per BCP observations to be deployed.	R	C
19	Create dashboard and reports for the Service	R	C

S No	Data Connectivity Service	FMS Vendor	GGL
20	Vendor needs to face internal/external and VA PT audit and implement observations and Noncompliance came part of Audit / Deploy the observations and Noncompliance as part of Audit closure actions.	R	C
22	Vendor needs to follow ITIL practices.	R	C
23	Continuous service Improvements must be provided to improve network environment for technical updates and Improvements.	R	C
24	Vendor need to provide daily dashboards/MIS Reports, continuous improvement to be done for these reports.	R	C
25	<b>Link Management Services</b> <ul style="list-style-type: none"> <li>Logging calls with Service Provider for calls related to failure</li> <li>Coordinating with respective Service Provider offices/engineers</li> <li>Updating the IT &amp; ERP team of the customer on the progress of the incident</li> <li>Liasioning with Service Providers for uptime for carrier network.</li> <li>Testing of Backup Links etc.</li> </ul>	R	C
26	<b>LAN / WAN / SAN / WLAN /VPN Management</b>	R	C
	• Ensuring the active ports are working properly	R	C
	• Resolve any loose connections between devices	R	C
	• Restart Switches in case of any Hung State	R	C
	• Configure ports / switches	R	C
27	<b>Configuration Management Tasks</b>	R	C
	• Performing network device reconfiguration.	R	C
	• Documenting and version control of the configurations.	R	C
	• Monitor and control configuration aspects like IP address, subnet mask, DNS settings	R	C
	• Performing normal startup and shutdown of routers, switches and modems as part of troubleshooting / administration activities.	R	C
	• Monitoring existing IOS & patch installed and managing new IOS upgrades as per change management process.	R	C
	• Hardening of Network Devices	R	C
	• Creating new users (Administrative and Privileged) and managing them	R	C
	• Store and document the above configuration and change details in the form of reports.	R	C
	• Any design solution and configurations related to existing design would be provided by team	R	C
28	<b>Cabling Management :</b>	R	C
	• Resolving cabling issues reported and registered.	R	C
	• Checking any new requirement and coordinating with cabling contractor for getting the cabling done as per the standards.	R	C
	• Maintaining and documenting all the measurements, drawings and standards.	R	C

S No	Data Connectivity Service	FMS Vendor	GGL
	<ul style="list-style-type: none"> <li>Coordinating with Inventory and arranging for patch cords, cables, connectors, other peripherals as per requirement.</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>Supervising cablings for other projects as per design and standards. Coordinating with cabling service provider for new projects and new offices.</li> </ul>	C	R
29	<b>VPN &amp; Data Card Support:</b>	R	C
	<ul style="list-style-type: none"> <li>Creating, configuring, RSA/VPN connections on Firewall and other periphery devices.</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>BCP DR of RSA/VPN Application</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>Ensure availability of primary and DR sever / Firewall and sync between both sites.</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>Patch management compliance as per GGL policy</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>Proactive review of security patch management</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>Troubleshooting issues, incidents, problems reported by end user for Data Card &amp; VPN Connections.</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>Coordinating with OEM, vendor/service provider for resolution.</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>Continuous monitoring status and usage log analysis of VPN access.</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>Managing inventory of Data Card, RSA Token and coordination with vendor for new requirements.</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>Coordination with RSA server admin for proper troubleshooting.</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>Documentation, Incident, Problem, Change, Release management for VPN.</li> </ul>	R	C
30	<b>Additional activities</b>	R	C
	<ul style="list-style-type: none"> <li>Usage and Bandwidth Analysis</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>Recommendations for upgrades consolidation.</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>Backup &amp; Restore</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>Perform Configuration Backup as per the policy</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>Restore from recent successful backup sets on need basis</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>Patch Management</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>Patch/IOS upgrade as per policy , Tracking of Patch/IOS versions</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>Security patches are applied on priority based on proactive review.</li> </ul>	R	C
	<b>Vendor Coordination:</b>	R	C
	<ul style="list-style-type: none"> <li>Log calls with respective vendors and Coordinate with OEM/Hardware</li> </ul>	R	C
	<ul style="list-style-type: none"> <li>Keep track of Vendor's SLAs, Response and Resolution time and records.</li> </ul>	R	C

## I. Data-Centre Facility Management Service

**Responsibility matrix** legend Responsible-R, Co-ordinate-C

Sr no	Data-Centre Facility Management Service	FMS Vendor	GGL
1	To provide High Availability and Management of all IT & ERP Security devices deployed within Data Centre at GGL.	R	C
2	Monitoring Data Centre Equipment's operation & recording important parameters as per policy	R	C
3	Operation of Data Centre equipment's (AC, UPS, Fire Safety, Water safety etc.) as per the list of equipment's mentioned above & as per the defined GGL procedure.	R	C
4	Breakdown & preventive maintenance of Data Centre equipment in coordination with OEM and AMC/Warranty vendors.	R	C
5	Checking and reviewing Data Centre access logs & CCTV logs. Escalating if anything found abnormal for resolution. Coordinate with Service Providers to ensure routine Preventive Maintenance activities are carried out as per schedule.	R	C
6	Being on call during non-business hours and reach to site within minimum time to attend issues.	R	C
7	Testing BCP DR plans as per schedule, maintaining test results, documentation.	R	C
8	Ensure to have BCP/DR test as per BCP Plan scheduled by GGL , BCP/DR to be activated as an when needed post GGL approval	R	C
9	Ensuring Data Centre security is adhered as per GGL documented policies, procedures and standards. Restricting access to data centre only to the authorized personnel	R	C

## m. Internet Service

**Responsibility matrix** legend Responsible-R, Co-ordinate-C

Sr	Internet Service	FMS Vendor	GGL
1.	Provide High Availability of Internet Service across GGL location and ensure users are able to access all external applications	R	C
2.	Monitoring proxy service performance , Ensuring availability of Proxy Service	R	C
3.	Monitoring Internet Access ( Speed, Bandwidth, URLs)	R	C
4.	User Management for Proxy Access	R	C
5.	Reporting and MIS of Proxy Performance, Internet access.	R	C
6.	Blocking websites as and when required/request by GGL IT & ERP Authorization matrix	R	C
7.	Backup of Proxy Configuration, Data	R	C
8.	Installation, troubleshooting, fault analysis, root cause analysis, fixing the root causes related to proxy and performance tuning.	R	C
9.	BCP Testing as per scheduled and activation in case of disaster.	R	C
10.	Create dashboard and reports for the Service	R	C
11.	Vendor needs to face internal / external and VA PT audit and implement /Deploy the observations and Noncompliance as part of Audit closure actions.	R	C
12.	Vendor needs to follow ITIL practices.	R	C

13.	Continuous service Improvements must be provided to improve network environment for technical updates and Improvements.	R	C
14.	GGL is using mix of Remedy, Motadata and any new tool GGL procure during contract period for Monitoring of network services	R	C
15.	Vendor needs to configure all devices and understand NMS tool for day to day operations and changes in configuration for devices, backend Tool Vendor support would be provided to team if first level they are not able to diagnose.	R	C
16.	Vendor need to provide daily dashboards / MIS Reports, continuous improvement to be done for these reports.	R	C
17.	End to End configuration, Hardware, monitoring & management for security devices for existing as well as new initiatives.	R	C
18.	Project support for network initiative taken during the Contract period	R	C

## n. Network Security Service-

**Responsibility matrix** legend Responsible-R, Co-ordinate-C

Sr no	Network Security Service	FMS Vendor	GGL
1	Maintain, manage and ensure availability of the GGL Network security infrastructure Components	R	C
2	Monitoring Security equipment's Hardware Failures, Interface status as per GGL Policy	R	C
3	Monitoring Security equipment's operation recording important parameters (Device availability, CPU, Memory utilization, Link Uptime, Packet Drops, Loop back status, Hardware Failures, Interface status) as per policy.	R	C
4	Checking and reviewing Network Equipment system logs, escalating in time if anything found abnormal. Pursuing and following up till resolution.	R	C
5	Liaise with Vendors / OEM in case of failures and provide necessary support to resolve network problems.	R	C
6	Record keeping and network documentation as per GGL Policies and procedures	R	C
7	Ensure the Backup of configuration for all network equipment's as per GGL Policy and change Management requirement.	R	C
8	Preparing MIS, trends, analysis reports related to Network.	R	C
9	Providing solution (existing as well as new) for GGL Network initiatives.	R	C
10	Breakdown & preventive maintenance of Security equipment's in coordination with OEM and AMC/Warranty vendors.	R	C
11	Provide network trouble-shooting that includes problem identification, its diagnosis and escalation to the respective support vendor.	R	C
12	BCP Planning for Security Services/Devices		R
13	Documentation of BCP/DR Scenarios, SOP. Performing BCP-DR as per schedule, documenting test results. Improvement plan / Lessons learnt per BCP observations to be deployed.	R	C
14	Configuration Managements of all Security devices, Documenting and version control of the configurations.	R	C
15	Monitor and control configuration aspects like IP address, subnet mask, DNS settings	R	C

Sr no	Network Security Service	FMS Vendor	GGL
16	Monitoring existing IOS & patch installed and managing new IOS upgrades/patch Management as per GGL Policy.	R	C
17	Hardening of Network / Security Devices as per GGL policy	R	C
18	Creating new users (Administrative and Privileged) and managing them	R	C
19	Store and document the above configuration and change details in the form of reports.	R	C
20	Design solution and configurations related to existing design would be provided by team	R	C
21	Project support for security domain.	C	R
22	End to End configuration, Hardware, monitoring & management for security devices for existing as well as new initiatives.	R	C
23	Vendor needs to come with tool for monitoring logs of Security devices, This will collect logs of security devices and provide security reports to GGL Team.	R	C
24	Vendor needs to analyses all security logs (High/medium criticality) and check the applicability	R	C
25	All corrective / Preventive action for security logs must be taken on priority	R	C
26	Security patches must be applied post evaluation with GGL SME and applied as per Change request process.	R	C
27	Upgrade firmware's & patches as on when released by OEM after relevant testing parameters in accordance with ITIL process for the devices being used for delivering the Services.	R	C
28	Create dashboard and reports for the Service	R	C
29	Vendor needs to face internal / external and VA PT audit and implement /deploy the observations and Noncompliance as part of Audit actions closure.	R	C
30	GGL has automatic ticket tool from remedy, so there should be integration by mail format with remedy, So this can be triggered as ticket.	R	C
31	Vendor needs to follow ITIL practices	R	C
32	Continuous service Improvements must be provided to improve network environment for technical updates and Improvements.	R	C
33	Vendor need to provide daily dashboards / MIS Reports, continuous improvement to be done for these reports.	R	C

## o. Video Communication Service

**Responsibility matrix**      legend Responsible-R, Co-ordinate-C

Sr no	Video Communication Service	FMS Vendor	GGL
1	Ensure High Availability of Video equipment's and tracking and monitoring VC bookings.	R	C
2	Supporting in scheduling and coordinating VCs at different locations.	R	C
3	Supporting for connecting VCs. Ensuring Uptime and availability of VC Equipment's as per SLA.	R	C
4	Breakdown and preventive maintenance of VC systems including TV systems.	R	C

Sr no	Video Communication Service	FMS Vendor	GGL
6	Ensuring VC Server operation and availability.	R	C
7	Taking feedback and correcting as per the recommendations.	R	C
8	Coordination and testing of Webcast with External and other parent sites whenever scheduled.	R	C
9	Configuration, activation of features for Webcast and recording test results as and when required.	R	C
10	Performing improvement activities to improve customer satisfaction.	R	C
11	Webcast testing, coordination & support management with GGL and other locations.	R	C
12	Reporting VC operation activities as per VC organizational chart.	R	C
14	Performance tuning and configurations of the VC equipment as per the requirement.	R	C
15	Coordinating with OEM and service provider for the VC related calls and issues.	R	C
16	Maintaining & updating spare inventory & documentation of GGL to support the VC equipment.	R	C
17	Ensuring VC Remote and other equipment batteries and other consumable requirements.	R	C
18	Pre-test and live support during important VCs like executive addresses, public meetings, hall meetings where more participants are there.	R	C
19	Coordination with Network team for any bandwidth related issue and resolving periodically.	R	C
20	Support any change & project activities	R	C
21	Maintaining & publishing VC report & MIS	R	C

## p. Data Centre Infrastructure Management Service

**Responsibility matrix** legend Responsible-R, Co-ordinate-C

Sr no	Data Centre Infrastructure Management Service	FMS Vendor	GGL
1	To ensure High Availability of Server Infrastructure –Blade and Standalone servers deployed within Data Centre	R	C
2.	Breakdown & preventive maintenance of Server Infrastructure – Blade and Standalone servers in coordination with OEM and AMC/Warranty vendors.	R	C
3	Regular Health check of servers and ensure proper Technical support and assistance during Server revamp and consolidation initiatives of IT & ERP	R	C
4	Daily Infrastructure Check list to be maintained and monitor all events /alerts generated by Remedy, Motadata, Nagios tools and ensure appropriate actions are taken against these alerts/events	R	C
5	To collect system resource utilization information, analyze data and generate reports that can be used by GGL to understand how IT & ERP resources are performing and how these resources can be optimized	R	C
6	Ensure to have BCP/DR test as per BCP Plan scheduled by GGL , BCP/DR to be activated as an when needed post GGL approval	R	C



## q. UPS Service

**Responsibility matrix** legend Responsible-R, Co-ordinate-C

UPS service will be managed as per GGL IT &amp; ERP Service Owner requirement/SOP

Sr no	UPS Service	FMS Vendor	GGL
1.	Monitor and ensure High Availability of UPS Service for Business Management.	R	C
2.	Daily UPS status and Service Health Check-up as per schedule for all GGL Offices.	R	C
3.	Performing periodic preventive maintenance of UPS & peripherals through Vendor as per PO Terms.	R	C
4.	Maintain record of new UPS Equipment installed ,movement/replacements of UPS across GGL sites	R	C
5.	Submit monthly UPS Call report & Asset inventory to Services owner.	R	C
6.	Monitoring UPS alerts in monitoring tool and responding to the alerts with proper actions and closure	R	C
7.	Take HSE permit for any UPS related Maintenance for Across the GGL.	R	C
8.	Escalating calls which require spare repairs/replacement by Vendor & pursue till they get repaired /replaced.	R	C
9.	Coordination with the ARC vendor for replacement/disposal of UPS batteries as per GGL contract	R	C
10.	Update Serial No at the time of replacement and keep service call in central location. Prepare UPS services incident call report in Excel Sheet. Add Missing UPS details and update. Preventive Maintenance should be done in every quarter through Vendor. Prepare UPS Vendor details and forwarded to local Helpdesk team for smoothen operation.	R	C

## r. Security Event and Incident Management

**Responsibility matrix** legend Responsible-R, Co-ordinate-C

SNo	UPS Service	FMS Vendor	GGL
1.	Ensure security alerts/events from respective IT & ERP services are available for review	R	C
2.	Ensure security alerts/events are analyzed, evaluated and inference is made out of it to identify risks to GGL IT & ERP Systems	R	C
3.	Ensure security alerts/events are properly stored for ready future reference to avoid any manual interference (in a read only mode)	R	C
4.	Ensure timely review of Security alerts/events so that timely action can be taken to prevent any security incidents	R	C
5.	Ensure alerts/events reporting process/tools are configured for respective team members so that they can take timely & appropriate actions	R	C
6.	Ensure that global security alerts/events trends are also analyzed so that appropriate mechanisms & controls can be aligned / implemented in GGL IT & ERP Infrastructure to deal with such alerts/events	R	C

7.	Ensure that appropriate skills / training are provided to the respective team members to manage Security Event and Incident Management process	R	C
8.	Respective Service Owners are responsible for Event review within agreed thresholds till as such time a centralized SIEM Solution is implemented	R	C

## s. Vulnerability Assessment &amp; Penetration Testing (VAPT) and Mitigation

**Responsibility matrix** legend Responsible-R, Co-ordinate-C

Sr no	Vulnerability Assessment & Penetration Testing (VAPT) and Mitigation	FMS Vendor	GGL
1.	Proactively provide VA assessment for each Information Asset and submission of report to GGL Information Security Officer (ISO) part of GGL Information Security Team member (IST)	R	C
2.	Mitigation of identified vulnerabilities before Induction into IT & ERP Infrastructure with a sign-off from ISO	R	C
3.	Monthly VA review/snapshot of the IT & ERP Infrastructure and submission of report to CISO	R	C
4.	FMS team to coordinate with technical support team / respective team members / SME for closure of action points	R	C
5.	Service desk lead to have meeting with technical support team / respective support team / SME for Tracking and Closure of the Action points as per Minutes of meeting	R	C
6.	Coordination with External auditors for assurance and closure of action points	R	C
7.	GGL also gets a Annual 3 <sup>rd</sup> party VAPT testing done, and coordination for closure of such points shall be in this service scope, at the same time GGL is also planning to implement internal VA Tool which can be run at increased frequency, hence responsibility for execution and closure of points arising shall be in this service scope	R	C

## t. BMC ITSM Platform Management

**Responsibility matrix** legend Responsible-R, Co-ordinate-C

Sr no	Antivirus Service	FMS Partner	GGL
1	To ensure all AD Users Synchronization with ITSM Solution with help of integration service of ITSM Solution and Job scheduling and update time to time.	R	C
2	To ensure all services and server of ITSM Solution up and follow daily checklist to check related services.	R	C
3	Troubleshoot first level issue and provide solutions to End-Users and IT & ERP Team on priority with help of available services and tools.	R	C
4	Log calls with OEM for provide second level solution on priority, till closure make sure take follow-up with vendor or OEM.	R	C
5	Take project management responsibility on any type of change and customization.	R	C
6	Coordinate with vendor to complete change in defined time period or approved Quote.	R	C
7	To ensure all SRDs and Workflow level task are completed at FMS level.	R	C

8	To ensure administrator service of ITSM Solution take care by FMS Team and keep backup of application as per defined policy and timeline.	R	C
9	FMS must follow and keep update asset registers on ITSM Solution.	R	C

## u. IT Asset Management

**Responsibility matrix legend Responsible-R, Co-ordinate-C**

Sr no	IT Asset Management Service	FMS Vendor	GGL
1	Service Owner to ensure that IT Assets are registered/added in the CMDB as soon as they are delivered by vendor to GGL	R	C
2	To ensure IT Assets are updated in the CMDB as soon as they are allocated . All allocated IT Assets must clearly be synchronized with GGL AD & GGL Anti-Virus systems/licenses. Any software that is installed must be as per GGL Authorized Software List and must have explicit approval for installation from GGL and software CMDB must be updated immediately. All asset mappings must be aligned to the assets / peripherals accordingly	R	C
3	To ensure IT Assets are updated with a clear differentiation whether it's in "Working" or "Repairable" condition after due physical verification, in the CMDB as soon as they are de-allocated/removed for end-users. Any license software must be removed except operating system software's. All such IT Assets must clearly be synchronized with GGL AD & GGL Anti-Virus and software CMDB must be updated immediately. All asset mappings must be aligned to the assets / peripherals accordingly	R	C
4	To ensure IT Assets are updated in the IT CMDB Solution as soon as they are identified to be disposed, so that it cannot be considered as a spare. The storage media must be wiped electronically of any trace of data from such assets only then it must be sent for disposal. Once the disposal is completed then the same must updated in the CMDB that includes end-users and core IT Team. All asset mappings must be aligned to the assets / peripherals accordingly	R	C
5	To ensure IT Assets are updated in the CMDB as soon as they are damaged. If the asset cannot be restored then the storage media must be wiped electronically of any trace of data from such assets only then it must be sent for disposal. An Incident Report form must be attached that is initiated by location / core engineer along with end-user. If insurance has been claimed then same must be updated in the CMDB. All asset mappings must be aligned to the assets / peripherals accordingly	R	C
6	To ensure IT Assets are updated in the CMDB as soon the theft is identified. An Incident Report form must be attached that is initiated by location / core engineer along with end-user. If insurance has been claimed then same must be updated in the CMDB. For a laptop end user must provide a FIR (First Information Report) from police station. All asset mappings must be aligned to the assets / peripherals accordingly	R	C
7	If any IT Asset replacement is received under Insurance then the same must be added to the CMDB separately as a new asset after physically verified by FMS Team. All asset mappings must be aligned to the assets / peripherals accordingly	R	C

8	IT Asset compliance reports must be submitted to GGL IT every week from CMDB	R	C
9	Approved Annual IT Asset Inventory Sign-off after physical verification must be submitted to GGL IT every year by 31-Mar based on CMDB at company level Periodic Asset inventory reconciliation (system stock v/s physical stock) shall be carried out as per the requirements laid in this SoW	R	C
10	Ensure the ITSM Asset Management system for is designed, operated, maintained, patched and updated as per the GGL requirement by the respective service owner / administrator	R	C
11	Ensure the Asset discovery is planned properly from frequency and resulting network traffic perspective	R	C
12	Ensure the discovery records are tallied on a monthly basis with the physical verification records	R	C
13	Ensure the policy & audit compliance is ensured as per GGL requirement	R	C
14	Any change the Asset Status has to be updated in the Asset Management System immediately so that it gets reflected and updated across the system on a timely basis (Including Asset Transfer Forms ATF)	R	C
15	Any gaps arising out of the system stock / physical stock and its status should be resolved immediately	R	C
16	Submit quarterly report of full compliance to GGL. The report should be certified by ITIL certified Project Manager and should include physical vis-à-vis system stock for all asset categories.	R	C
17	Team must be share active domain users details with GGL for cross check asset users count.	R	C
18	Ensure sharing of active host details with GGL to cross check users count as per CMDB	R	C
19	Ensure SME will check and confirm to GGL, the relevant asset details as per purchased/procurement PO for CMDB updation	R	C
20	Ensure and keep update to GGL for any changes in the Core Infrastructure environment	R	C

## v. End-Point Security/Anti-Virus

**Responsibility matrix** legend Responsible-R, Co-ordinate-C

Sr no	Antivirus Service	FMS Partner	GGL
1	To ensure all End-user devices and Servers (Virtualized and Standalone) are updated with Antivirus and patches are updated as per policy.	R	C
2	Check Master Antivirus server updated with latest virus definition file, coordination with OEM in case definition file is not updated to latest version.	R	C
3	Scheduling virus definition updates from the Master server to primary and secondary servers, Managing the servers and desktops from the centralized Antivirus console, Regular Antivirus signature update on all desktop/Laptops	R	C
4	Scheduling and performing Antivirus sweep scans across all assets, ensure that the patch / update flows automatically to the desktops across the enterprise.	R	C

5	Taking precautionary actions in terms of definition file updates and interim solutions released during the high alert situations	R	C
6	Troubleshooting virus related incidents, coordination with OEM/Vendor for Virus definition updates	R	C
7	Escalation and coordination with principles for problem resolution	R	C
8	Virus updates to be done manually on servers as per the Policy defined at GGL	R	C
9	Provide Monthly Virus Detections – Action Summary for all desktops and servers for all processes across all locations.	R	C
10	Providing feedback on any new viruses detected. (Limited to real-time observation based on behavioral characteristics)	R	C
11	Registering and updating the anti-virus system periodically as per the policy and procedure followed by GGL	R	C
12	Ensure respective GGL team provide information and access for the Desktops/Servers/Laptops at the time of deployment.	R	C
13	Ensure respective GGL team reboot the Desktops/Servers/Laptops after the deployment of Anti-Virus and periodically patches installation process as it is mandatory process to run effective service of Anti-virus.	R	C
14	If the malware, virus or any malicious definition found on the device, GGL team / GGL user provide the access to device for further analysis of found malware, virus or malicious definition.	R	C
15	All Alerts and Events showing up on the AV-XDR Dashboard (sourced from Endpoints, Servers or ATP) requiring intervention shall be resolved as per agreed SLA	R	C
16	Monthly incident analysis report shall be prepared and submitted to the GGL Service Owner	R	C
17	Periodic / Quarterly incident analysis report shall be prepared and circulated to the GGL Service Owner	R	C
18	Ensure that the Asset details in Anti-Virus XDR system is in sync with other key systems i.e. Active Directory, ITSM, SIEM or any other monitoring system as implemented from time to time	R	C
19	Ensure that the Anti-Virus XDR system is upgraded / updated as per the recommendations from the OEM and approvals from GGL Service owner	R	C
20	Security incidents reported by AV-XDR are resolved as per the SLA	R	C

## w. Endpoint/Server Patch Management

**Responsibility matrix      legend Responsible-R, Co-ordinate-C**

Sr no	IT Asset Management Service	FMS Vendor	GGL
1	To Ensure all Desktops/Laptops/Servers are installed with the BCM Patch Management Agent as they are delivered by vendor to GGL and physically verified by GGL Team.	R	C
2	After successfully patch deployment, all Desktops/Laptops/Servers are rebooted manually with the help of location wise helpdesk or IT service desk.	R	C
3	Ensure that GGL policy of Q-2 (or as required by business) is followed for patching	R	C

4	Coordinate with the respective service owners for authorization to deploy the agreed patches	R	C
5	Ensure that patches are delivered in suitable batches to minimize network / service saturation	R	C
6	Ensure Patch compliance reports are circulated on a Fortnightly basis	R	C

## x. Project Management / Coordination

**Responsibility matrix      legend Responsible-R, Co-ordinate-C**

Sr no	Project Management / Coordination	FMS Vendor	GGL
1	Lead the FMS (EUS + DCS) engagement and ensure contractual deliverables are met. Establish and maintain for operational, tactical, and strategic levels requirements. Conduct periodic review meetings (monthly/quarterly) with all stakeholders	R	C
2	Supervise the Service Desk Lead and ensure proper functioning of the FMS teams. Plan team structure, hiring, performance evaluation, and escalation matrices. Promote knowledge sharing, training, and development of team skills	R	C
3	Plan and align FMS strategy with GGL IT & ERP objectives. Identify opportunities for process improvement, automation, and cost optimization	R	C
4	Will be the primary contact for GGL escalations, feedback, and relationship management. Manage third-party vendors and ensure performance / SLA compliance	R	C
5	Review service performance dashboards and reports submitted by the SDL. Ensure SLA, KPI, and compliance targets are met across all services. Address problems, capacity planning, and resource optimization	R	C
6	Identify operational and compliance issues and close the action points. Ensure compliance with IT Policies & Procedures	R	C
7	Identify operational and compliance issues and close the action points. Ensure compliance with IT Policies & Procedures	R	C

## i. Additional Information

## 1) Clarifications related to various services

- a) In case of following services the DCS FMS Service Provider shall have full responsibility to Drive (Administer, Operate & Monitor) and whereas EUS FMS Service Provider will only support and coordinate with DCS FMS Service Provider

1. Server Virtualization Service
2. Desktop Virtualization Service
3. Wintel Service
4. Directory Service
5. Messaging Service
6. UNIX/AIX Service
7. SAP BASIS Support Service
8. Backup/DLO Service
9. Storage Service
10. Network Service
11. Data Connectivity Service
12. Internet Service
13. Network Security Service



14. Video Communication Service
15. DC Infra Management Service
16. UPS service
17. Security Event and Incident Monitoring
18. Vulnerability Assessment & Penetration Testing (VAPT) and Mitigation
19. IT Assets Management Service (Core-Infrastructure Assets)
- b) EUS RFP clearly specifies following services where EUS FMS Service Provider shall have full responsibility to Drive (Administer, Operate & Monitor) and where DCS FMS Service Provider will only support and coordinate with EUS FMS Service Provider
  1. End User Computing
  2. End-Point Security/Anti-Virus
  3. IT Assets Management Service
  4. Endpoint Encryption Service
  5. BMC ITSM Platform Management
  6. Endpoint/Server Patch Management
- 2) GGL Delivers all Security patches through the centralized ITSM tool for patches that are made available from the OEM on their respective portals
- 3) Physical Asset Verification as required by GGL (Annually & Periodically) is part of the Scope
- 4) Overall ITSM Ticket count may vary between 40-50K per annum
- 5) Currently a team of 2 Service Desk engineers handle the IT Centralized ServiceDesk and overall FMS onsite team shall be led/coordinated by Service Desk Lead
- 6) In case of GGL Senior management the generally the EUS FMS engineers is expected to extend the support a residence of the Senior management, however in rare case DCS FMS engineers may also need to attend to such calls
- 7) GGL has primary data co-located at Gift City Gandhinagar and DR Site at Adajan, Surat. GGL also has installed File Servers at key GA offices and network components for connectivity at respective offices
- 8) Anti-Virus (AV) service has three components (End-User, Server & Network ATP)
- 9) EUS FMS Service providers are responsible for Ticket logging, Coordination and Completion of action points with the AMC/Warranty service providers. GGL has policy of Warranty, AMC or on call repairs for relevant IT & ERP Assets
- 10) All Applications / Services needs to be tested once a year from point of view preparedness to deal with abrupt failure / disasters. Annual plan is prepared which the FMS Service provider has to comply to
- 11) There may be approximately 40-50 IT Service Desk remote calls per month
- 12) Billing Compliance Checklist (Refer Annexure) may change based on the Laws/Regulations/Rules changes by Government from time to time
- 13) BMC ITSM Platform Management (customization) - In case any customization is done then its done only as required under guidance of the BMC Service Provider who is the Service Provider for GGL existing ITSM Solution
- 14) GGL expects the EUS FMS Vendor to consistently work on Service Improvement programs to reduce the repeated incidents @2% MoM
- 15) GGL carries out an Annual VA/PT (Vulnerability Assessment & Penetration Testing) exercise through third party service provider as per GGL Information Security policy to identify security issues, feasibility for closure and resolution of action points. GGL expects FMS Service providers to comply to GGL ISMS (Information Security Management Systems) policy for tracking, addressing such issues identified as part of VAPT exercise
- 16) Preventive Maintenance - EUS FMS Service provider need to carry out Quarterly Preventive Maintenance
- 17) GGL has almost 140+ KEDB articles published under KM Module and FMS Service provider is required to keep the KEDB database updated and enriched from time to time
- 18) Security Event and Incident Monitoring - GGL has implemented tools to monitor certain key Applications/Services i.e. Motadata, DCS and Manual events review. FMS Service provider have



to make use of these existing tools and any other tools/solutions that GGL may invest in to Monitor and Resolve any related issues

19) IT ServiceDesk Catalogue

- VIP support may be required (onsite / remote OR during business / non-business hours) depending on the business requirement
- Please refer to Annexure b for list of End-User Applications used at GGL
- GGL has well defined SOP's for all key areas of IT & ERP systems over and above ISMS & ITSM Policies & Procedures

20) GGL Current ITSM Stack comprises of Old ITSM and New Hardware Tool and respective DCS engineers shall follow same to create, manage, update tickets its status for respective calls. SLA Calculations shall be done on the basis of ITSM Tool only

21) All key locations of GGL have UPS power supply all 7 days a week, however UPS battery backup time may vary depending on business requirements

## 12. ITSM Process Details

The IT & ERP Process/Service SLA are measured based on the target defined against them, following are the major SLA for compliance of defined service/processes. All of these must be captured and reported with Monthly reports. These would be reviewed and if the target is not met Non Performance deduction would be passed on.

- GGL shall expect all Backend Server & Network services available 24 x 7. Front end Hardware services to be made available during GGL Business working timings.
- The availability calculation reference has to be considered as per following.  
Front End Hardware & end user services – Covering weekday's business hours. I.e. 12 x 6 (8.30 to 20.30 x 6 days) = 72 hours per week

Required service availability Targets for GGL:

KPI-ID	Category	Description	Scope	SLA-Monthly target - Updated	Compliance(Quarterly)	Penalty [Non Performance Deductions] Penalty (%) is % of Monthly Invoiced Value of Respective Service Line Item for which KPI has not been complied to
KP003	Server Services	Ensuring Availability	Server Virtualization Service	99.50%	100.00%	2% for every 1% reduction from SLA-Monthly target
KP004	Server Services	Ensuring Availability	Wintel Service	99.50%	100.00%	2% for every 1% reduction from SLA-Monthly target
KP005	Server Services	Ensuring Availability	Directory Service	99.50%	100.00%	2% for every 1% reduction from SLA-Monthly target
KP006	Server Services	Ensuring Availability	Messaging Service	99.50%	100.00%	2% for every 1% reduction from SLA-Monthly target
KP007	Server Services	Ensuring Availability	UNIX/AIX Service	99.50%	100.00%	2% for every 1% reduction from SLA-Monthly target



KP008	Data Backup and Storage Services	Ensuring Availability	Backup/DLO Service	98.00%	100.00%	2% for every 1% reduction from SLA-Monthly target
KP009	Data Backup and Storage Services	Ensuring Availability	Storage Service	99.50%	100.00%	2% for every 1% reduction from SLA-Monthly target
KP010	Network Services	Ensuring Availability	Network Infra Service	99.50%	100.00%	2% for every 1% reduction from SLA-Monthly target
KP011	Network Services	Ensuring Availability	Data Connectivity Service	99.50%	100.00%	2% for every 1% reduction from SLA-Monthly target
KP012	Network Services	Ensuring Availability	Internet Service	99.50%	100.00%	2% for every 1% reduction from SLA-Monthly target
KP013	Cyber Security	Ensuring Availability	Network Security Service	99.50%	100.00%	2% for every 1% reduction from SLA-Monthly target
KP014	VC Services	Ensuring Availability	Video Communication Service	99.50%	100.00%	NA
KP016	Datacenter Services	Ensuring Availability	DC Infrastructure Mgmt. Service	99.50%	100.00%	2% for every 1% reduction from SLA-Monthly target
KP017	Datacenter Services	Ensuring Availability	DC facility Mgmt. Service	99.50%	100.00%	2% for every 1% reduction from SLA-Monthly target
KP018	Network Services	Capacity Utilisation	Network	>50 - <=80	95.00%	NA
KP019	Network Services	Capacity Utilisation	Network Bandwidth	>50 - <=80	95.00%	NA
KP020	Data Backup and Storage Services	Capacity Utilisation	Storage	>50 - <=80	95.00%	NA
KP021	Capacity Management	Capacity Utilisation	Processor/CPU	>50 - <=80	95.00%	NA
KP022	Capacity Management	Capacity Utilisation	Memory	>50 - <=80	95.00%	NA
KP023	Server Services	All Critical, Security, OS/IOS update	Server	(98%) No of patches installed within 90 days of release/Released by OEM	98.00%	2% for every 1% reduction from SLA-Monthly target

KP024	Network Services	All Critical, Security, OS/IOS update	Network devices	(98%) No of patches installed within 30 days of release/Released by OEM	98.00%	2% for every 1% reduction from SLA-Monthly target
KP026	Cyber Security	All Critical, Security, OS/IOS update	Cyber Security	(98%) No of patches installed within 90 days of release/Released by OEM	98.00%	2% for every 1% reduction from SLA-Monthly target
KP027	BCP-DR	DR Testing as per BCP Plan-	Business Services	DR testing - 100% Quarterly	100.00%	2% for every 1% reduction from SLA-Monthly target
KP028	BCP-DR	Data Replication to DR site	Business Services	Successful Data Replication to DR site-100% on daily basis	100.00%	2% for every 1% reduction from SLA-Monthly target
KP029	BCP-DR	Documentation Update	Business Services	(100%) No of SOP documents review completed / SOP Document review DUE within period	100.00%	2% for every 1% reduction from SLA-Monthly target
KP030	Cyber Security	Security log review and applying fixes/treatment	Business Services	(100%) Zero data loss due to Security Incident	100.00%	2% for every 1% reduction from SLA-Monthly target
KP031	Cyber Security	Co-ordination with Third party vendor	Business Services	(100%) Zero data loss due to Security Incident	100.00%	2% for every 1% reduction from SLA-Monthly target
KP032	Cyber Security	Security hardening of all devices as per ISMS policy,ISO27001	Business Services	(100%) Zero data loss due to Security Incident	100.00%	1% for every 1% reduction from SLA-Monthly target
KP033	Documentation	SOP	Business Services	(95%) Within 30 days of Change	100.00%	NA
KP034	Documentation	Manuals	Business Services	(95%) Within 30 days of Change	100.00%	NA
KP035	Documentation	Infrastructure Diagrams	Business Services	(95%) Within 30 days of Change	100.00%	NA
KP036	Documentation	Check list	Business Services	(95%) Within 30 days of Change	100.00%	NA
KP037	Documentation	Knowledge articles	Business Services	(95%) Within 30 days of Change	100.00%	NA
KP038	Documentation	Project Document	Business Services	(95%) Within 30 days of Change	100.00%	NA

KP039	Documen tation	Configuration Document	Business Services	(95%) Within 30 days of Change	100.00%	NA
KP040	Documen tation	Business Communication	Business Services	(95%) Within 30 days of Change	100.00%	NA
KP041	Governan ce	Audit Preparation	All IT & ERP Audits	(100%) P1 to be closed within 15 Days	100.00%	2% for every 1% reduction from SLA- Monthly target
KP042	Governan ce	Participation in Audit	All IT & ERP Audits	(100%) P2 to be closed within 30 Days	100.00%	2% for every 1% reduction from SLA- Monthly target
KP043	Governan ce	Audit point closures	All IT & ERP Audits	(100%) Observation to be closed within 60 days	100.00%	2% for every 1% reduction from SLA- Monthly target
KP044	Project Managem ent	Participation in internal infrastructure improvement initiatives.	IT Projects & Initiatives	(100%) Initiatives completed as per agreed time lines.	100.00%	NA
KP045	Project Managem ent	Infrastructure readiness for all IT & ERP Projects	IT Projects & Initiatives	(100%) Resources provided as per agreed time lines.	100.00%	NA
KP046	Project Managem ent	Operational Takeover of Infrastructure Project in production	IT Projects & Initiatives	(100%) HOTO completed as per agreed time lines.	100.00%	NA
KP047	Asset Managem ent	Inventory review & reporting	IT Assets	100% Monthly	100.00%	2% for every 1% reduction from SLA- Monthly target
KP048	Asset Managem ent	Follow Inventory management processes	IT Assets	100% Monthly	100.00%	2% for every 1% reduction from SLA- Monthly target
KP049	Asset Managem ent	Inventory Add, Move and Remove	IT Assets	100% Monthly	100.00%	2% for every 1% reduction from SLA- Monthly target
KP050	Asset Managem ent	Configuration Update	IT Assets	100% Monthly	100.00%	2% for every 1% reduction from SLA- Monthly target
KP051	Incident Managem ent	Adhere to defined ITSM Incident Management process	All Business Services	(99%) P1-30 mnts-2 hrs	100.00%	2% for every 1% reduction from SLA- Monthly target
KP052	Incident Managem ent	Adhere to defined ITSM Incident Management process	All Business Services	(98%) P2-60 mnts-4 hrs	100.00%	2% for every 1% reduction from SLA- Monthly target
KP053	Incident Managem ent	Adhere to defined ITSM Incident Management process	All Business Services	(95%) P3-2 hrs-6 hrs – 95%	100.00%	2% for every 1% reduction from SLA- Monthly target

KP054	Incident Management	Adhere to defined ITSM Incident Management process	All Business Services	(95%) P4-4hrs-48 hrs	100.00%	NA
KP056	Change Management	Adhere to defined ITSM Change management process	All Business Services	(98%) % of successful changes-100%	98.00%	2% for every 1% reduction from SLA-Monthly target
KP057	Problem Management	Adhere to defined ITSM Problem Management process.	All Business Services	(100%) 10 Knowledgebase Articles per month No of Problem Tickets Raised based on repeat Incidents	100.00%	NA
KP058	Server Services	Adhere to defined ITSM Service Request Management process	All Business Services	(98%) P1-2 hrs-4 hrs	100.00%	2% for every 1% reduction from SLA-Monthly target
KP059	Server Services	Adhere to defined ITSM Service Request Management process	All Business Services	(95%) P2-4 hrs-8 hrs	100.00%	2% for every 1% reduction from SLA-Monthly target
KP060	Server Services	Adhere to defined ITSM Service Request Management process	All Business Services	(95%) P3-4hrs-48 hrs	100.00%	NA
KP061	Server Services	Adhere to defined ITSM Service Request Management process	All Business Services	(95%) P4-8hrs-as agreed	100.00%	NA
KP062	Vendor Management	Coordination/escalation with Third party vendors/ partner	All Business Services	(98%) * As per agreed timelines * No of 3rd Party calls resolved within SLA	100.00%	NA
KP063	Cyber Security	Minimise vulnerabilities in the IT & ERP Infrastructure and Closure of all unapproved vulnerabilities identified in IT & ERP Infrastructure based on VAPT	All Business Services	100% Closure of approved vulnerabilities No unknown vulnerabilities	100.00%	2% for every 1% reduction from SLA-Monthly target

		in a timely manner				
KP064	Cyber Security	Detection & Closure of cyber security threats in a timely manner as per agreed global benchmarks	All Business Services	100% Proactive cyber security threat detection Timely mitigation/resolution of threats	100.00%	2% for every 1% reduction from SLA-Monthly target

Note : Threshold / Values for the KPI mentioned above table will always get over ruled by the respective ITSM / ISMS procedure

### 13. Resources Management

#### a. Onsite Resource-Baseline

GGL wish to have this contract purely based on SLA. Vendor has to manage the numbers as per the SLA requirement. However, as a baseline GGL recommends minimum resource requirements as per the details below. Vendor needs to ensure that below baseline is adhered to in terms of number of resources and their skills mentioned subsequently in this section. GGL will have the option of resource substitution/realignment/combination (FMS/Contractor) based on IT & ERP services catalogue from time to time with mutual understanding.

#### b. Business Hours

- The Working Window for FMS services is defined as twelve hours (8.30–20.30 hours) per day unless otherwise specified. A week is considered as from Monday–Saturday
- All the shifts need to be planned within the Working window
- FMS Vendor will have Holiday as per GGL Holiday list published for that calendar year
- Further, FMS Vendor resources will be available after working hours and on holidays for emergency call response and resolution, subject to request/ approval of Service Desk Manager or Operation Manager

#### c. Resource Deployment Plan

Minimum Resource Deployment Plan – Minimum Resources shall be deployed by bidder as per following table at give location. Further, Bidder can deploy additional resource based on their internal calculation to meet SLAs mentioned in the bid.

GGL may further optimize existing resources deployed going forward based on addition of new location / GA, SLA maintenance of EUS services at location / GA and other parameters. Bidder shall support accordingly.

Details of the existing FMS team deployment is provided herewith to assist the FMS bidder in appropriate planning and deployment of the FMS team for SLA compliance

S.No	GA/Location	Deployment of Core Engineers (FMS Vendor)	Working Hours (including lunch hours)
1	Gandhinagar/Ahmedabad	<ul style="list-style-type: none"> <li>Server L2 (AIX/Unix)</li> <li>Network L3</li> <li>Server L3</li> <li>Server L1</li> <li>UPS / VC Services</li> <li>Network L1</li> <li>Cyber Security</li> <li>Project Lead / Coordinator (Project Management / Coordination)</li> <li>SAP BASIS Support (L2)</li> </ul>	<ul style="list-style-type: none"> <li>10 AM to 6:30 PM</li> <li>10 AM to 6:30 PM</li> <li>10 AM to 6:30 PM</li> <li>08 AM to 4:30 PM</li> <li>10 AM to 6:30 PM</li> <li>11:30 AM to 8 PM</li> <li>10 AM to 6:30 PM</li> <li>10 AM to 6:30 PM</li> <li>10 AM to 6:30 PM</li> </ul>
2	Surat	<ul style="list-style-type: none"> <li>Storage/Backup</li> </ul>	<ul style="list-style-type: none"> <li>09 AM to 5:30 PM</li> </ul>

Note: FMS Vendor need to plan the resource planning/deployment as per the SLA requirements

- d. Minimum Resources shall be deployed as per following table. Bidder may propose additional resources to meet SLAs. (explanation of Resource Deployment Plan). Office location may change as per GGL requirement in future.

- i. FMS Vendor-> Resources that will be deployed by bidder as part of this RFP

S.No	GA / Cluster	GA/Key Location	Core Support Roles (Resource Level)	Bidder's Resource Required
1	Corporate	Ahmedabad – Avdhesh House	VC/UPS Support Engineer (L2)	1
2	Corporate	Gandhinagar - Sector 5	Wintel Server Support(L1) Wintel Server Support (L3) Network Support (L1) Network Support (L3) Cyber Security SOC (L3) AIX/UNIX Server (L2) SAP BASIS (L2)	7
3	Corporate	Gandhinagar	ITIL certified Project Manager/Coordinator for DCS Central Office (L3)	1
4	Surat	Surat	Storage Support L2	1
<b>Total Minimum Resources Required</b>				<b>10</b>

- e. Basic Qualification (as per the attached table).

- i. FMS Vendor must ensure resources deployed for GGL FMS support onsite/offsite should possess the below minimum skill sets based on the role.
- ii. The resources should be well versed with English, Hindi, Local Language (Optional)

S. No	Role	Services to be Managed	Level	Qualification	Experience/Skills
1	Server L1	Virtualization Service	L1	1) Any Graduate with Diploma in Computers/IT/Electronics/Instrumentation	Minimum 3+ Years in Handling Data Center, Microsoft, Virtualization, Backup
		Wintel Service		2) ITIL Foundation Trained	
		Active Directory Service		3) Vendor Certification for L1	
2	Server L2 (AIX / UNIX)	HP-UX and AIX Administration	L2	1) Any Graduate with Diploma in Computers/IT/Electronics/Instrumentation	Min 5-6 Years of experience in AIX, HP-UX Administration. HP-UX and IBM Power VM Cluster Management
		Backup Management		2) ITIL Foundation, IBM AIX, HP-UX Trained	
		Cluster Management		3) Vendor Certification for L2	
3	Server L3	Virtualization Service	L3	1) Graduate in Computers/IT/Electronics/Telecommunication	Minimum 6-7 Years in Handling DC, Microsoft Technologies, Vmware, Hypervisor, Virtualization, VDI Backup, Microsoft Exchange.
		Wintel Service		2) ITIL Foundation Trained	
		Active Directory Service		3) MCSE/MCSA Certified	
		Data Center		4) VMware & Microsoft Hypervisor Trained (Certified Preferred)	



		Infrastructure Management BCP and DR drill management SLB / LLB Management Messaging Services		5) Vendor Certification for L3 in Server Management	
4	Storage L2	Storage Management Service SAN Management Replication Management	L2	1) Graduate in Computers/IT/Electronics/Telecommunication 2) ITIL Foundation Trained 3) Storage (HP, IBM, EMC) Trained (Certified Preferred) 4) Vendor Certification for L2 in Storage Management	Minimum 5-6 Years in Handling DC, VERITAS, Handling Storage of NetApp, EMC, HP and IBM.
5	Network L1	Internet Mgmt Service Data Connectivity Service Network Infra Service	L1	1) Any Graduate with Diploma in Computers/IT/Electronics/Instrumentation 2) ITIL Foundation Trained 3) Vendor Certification for L1 for Network Management	Minimum 3+ Years in Handling CISCO Network, WAN Link management with different vendors, Cabling of UTP, OFC
6	Network L3	Network Security Service Data Center Infrastructure Management	L3	1) Graduate in Computers/IT/Electronics/Instrumentation 2) ITIL Foundation Trained 3) CCNA/CCNP Certified 4) Vendor Certification for L3 for Network 5) To manage Network Security devices	Minimum 6-7 Years in Handling CISCO Network - Switches, Routers, Firewall, IPS, , Proxy, LLB, WAN Links management, MPLS
7	VC/UPS	Video Communication / UPS Service	L1	1) Any Graduate with Diploma in Computers/Electronics/Telecommunications; 2) ITIL Foundation Trained; 3) Vendor Certification for L1	Minimum of 3+ Years in handling IT & ERP Hardware and peripherals
8	SAP BASIS Support	SAP BASIS Support for GGL SAP Landscape	L2	1) Graduate in Computers/IT/Electronics) 2) SAP BASIS trained 3) ITIL Foundation trained	Minimum 5-6 years of SAP BASIS Administration experience on ECC, CRM , BW, PO, Gateway Landscape
9	Cyber Security	Cyber Security Services	L3	1) Graduate in Computers/IT/Electronics) 2) ITIL Foundation Trained; 3) Vendor Certification <ul style="list-style-type: none"> <li>• CEH / CISSP</li> <li>• ISO 27001 (LI / LA)</li> </ul>	Minimum 6-7 Years in Handling Cyber Security formulating Policies, Incident Investigations, SIEM/DLP/NAC implementation

10	Program Manager/Coordinator (Central DCS Project Office)	Project Management		1) Diploma/Graduate in Computers/ Electronics/ Telecommunications/ IT 2) ITIL 4 Foundation OR Managed Professional Certified with minimum 5 years' experience (we can think of having a single Central office for DCS & EUS manned by a single ITIL certified project manager) Minimum Product Skills / Competencies * Managing IT Asset * Managing IT Patching * Managing Roster * Managing Resources * Managing Change delivery * Managing ITSM Policies * Managing cross team / support	Minimum 7-8 Years in Handling 15+ sites Approximately 500+ users ITIL Framework driven ServiceDesk and experience in Server, Network, Service Delivery domains
----	--	--------------------	--	---	--

f. Resource Competencies Groupings

Below is a guidance to the FMS Service provider to utilize domain competencies that are complimenting as well as commonly found so as to cover each domain

- i. Windows Administrators + Storage Administrators
- ii. Network Administrators + Storage Administrators
- iii. Windows Administrators + SAP Basis Administrators
- iv. Network Administrators + Cyber Security Administrators
- v. Cyber Security Administrators + ITSM

**Bidder cannot substitute an L3 for L4 or vice-versa as a backup beyond the PO Terms & Conditions**

g. Specific Skills Requirements

i. Soft Skill – All engineers

- Must be polite and presentable
- Must be able to communicate fluently in Hindi and English
- Must wear proper attire as per GGL policy
- Experience of handling VIP users for required locations
- Good Customer Handling Skills
- Good Troubleshooting Skills
- Good Communication Skills - Verbal & Written
- Very Good Learning Skills
- Good to work with team

ii. Technical Requirements

- Basic Qualification as mentioned above
- Relevant work experience
- Must seek and attend the relevant IT & ERP Training programs
- Must be able to and maintain the respective and relevant documentation
- Must have email etiquettes
- To ensure objectivity and transparency of the preparing various IT & ERP MIS / Reports, GGL is using mix of tools that includes high end ITSM and Monitoring tools like BMC, HP Arch sight and Motadata and any future tool procured by GGL. Hence FMS vendor needs to take this into account and plan resources accordingly. GGL may from time to time upgrade/replace tools accordingly and provide training as required

#### h. Interview / Validation

- i. All resource deployments should be interviewed by GGL.
- ii. FMS Vendor has to first take the understanding from GGL and then take first level interview themselves
- iii. Once the FMS Service provider has identified the potential candidates and carried out preliminary selection, then same shall be interviewed subsequently by GGL also for final selection
- iv. If found suitable for the requirement, they should recommend that resource for GGL interview along with formal assessment as per the above-mentioned basic qualification
- v. After successful interview by GGL, we may take validation test to check the knowledge and suitability with the job requirement. The validation test may be verbal OR written depending on the situation. The same must be recorded properly
- vi. Once confirmation given then only vendor can depute that resource at GGL site
- vii. Vendor to deploy additional resources in case the SLAs are not met with existing resources
- viii. FMS location resources must have competencies to provide L1/L2 services for all services e.g. Switch, UPS, VC, Printer/Scanner etc.
- ix. An induction record has to be maintained for all FMS engineers if the format as required by GGL and as per FMS HR policy and to be produced at the time of audit as required by GGL

#### j. End user Training

- i. FMS Vendor Service delivery staff has to educate and train end user as and when required. This is to improve end user skill set and avoid common problems which can be self-serviced by end user.
- ii. This includes monthly email communication on a particular ITSM (end-user specific) topic and in-person trainings by local / resident engineers to the end-users

#### i. Availability, Leaves / Absenteeism & Communication

- i. FMS Vendor must keep schedule of resources with their availability and absenteeism planned in advance
- ii. Daily morning update on availability of FMS Team members latest by 10am over WhatsApp or mechanism as advised
- iii. SDL has to ensure FMS teams attendance is documented and validated on daily basis from respective sites
- iv. FMS Vendor shall follow GGL leave calendar (except Saturday's) and plan leaves of the team accordingly
- v. Any unplanned absenteeism has to be communicated to GGL in advance and in time to avoid any service outage
- vi. Engineers can be on leave for 2 additional days in addition to Sundays and GGL (Public Holidays)
- vii. In case any engineer is on leave then FMS vendor has to provide backup
- viii. Absenteeism shall be considered very seriously and may lead to disciplinary actions
- ix. Alternate/backup resources should be deployed in case of planned/unplanned absenteeism of the primary resource
- x. In case of any change of FMS engineer the parallel run should be for 15 days and for any other case it has to be one month
- xi. There shall be a disciplinary/penal mechanism defined & implemented by Vendor to deal with engineers who do not report to duty without approval/intimation to Contract Owner / Service Desk Lead
- xii. Project Manager shall certify monthly attendance sheet generated out of the online attendance system of GGL

#### j. Resource Backup

- i. FMS Vendor must keep sufficient resource backup for respective level/role to tackle attrition and other emergencies. These resources can be parallel trained in spare time with deployed resources.
- ii. In case of long leaves or absenteeism (>2 days) of any FMS team member, only these backup resources should be deployed at GGL sites from the nearest site to avoid any delay
- iii. Once original resource comes back then and then backup resource can be relieved from site
- iv. In case of attrition backup resource would automatically become permanent and FMS Vendor has to initiate for another backup resource to avoid any service outage
- v. FMS Vendor should share monthly planned leave calendar of all resources in advance for every month, FMS Vendor should ensure that there is immediate alternate resource with appropriate skills provided in case resource going on leave

**k. Skill Management**

- i. There must be a transition plan (HOTO - Hand Over Take Over) all the way from Service Desk Lead up to an engineer level
- ii. There has to be a definite system in FMS Vendor for skill enhancement of resources, regular training of resources on Latest Technology/tools to Service GGL
- iii. There must be a plan to train the backup resource so that GGL IT & ERP services does not suffer in case any resource decides to leave abruptly

**l. Onsite Team management**

- i. GGL has a zero tolerance towards Cyber Security (Internet/External) and FMS Vendor is prohibited to disclose any GGL information to a third party without explicit permission from GGL Management.
- ii. FMS MUST always and at all times ensure GGL Data/Information security
- iii. The FMS Vendor has to ensure that 2nd & 4th Saturdays are utilized in following ways
  - To complete the pending activities if any so that week's tasks/activities do not spill over to next week
  - To organize ITSM modules/activities training for FMS team members
  - Complete the Asset validation/documentation/verification
- iv. Group gathering outside office within office hours is prohibited without explicit permission from GGL
- v. Lunch timings must be followed as per GGL policy with considering
  - Central Service Desk must be manned at all times during business hours except HSE emergency
  - The core service must be manned at all times wherever there are more than 1 FMS team members
- vi. FMS Vendor to provide list of their offices from where they operate
- vii. Seating space & landline telephone facility will be provided by GGL
- viii. Cell phone (as applicable / required) for official calls shall be provided case to case basis by GGL, otherwise Vendor has to provide
- ix. GGL wants to ensure customer satisfaction and SLA achievement. For this it is FMS Vendor responsibility to ensure whatever level of non-business support is required by their engineers
- x. FMS Vendor should provide recruit and deploy local onsite support staff
- xi. The staffing plan would be assessed by FMS Vendor based on the current Infrastructure details provided by GGL with this document
- xii. FMS Vendor should provide /capable resources who can handle/support the technology deployed and covered under their scope of work at GGL sites
- xiii. FMS Vendor should have adequate resource backup against all services
- xiv. FMS Vendor should not have attrition rate more than 30% during the contract period
- xv. FMS Vendor should replace the resource if GGL IT & ERP team is not satisfied with delivery of FMS services provided
- xvi. FMS Vendor will be accountable and responsible for any damage / loss of GGL property provided to onsite FMS Team for delivering FMS Services
- xvii. FMS Vendor staff should maintain good behavior and should avoid use of Tobacco products/drugs/alcohol within GGL premises, if anyone found violating these clause strict actions such as issuing memo or removing the resource from GGL site
- xviii. FMS Vendor should deploy all resources that have already cleared Vendor internal exams / validation tests
- xix. FMS Vendor will ensure that appropriate IT & ERP Inventory management and support GGL and coordinated by IT ServiceDesk Lead
- xx. FMS vendor will not mobilize or remove any resource from GGL sites without discussion and agreement with GGL
- xxi. FMS Vendor should ensure there is proper handover /takeover plan for smooth transition of responsibility/ activity agreed and signed by GGL IT & ERP before releasing any resource from GGL sites
- xxii. Lodging, boarding and cost for travelling to GGL sites for service support purpose to be borne by FMS Vendor
- xxiii. Onsite resource shall have to travel within states as required at their own cost for the call resolution and project support
- xxiv. Onsite resource shall have to provide support IT arrangement including Network Setup, VC, Webex etc. for the Board / Management meetings

#### 14. Reports Review

FMS Vendor must report as per following requirement to GGL respective in charges. The format can be mutually agreed between FMS Vendor and GGL Service In charge at the time of starting the delivery of the service. The reports are configured in tools (BMC, Motadata, Nagios), FMS Vendor need to ensure these reports are generated on monthly basis. All reports should be certified by ITIL certified Project Manager.

Legend-√ (Responsible)

Sr No	Reports	Daily Report	Weekly Sign-off	Monthly Sign off	Quarterly Sign off
1	Incident Compliance report	√			
2	Service Request Compliance report	√			
3	Infrastructure Availability report	√			
4	Infrastructure Capacity utilization	√		√	
5	Service uptime report	√		√	
6	Resource utilization report	√		√	
7	Asset inventory report with system & physical stock		√	√	√
8	S/W License Compliance report		√	√	√
9	ITSM Process Compliance report			√	√
10	IT Service KPI Compliance report			√	√
11	IT Service Availability Report			√	√
12	Contract Compliance report			√	√
13	Data Centre Uptime/Health report	√		√	
14	FMS Attendance report	√		√	
15	Non Performance deduction report			√	
16	Payment Invoice ( Post deduction of NPD)				√

Note : Other reports / frequency may be decided upon from time to time as per business requirement

**15. Performance review**

There would be performance review of the FMS Vendor as per following frequency.

FMS Vendor shall prepare reports / presentation as per defined / agreed format in the performance review.

S.No	Review	frequency	FMS Vendor	GGL
1	SLA Performance + Non-Performance review	Monthly	Account Manager	Service Delivery/ Service Group Manager, SME
2	SLA & KPI's Performance review	Quarterly	regional Head	IT Lead + Service Delivery Manager
3	Contract performance review	Yearly	Country head	HoD + IT Lead + Service Delivery Manager

All the points will be discussed within GGL and FMS Vendor team. All discussion and decision points would be noted down as a part of MOM as per format attached hereto and the same would be circulated by FMS Vendor to all concerned.

a. Awards and recognition

- i. There must be a plan to train the backup resource so that GGL IT & ERP services does not suffer in case any resource decides to leave abruptly
- ii. If the FMS Service provider exceeds the agreed SLA / Compliance for two consecutive Quarters for the agreed IT Services and processes defined in ITSM Process details, then in such case the FMS Service provider will be entitled for incentive that will be equivalent to 2% of Invoice value of 1 quarter bill. For elaboration purpose, if the two blocks for incentive consideration are Q1 (Month Jan'25, Feb'25 & Mar'25) and Q2 (Month Apr'25, May'25 & Jun'25) then the incentive will be 2% of invoice value of Q1 OR Q2 whichever is lower, subsequently the next two blocks shall only be Q3 (Jul'25, Aug'25 & Sep'25) and Q4 (Oct'25, Nov'25 & Dec'25).
- iii. Cumulative bonus outgo during entire contract period shall not exceed 1% of total basic PO Value
- iv. The FMS contract shall be reviewed periodically to assess whether the desired outcomes are achieved, pain areas are addressed and performance improvement plans are agreed

b. Non-Performance review

- i. Non Performance would be calculated on Monthly basis as per the conditions mentioned against each IT service and ITSM Processes.
- ii. Penalty on resource not deployed on time OR resource or his backup not available on GGL Sites, unless alternate plan agreed with GGL.
- iii. Non Performance deduction (NPD) should be submitted by FMS Vendor in the below format along with monthly reporting to be signed off by GGL.

Resource	L1	L2	L3	Lead
Penalty per Day (Rs)	500.00	1,000.00	2,000.00	5,000.00

Sr.	ITSM Process/ IT Service	Target%	Actual%	Deviation%	% NPD as per agreed SLA	Total % NPD	Cost for that month= V
1	SLA1	X	Y	X-Y=Z	A	A x Z	V = WO value of respective service for month x (AxZ)

2	Resource Non Availability	X1	Y1	$X1-Y1=Z1$	A1	$A1 \times Z1$	$V1 = A1 \times Z1$
	<b>Total NPD = <math>\sum V+V1</math></b>						

- iv. Monthly Non-Performance deductions will be adjusted against Quarterly Invoice., as per applicable tax (if any)
- v. Cumulative Penalty / Non-Performance Deductions during the entire contract period will not exceed 10% of basic PO Value
- vi. FMS vendor shall submit the Invoice on a Quarterly basis between 1-5 of every month after due SLA compliance calculation along with all relevant documents; payment shall be done on Quarterly arrear basis
- vii. If the SLA is not achieved continuously for two months for any of the Services or process, an improvement plan need to be submitted by Vendor in the Quarterly review.
- viii. If the SLA Compliance is not achieved for Consecutive two Quarters for any of the services or process than immediately performance review meeting to be scheduled with IT group head to review the Contract.

## 16. Escalation Management

All services, issues, activities need to be resolved within SLA. For this there is Escalation matrix defined as below: Functional and Hierarchical Matrix for illustrative purposes only.

FMS Vendor needs to follow the escalation matrix defined in individual Service Processes (Incident, Service request, Change etc.) for Escalation to GGL. A summary of the escalation metrics is given below.

Functional Escalation Matrix			
	Infra	Apps	SAP
L0	Service Desk	Service Desk	Service Desk
L1	Domain - L1	Domain - L1	SI Partner - L1
L2	Domain - L2	Domain - L2	SI Partner - L2
L3/SME	Domain - L3/SME	Domain - L3/SME	SI-Partner – L3
Vendor/External Party	Vendor/OEM/TSG	Vendor/OEM	OEM

Hierarchical Escalation Matrix				
	Service Desk, Security, Governance	Infra	Apps	SAP
Function Manager	Vertical Lead	Vertical Lead	Vertical Lead	Vertical Lead
Function Head	IT-Lead	IT-Lead	IT-Lead	SAP-Lead
Group Head	HoD	HoD	HoD	HoD

Technical Escalation Matrix				
Services	L1	L2	L3/SME	Vendor/OEM/TSG
All Business Services	immediately	When 30% of SLA Breached	When 75% of SLA Breached	When 100% of SLA Breached



### 17. Compliance and Audit

- a. GGL Security standards are ISO 27001 compliant. Hence all processes and procedures are established as per ISO 27001 standards
- b. FMS Vendor has to understand and learn all the processes and accordingly comply with all those during service delivery process
- c. FMS Vendor has to be part of Internal and External Audits as per schedule
- d. FMS Vendor team has to face these audits and close all NCs, Observations in time as per SLA
- e. Information Security Compliance:
  - i. Once contract is awarded vendor must sign on Non-Disclosure Agreement with GGL.
  - ii. All the person and people working with GGL must ensure that they must not use any GGL information for any purpose other than official use
- f. Vendor must not try to misuse the privileges given for service delivery
  - i. Rights and Password privileges not to hack OR steal any information out of GGL without GGL consent.
  - ii. Spy or do any kind of malicious activity
- g. In any such cases if proven vendor contract can be terminated as per the notice agreement and the person who performed the activity may get prosecuted under the jurisdiction of law
- h. All the Audit action points have to be tracked and managed centrally on the Portal/CMDB

### 18. Asset and Inventory Management

Asset and inventory management is an important function during service delivery process and same shall be managed by GGL appointed person who has to follow the Asset Management process as per the defined GGL Asset management process. A crucial factor is Physical Verification of all assets and their tagging so that they could be identified, located and managed properly.

NOTE: For lifting and shifting GGL would be arranging proper trained manpower for the vendor who will be professional lifters trained to do that specific job with all HSE compliance. This manpower would be from separate specialized skilled vendor and not required from FMS Vendor. The Asset and Inventory Management includes

- a. Asset Life Cycle
  - i. Registration
  - ii. Allocation
  - iii. Maintaining Spares
  - iv. Dispose
  - v. Lost/Damaged IT Assets
- b. Testing of IT Assets
- c. Use of Spares
- d. Movement of IT Assets
- e. Maintenance
- f. Compliance & Audit
- g. IT Assets Details

Same has been provided as summary and detailed list shall be provided to successful bidder

### 19. Service Desk

GGL is currently using BMC Remedy for service desk management. FMS Team need to be familiar with the tool and use it to effective way to achieve the goals of service management.

- h. Service Desk Tool
  - i. FMS Vendor to deploy resources with skills on BMC ITSM tools, Motadata and any new tool procured by GGL to for monitoring and management of IT & ERP
  - ii. FMS Vendor will record and monitor all incoming tickets/service requests in call management system without fail. These requests maybe directly entered by the users in the call management software/Intranet, Email or maybe received over the phone. Every reported request should be logged in GGL IT & ERP Service delivery tool prior to working on the ticket.
  - iii. FMS Vendor will train the users to log ServiceDesk tickets in an effort to reduce their workload and number of ServiceDesk calls

- i. **Centralized Service Desk & DCS Team**
  - i. FMS Vendor needs to maintain a centralized service desk. GGL would provide necessary infrastructure like sitting place, SIM Card (optional), telephone extension (common), desktop, access to ServiceDesk tool to carry out service desk activities as required. A Mobile phone may be provided based on the separate requirement analysis and approval
  - ii. FMS Vendor would take the calls centrally and then manage them as per the category and priority defined and agreed
  - iii. FMS Vendor has to maintain a centralized service desk preferably at Ahmedabad and the localized service desk separately at different key sites. However customer has choice of calling at centralized OR localized service desk whichever is convenient and faster.
  - iv. FMS Vendor shall ensure that all the calls / requests are logged centrally tracked and acted upon from single location.
  - v. Local service desk team has to be in touch and coordination with centralized service desk.
- j. **Service Desk Coordination**
  - i. FMS Vendor has to ensure availability of mobile phones to all the engineers and delivery team
  - ii. Service Desk Lead has to keep all these numbers handy, printed against sitting place and noted in the mobiles
  - iii. Vendor has to maintain immediate and proper coordination between engineers on the calls and issues without any time loss.
  - iv. Engineer must carry a mobile during business / non-business hours. The same has to be kept ON for any emergency communication by end user with service desk OR GGL IT Team with service desk.
- k. **Monitoring of Infrastructure**
  - i. GGL has deployed multiple tools to Monitor IT Infrastructure & Services availability and capacity management. The reporting processes alerting standards in these tools need to be adhered to have timely escalations and smooth functioning of the IT services however there may also be cases where a specific Application's/Services are being monitored manually
  - ii. FMS Vendor should be able to understand and manage these monitoring tool sets and should have adequate experience in using them
- l. **Support to FMS Vendor**
  - i. GGL has active support agreements with internal and external organizations for the duration of the contract for the tools, systems and third party packages and products in scope used for Infrastructure Management
  - ii. GGL has necessary licenses for third party tools and products so that the FMS VENDOR team can use these third party tools and products
  - iii. Most of the IT & ERP Infrastructure in under Warranty or AMC. There are few infrastructure items without warranty as well. FMS Vendor will be the facility provider to coordinate and ensure timely service and support with external vendors
- m. **Transportation and Logistics**
  - i. FMS Vendor has to ensure transportation and logistics of people and items required during service delivery process.
  - ii. Vendor has to follow HSE transportation rule while travelling for Official purpose
  - iii. Travel to remote locations may be facilitated by GGL on case to case basis and as per the prevailing company policies
- n. **Termination Provision**
  - i. Termination provisions shall be as mentioned under General Terms and Conditions.
  - ii. Upon termination, FMS vendor has to transfer all the data, information & knowledge to the new vendor.
  - iii. Vendor has to ensure that all data, hardware and any associated infrastructure provided for FMS Services is returned to GGL at the time of contract expiry/exit.
- o. **Out of Scope activities**
  - i. Application Helpdesk & Managed Security Services will be managed by a third party
  - ii. This maintenance contract does not cover supply and/or warranty parts or equipment's

## 20. Vendor Management

- a. FMS Vendor team has to timely coordinate with other service providers for effective delivery of services
- b. GGL will share all escalation matrix, contact, call logging procedures and process as agreed between GGL & Service providers
- c. FMS Vendor has to ensure that effort has been put correctly and effectively to resolve all the calls, incidents and problems in time
  - i. FMS team has to co-ordinate with respective vendor/Service provider for delivery/ repair, material verification, installation, Go-Live, invoice submission and Payment.
  - ii. All IT/Asset related invoices, delivery challan's, documents needs to be submitted duly signed and stamped to IT Asset/Procurement Team immediately to avoid any delay in payment.
  - iii. Asset management system / CMDB should be updated at the same time so that it reflected in the asset inventory.
  - iv. Wherever required status has to be updated in the ITSM system as applicable
- d. Service provider coordination has to be recorded in the ITSM tool as per the defined process
  - i. Engineer has to add vendor ticket number in the ticketing tool or communication before making ticket pending with vendor, otherwise it will be treated as non-compliance.
  - ii. These tickets ( pending with vendor) needs to be specifically shared with GGL along with GGL tickets status change data & time, vendor ticket number, reported date & time, response date & time month on month basis.

## 21. Transition/Onboard Plan

- a. FMS Vendor should produce a comprehensive plan and standard by which they will take over and run the IT FMS service as per ITIL framework and GGL Contract
- b. FMS Resources shall be mobilized onsite within 30 days of Contract award
- c. The successful vendor/vendor should take over FMS or transition the service to the new model latest within 30 days of Contract award.
- d. FMS Vendor will have to go through HSE training for safety passport to work at GGL premises
- e. FMS Vendor will have to carry out IT Information asset/Inventory Verification across GGL site as part of Service engagement
- f. FMS Vendor to provide one dedicated Program Manager to ensure that the IT Services will be transitioned in a controlled and fully managed manner that will not have any interruptions to the IT Services
- g. The Migration and Cutover plan Check list to be prepared by FMS Vendor.
- h. FMS Vendor to provide the Transition plan, mentioning transition timelines and Risk with mitigation plan against each IT services.
- i. FMS Vendor to track the progress of transition in Weekly meeting and submit Minutes of meeting
- j. SLA and Compliance and KPI compliance is expected post 2 months of awarding the contract. Vendor to ensure compliance to the KPI and SLA within this period.



- Voice/Data Card Dialer utility, CISCO VPN Connection Utility
- Adobe Acrobat Reader & Writer
- Trend Micro
- Other Application & free software like Win Zip , flash player ,etc
- Auto CAD
- MS EPM &Power BI
- SAP
- Browser based various applications like nProcure, Crisil, GST portals
- Veritas / DLO
- MS Office Products; MS Office with Access
- Pipeline Studio
- Polycom & cisco unified communication applications –Cisco WebEx ,Jabber
- MS SQL Server
- Tally
- MS Visual Studio
- VMS
- XManager
- MS Exchange
- Windows 7,8,10 and new versions FTP/SFTP tools; MS Windows Server
- Cisco
- Checkpoint
- McAfee
- Watchguard
- SynerGee Gas

**b. Induction Checklist For IT & ERP Services**

This document has to be signed off whenever any new ServiceDesk Resource joins at any of the GGL Location. Following checklist needs to be filled up, signed by Location / ServiceDesk In charge and at end signed by ServiceDesk Resource.

The document has to be filed in as a record of induction and to be produced at the time of audit.

SNo	Description (Explained By ServiceDesk Lead and Understood by ServiceDesk Resource)	Sign of Location / ServiceDesk I/C
1	ServiceDesk resource introduced with GGL IT & ERP Team members	
2	Explained the Roles and Responsibilities of each GGL IT & ERP Team member	
3	Provided contact information including mobile, intercom, email of GGL IT & ERP team members	
4	ServiceDesk resource has been briefed about GGL HSE Policy	
5	In-Person guided round of all physical IT & ERP assets in the premises	
	i) Desktops	
	ii) Printers	
	iii) Servers	
	iv) Network	
	vi) VC	
	vii) Others	
6	Explained Operation of all the VC equipment's in premises	
7	Explained the IT & ERP Acceptable Use Policy	
8	Explained Daily Activities/Jobs of ServiceDesk	
9	Explained Escalation matrix in GGL for each Application/Service (e.g. Exchange, Storage , Application)	
10	Explained Voice Communication Etiquettes as per GGL Standards	
11	Explained Email Etiquettes as per GGL Standards	
12	Explained Information Security Policy & rules and regulations	
13	Explained NDA, Confidentiality, Privacy requirements of GGL	
14	Explained ITSM Process flows (e.g. Gadget Request Process)	
15	Completed site visits of relevant locations Corporate office, GA Zonal office as well as its Satellite locations, Warehouses, CNG Stations etc.	
16	Explained GGL SLA	
17	Explained Ticket priorities (user wise. Example - What should be the priority if there is a call from MD office and what should be the priority if there is a call from CNG office etc.)	
18	Explained location specific information i.e. If any switch is hidden in Conference Hall OR a specific device works differently than established standard. Known Issues OR work around	

Agreement of ServiceDesk Resource:

I have gone through all the above points and understood them properly.

Signature:

Name:

Date:

Location:

c. Template of Minutes of meeting

All points discussed in the meeting have to be uploaded on the online Portal in the Action Tracker, Reference template is provided below

[illegible]



## d. Billing Compliance Checklist (For reference only) – This may change from time to time

NAME OF CONTRACTOR				
PO NO.				
INVOICE NO.				
VENDOR CODE				
WAGE MONTH				
Compliance Check List				
Sr. No.	Particulars	Applicable Act	(A) Compliance Required One Time	(B) Compliance Required Monthly
1	Max. no workmen employed during the year		Y	N
2	Copy of Labour License. If workmen are 20 or more	CL(R&A)Act 1970	Y	N
3	Renewl of Labour License (30 day prior on expiry)	CL(R&A)Act 1970	NA	N
4	BOCW license	BOCW 1996	NA	N
5	Payment of Levis under BOCW	BOCW 1996	NA	N
6	PF Registration Certificate	EPF&MP Act 1952	Y	N
7	Salary payment through bank - Bank receipt/Statement		NA	Y As per statutory format
8	Form no. 13 Register of workmen employed under CL(R&A) Act 1970	CL(R&A)Act 1970	Y	Y
9	Form no. 16 Muster roll under CL (R&A) Act 1970	CL(R&A)Act 1970	Y	Y
10	Form No. 17/18 Register of wages/ Muster cum Reg. of wages under CL (R&A) Act 1970	CL(R&A)Act 1970	Y	Y
11	Form No. 19 Wages slip under CL (R&A) Act 1970	CL(R&A)Act 1970	NA	N
12	Form No. 22 Register of advances under CL (R&A) Act 1970	CL(R&A)Act 1970	Y	Y
13	Form No. 23 Register of Overtime under CL (R&A) Act 1970	CL(R&A)Act 1970	Y	Y
14	Form No. 24 Half yearly return under CL (R&A) Act 1970	CL(R&A)Act 1970	Y	N
115	PF challan & ECR copy	EPF&MP Act 1952	NA	Y
16	Undertaking in case if PF challan is common		NA	N
17	Form III (Mini. Wages Act) Annual return	MWA 1948	Y	N
18	I-card Register under Factories Act	Factory Act 1948	NA	N
19	ESI Registration Certificate - (If Applicable)	ESI Act1948	Y	N
20	ESI ECR & Payment Slip (If Applicable)	ESI Act1948	Y	Y
21	WCA Policy under Worker's Compensation Act (If Applicable)	WCA 1923	Y	N