

**REQUEST FOR PROPOSAL (RFP)
FOR
HOSTING & MANAGEMENT OF
GIC RE HYBRID CLOUD
INFRASTRUCTURE**



आपत्काले रक्षिष्यामि
GIC Re

भारतीय साधारण बीमा निगम

General Insurance Corporation of India

Suraksha, 170, J. Tata Road, Churchgate,

Mumbai – 400020

☎ → +91-22-2286 7158; E-mail → itmg@gicofindia.com

Ref. No.: GICRE/ITMG/RFP/05/2021-22

Date of issue of Tender Document: 22nd March 2022

Submit before: 1:00 PM, 22nd April 2022

Table of Contents

GLOSSARY.....	4
SECTION – I: REQUEST FOR PROPOSAL (RFP).....	7
1. INTRODUCTION.....	7
2. OVERVIEW.....	7
3. REGISTRATION OF SERVICE PROVIDERS/ BIDDERS.....	7
4. BROAD REQUIREMENTS OF RFP	7
5. SCOPE OF WORK.....	9
6. PERFORMANCE/ SERVICE LEVEL SUMMARY(SLS) MANAGEMENT.....	47
7. IMPORTANT DATES	49
SECTION – II: INSTRUCTIONS/ GUIDELINES TO BIDDERS.....	51
1. BINDING TO ALL - TERMS & CONDITIONS.....	51
2. PRE-QUALIFICATION CRITERIA (PQC)	51
3. METHOD OF BID SUBMISSION.....	51
4. EARNEST MONEY DEPOSIT (E.M.D.).....	51
5. PREFERENCE TO MICRO AND SMALL ENTERPRISES (MSEs).....	52
6. SPECIAL CONDITIONS FOR STARTUPS	53
7. OPENING OF PRE-QUALIFICATION AND TECHNICAL BID.....	53
8. PROCEDURE FOR PROCESSING THE BIDS.....	53
9. REJECTION OF BIDS	54
10. BID VALIDITY PERIOD	54
11. DEBARMENT FROM BIDDING.....	54
12. CLARIFICATION OF BIDS, SHORTFALL OF INFORMATION/ DOCUMENTS.....	55
13. SERVICE LEVEL AGREEMENT AND PERFORMANCE BANK GUARANTEE.....	55
14. INTEGRITY PACT.....	55
15. CODE OF INTEGRITY.....	55
16. COMPLIANCE WITH INFORMATION SECURITY POLICY.....	56
17. NON DISCLOSURE AGREEMENT.....	56
18. DEED OF INDEMNITY	56
19. GENERAL TERMS.....	57
20. PRICE	58
21. SCHEDULE & PAYMENT TERMS	58
22. LIQUIDATED DAMAGES.....	58
23. TERMINATION OF CONTRACT.....	58
24. DISASTER RECOVERY SUPPORT.....	58
25. INTELLECTUAL PROPERTY RIGHTS.....	58
26. SUB-CONTRACTING	58
27. BIDDER’S UNDERSTANDING OF THE RFP.....	59
28. GOOD FAITH STATEMENT	59

29. PUBLICITY	59
30. ANTI FRAUD AND CORRUPTION	59
31. COMMUNICATION.....	60
32. NON-CONFORMITIES BETWEEN FIGURES AND WORDS:.....	60
33. NO AGENCY:.....	60
34. CONTRACT VARIATIONS.....	61
35. GOVERNING LAW AND JURISDICTION	61
36. RIGHT TO AUDIT	61
37. ADHERENCE TO STATUTORY OBLIGATIONS/ COMPLIANCE WITH LAWS	62
38. NO LEGAL RELATIONSHIP.....	62
39. CANCELLATION OF TENDER PROCESS.....	62
40. VERIFICATION OF DOCUMENTS.....	62
ANNEXURE I.....	63
E-TENDER PROCESS.....	63
ANNEXURE II.....	65
PRE-QUALIFICATION CRITERIA.....	65
ANNEXURE III.....	69
TECHNICAL BID EVALUATION.....	69
ANNEXURE IV.....	75
COMMERCIAL BID.....	75
ANNEXURE V.....	81
SERVICE LEVEL AGREEMENT.....	81
ANNEXURE VI.....	105
PERFORMANCE BANK GUARANTEE.....	105
ANNEXURE VII.....	108
RECIPROCAL NON-DISCLOSURE AGREEMENT.....	108
ANNEXURE VIII.....	114
DEED OF INDEMNITY.....	114
ANNEXURE IX.....	118
UNDERTAKING BY BIDDER.....	118
ANNEXURE X.....	119
CODE OF INTEGRITY	119
ANNEXURE XI.....	120
APPLICATION LANDSCAPE	120
ANNEXURE XII.....	121
NETWORK BANDWIDTH & ENDPOINT DETAILS	121
ANNEXURE XIII.....	122
CURRENT DC & DR SIZING (VIRTUAL AND ORACLE PHYSICAL SERVERS).....	122
ANNEXURE XIV	126
PROPOSED SAP HANA DB CLOUD SIZING	126
ANNEXURE XV.....	127
TECHNICAL BID COMPLIANCE.....	127

GLOSSARY

AD	Active Directory
AMC/ ARC	Annual Maintenance Contract/ Annual Recurring Charges
APT	Advance Persistent Threat
BGP	Border Gateway Protocol
BIW	Business Information Warehouse
BOBJ	Business Object
BOQ	Bill of Quantities
CAPEX	Capital expenditure
CCA	Controller of Certifying Authorities
CCTV	Closed-circuit television
CPE	Customer Premises Equipment
CPPP	Central Public Procurement Portal
CPSE	Central Public-Sector Enterprises
CRM	Customer Relationship Management
DB	Data base
DC	Data Center
DMS	Document Management System
DR	Disaster Recovery
DSC	Digital Signature Certificate
EAA	Enterprise Application Access
EDS	Enterprise Defender Standard
EMD	Earnest Money Deposit
EP	Enterprise Portal
ERM	Enterprise Risk Management
ETP	Enterprise Threat Protection
GCC	Government Community Cloud
GIC Re	General Insurance Corporation of India Reinsurer
HO	Head Office
IDS	Intrusion Detection System
IEMs	Independent External Monitors
ILL	Internet Leased Line
INR	Indian Rupees
IP	Internet Protocol
IPS	Intrusion Prevention System
IR	Incident Request
IS Policy	Information Security Policy
IS-IS	Intermediate System – Intermediate System
IST	Indian Standard Time
IT	Information Technology
ITMG	Information Technology Management Group
JV	Joint Venture

LAN	Local Area Network
LD	Liquidated Damages
LLP	Limited Liability Partnership
LUN	Logical Unit Number
MPLS	Multiprotocol Label Switching
MSEs	Micro & Small Enterprises
MSMEs	Micro, Small & Medium Enterprises
NDA	Non-Disclosure Agreement
NEFT	National Electronic Funds Transfer
NIC	Network Interface Controller
NOC	Network Operations Center
NSIC	National Small Industries Corporation Ltd.
OEM	Original Equipment Manufacturer
OPEX	Operational Expenditure
OS	Operating System
OSPF	Open Shortest Path First
PBG	Performance Bank Guarantee
PERT	Project Evaluation and Review Technique
PI/ PO	Process Integrator/ Process Orchestration
PO	Purchase Order
PQC	Pre-Qualification Criteria
RFP	Request for Proposal
RPO	Recovery Point Objective
RTGS	Real-Time Gross Settlement
RTO	Recovery Time Objective
SAN	Storage Area Network
SASE	Secure Access Service Edge
SB	Selected Bidder
SC/ST	Schedule Castes/Schedule Tribes
SD-WAN	Software Defined Wide Area Network
SEBI	Securities and Exchange Board of India
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SLS	Service Level Summary
SOAR	Security Orchestration & Automation
SOC	Security Operations Center
SOP	Standard Operating Procedure
SOW	Scope of Work
SPLA	Services Provider License Agreement
SR	Service Request
SSD	Solid State Device
VMs	Virtual Machines
VPN	Virtual Private Network
vSAN	Virtual SAN
WAF	Web Application Firewall

WAN	Wide Area Network
ZTNA	Zero Trust Network Access

SECTION – I: REQUEST FOR PROPOSAL (RFP)

1. INTRODUCTION

General Insurance Corporation of India (hereinafter referred to as ‘GIC Re’), designated “Indian Reinsurer”, is a Government of India Company and has been catering to the needs of Indian General Insurance Industry for the past four decades. GIC Re also transacts reinsurance business with foreign insurance and reinsurance companies. GIC Re has been leading the reinsurance programs of several insurance companies in India and the neighboring SAARC countries, Southeast Asia, Middle East, and African continent. To offer its international clientele easy accessibility and efficient service, GIC Re also operates from its branch offices in London, Kuala Lumpur, and subsidiary offices at Moscow, Russia and Johannesburg, South Africa.

2. OVERVIEW

GIC Re’s Data Center (DC) and Data Recovery (DR) sites are hosted and managed for past 5 years by M/s Sify Technologies Ltd. The current architecture is based on MPLS Hub and Spoke model, with two hub locations (DC and DR: Airoli & Bengaluru) and 4 Spoke locations at Delhi, Ahmedabad & Mumbai (Suraksha and Oriental house). Users in all domestic branch offices access both applications and internet through this MPLS setup. Foreign Branch offices are connected to DC via IPsec (site-to-site) VPN. Only application traffic flows through these IPsec links and foreign branches access internet independently. GIC Re has decided to procure services for Hosting and Management of GIC Re’s Hybrid Cloud Infrastructure through an open tender exercise.

3. REGISTRATION OF SERVICE PROVIDERS/ BIDDERS

Besides selecting a Service Provider/ Bidder for the above said requirements, a panel of eligible and capable Bidders will also be created by shortlisting them based on the prequalification and technical criteria in this exercise. The Service Providers/ Bidders so selected will be part of a list of ‘Registered Service Providers/ Bidders’ for providing **RFP for Hosting and Management of GIC Re Hybrid Cloud Infrastructure** to GIC Re. This panel will remain valid for the Contract Period (as defined in **Annexure V**).

4. BROAD REQUIREMENTS OF RFP

GIC Re’s Data Center (DC) and Disaster Recovery (DR) Sites are presently hosted and managed by an external Professional Service Provider. The DC is in Mumbai and DR is in Bengaluru. The current infrastructure in DC and DR infrastructure is in OPEX model.

GIC Re is in requirement of Pay-as-you-Go model services for all its compute, storage, security, and network requirements for its DC and DR sites. This Hybrid Cloud Setup will consist of 3 different Clouds:

- a) **Government Community Cloud (GCC):** All application VMs must be hosted on the GCC and managed by the Selected Bidder. List of current VMs provided in **Annexure XIII**. The Selected Bidder shall migrate the listed VMs from current DC to proposed DC and then setup a DR site as per the Annexure. GIC Re must be able to Scale Up/ Down the VMs, compute, storage, etc. on a Pay-as-you-Go Model for this Cloud.
- b) **SAP HANA Certified Cloud:** For hosting and managing all the HANA DBs as per **Annexure XIV**. The SAP Application VMs hosted in GCC must be able to communicate seamlessly (near-zero latency) with the respective HANA DBs hosted in this cloud. GIC Re must be able to Scale Up/ Down the compute, storage, etc. on a Pay-as-you-Go Model for this Cloud.
- c) **Private Cloud for Oracle DB:** The Selected Bidder shall host and manage 2 Physical Servers for Oracle DB at DC site and 1 at DR site (hereinafter referred to as Oracle Cloud or Oracle Private Cloud), as per sizing in **Annexure XIII**. GIC Re must be able to Scale Up/ Down the compute, storage, etc. on a Pay-as-you-Go Model for this Private Cloud. This setup must be compliant with Oracle’s license requirements.

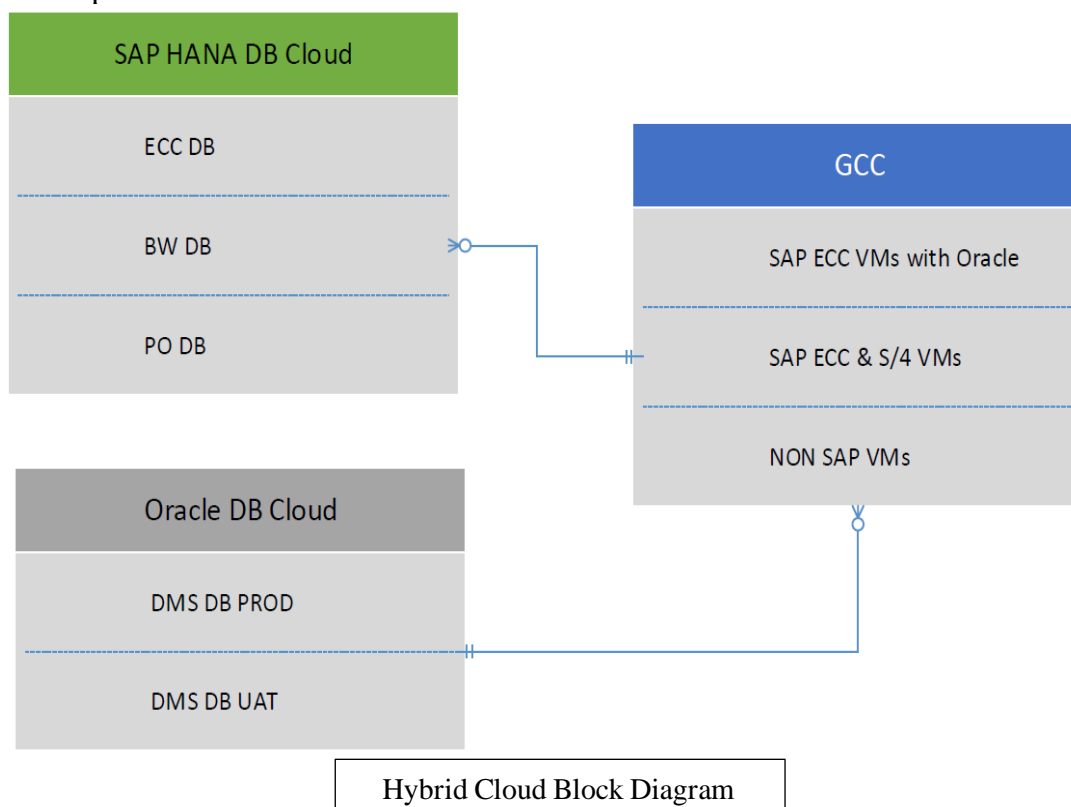
The entire Cloud Setup, including Network, (hereinafter referred to as Hybrid Cloud Infrastructure) for GIC Re should be on a Pay-as-you-Go Model.

For executing this activity, the Selected Bidder shall follow below instructions which are not exhaustive:

- a) The proposed cloud solutions shall be hosted in India-based facilities. The Selected Bidder must certify the same.
- b) The Selected Bidder shall provide at least 99.95% availability & uptime per month.
- c) The proposed solution shall connect all GIC Re's domestic branches over Dual MPLS & Dual ILL links with SD-WAN solution. Bandwidth details mentioned in **Annexure XII**.
- d) The cloud environment shall include the option to connect to internet seamlessly for all web traffic from end-users.
- e) The cloud environment shall have latest cutting-edge security in place. The Selected Bidder shall implement a full-fledged Managed Security Services (MSS) for the entire Hybrid Cloud Infrastructure through its Security Operations Center (SOC). A detailed list of MSS requirements is mentioned in **Table T.4 of Scope of Work** of this document.
- f) The Selected Bidder shall provide 24*7*365 support for the overall environment. The support mechanism must be confirmed by the Selected Bidder with response times. Response times to be mentioned for both Incident and Service Requests.
- g) The Selected Bidder shall have full time CCTV surveillance at the proposed DC & DR sites where cloud setup is being installed.
- h) The Selected Bidder shall provide secure remote connectivity for selected GIC Re's roaming users through SASE ZTNA EDS based technology. The Selected Bidder shall migrate the current SASE ZTNA EDS Solution from current DC to new DC & DR and manage the same with fresh licenses as per Commercial. The details of licensing & capacities provided are to be mentioned in the proposal from the Selected Bidder.
- i) The Selected Bidder shall provide IPSEC Site-to-site VPN for GIC Re's foreign office locations at London, and Kuala-Lumpur. The Selected Bidder must enable connection to these locations by making necessary changes at both end Firewalls for the site-to-site VPN configuration as required. The contact details of branch location are provided on GIC Re's website. Selected bidder shall contact the branches and facilitate the entire process of IPSEC Site-to-site VPN configuration.
- j) The Selected Bidder shall provide valid licenses from OEMs for all components (Hypervisor, OS, DB, MSS, SD-WAN, etc.) and submit certificates from OEMs for the same.
- k) The Selected Bidder shall provide the backup solution as per GIC Re's **indicative backup policy** mentioned in the SOW.
- l) The Selected Bidder shall appropriately size and propose the options of virtual machines and underlying physical servers as per current sizing & proposed HANA sizing given by GIC Re in **Annexures XIII & XIV** respectively. The Virtual environment should not be sized beyond 70% utilization of physical Workload.
- m) The Selected Bidder shall provision processing/ compute, memory, storage, network and security devices, components, licenses, and other fundamental computing resources including Operating system (Windows & RHEL), Databases (Oracle & MSSQL) and Hypervisors. The licenses for these components must be on SPLA Subscription model and must support version upgrades throughout the Contract Period. Only SAP Licensing (App bundled with Oracle DB and HANA DB) and other application licenses will be provisioned by GIC Re. Details provided in **Annexure XI**.
- n) The scope shall include provision of OS licenses for all the Servers (Virtual and otherwise), Hypervisor licenses, OS support subscription from respective OEMs, and DB licenses (Oracle & MSSQL), support, and subscription from respective OEMs (except SAP Oracle & HANA DBs).
- o) The Selected Bidder's Hosting, Implementation & Management Services shall include provision of VMs, configuration of network and security devices, OS installation, DB installation and setup, Hypervisor Installation. Services shall also include setup, configuration, and licensing as per **Annexure XI**.
- p) The Selected Bidder shall ensure IPv6 compliance for the entire solution.
- q) The Selected Bidder's Managed Services shall include (but not limited to) providing up/ down status reporting, backups/ restoration, security, malfunction alarms/ alerts, fault monitoring, incident

management, patch management, performance management, change management (including device configuration, backups, and log reporting), escalation, and resolution; 24*7*365 network monitoring; and online portal-based device/ network availability performance reporting.

- r) Applicable SLAs (for Incident Requests, Service Requests, and Uptime) and Delivery timelines shall be submitted along with the proposed solution.
- s) The proposal shall have deployment and operation support including, but not limited to, design, architecture, implementation, and support of all the proposed components.
- t) The Selected Bidder shall provide compliance, scope of work and SLAs for all Services.
- u) The Selected Bidder shall be solely responsible for migration & implementation of the data, applications, OS, and DBs at proposed DC & DR sites, as mentioned in **Annexures XIII & XIV**.
- v) The Selected Bidder shall provide the complete Hosting & Managed Services for Government Community Cloud (GCC), SAP HANA Certified Cloud and Private Cloud for Oracle DB. The proposed Setup must be a Hybrid Cloud environment comprising of these 3 components on Pay-as-you-Go Model.
- w) The Selected Bidder shall migrate the complete workload from existing Hybrid Cloud to proposed Hybrid Cloud Infrastructure through this RFP.
- x) The Selected Bidder shall propose a solution which shall be scalable, extensible, highly configurable, secure, and very responsive and shall support integration and optimization including scale up and scale down of required services and solutions (existing and acquired in future), designed for, and used by GIC Re.
- y) The Selected Bidder shall provide a complete virtual environment and necessary infrastructure in Pay-as-you-Go model on GCC, HANA & Private Oracle Cloud for the Primary (DC) as well as DR site. The detailed scope of work is mentioned below.



5. **SCOPE OF WORK**

Scope of Work for this RFP is defined below:

A. Cloud Infrastructure Design:

- The Selected Bidder shall migrate GIC Re's complete setup from existing Service Provider's premises to their own DC and DR premises. All necessary installations and configurations are to be done by the Selected Bidder and the bidder must propose a solution strategy to migrate within a specified downtime.

- The Selected Bidder shall ensure minimum downtime while migrating from the existing setup. This should include migrating VMs, data, applications, databases, and associated services. The Selected Bidder should ensure quick and efficient migration. The selected bidder shall submit a detailed migration plan as part of Technical Bid submission.
- The Selected Bidder shall set up and manage the entire cloud solution deployed for GIC Re by Provisioning and Managing Cloud based resources. The Applications for Business Partners in the public domain must be hosted in DMZ and database MZ with WAF.
- The Selected Bidder shall ensure that the DC & DR sites are located within India, in separate seismic zones, and the DC is in Mumbai. GIC Re will undertake yearly audits of the provisioned cloud environment; Selected Bidder is required to facilitate such timely audits as decided by GIC Re.
- The Selected Bidder shall propose the DR site with only VMs & HANA Servers as specified in **Annexures XIII & XIV**. The Selected Bidder shall conduct DR Drills bi-annually in association with GIC Re and its application Service Providers.
- The Selected Bidder shall provide a detailed solution document for setting up of the DC & DR Hybrid Cloud Environment. The same shall be approved by GIC Re project in-charge.
- The Selected Bidder shall provision the entire Hybrid Cloud infrastructure (compute, storage, network, security, software, bandwidth etc.) required for setting up of the DC & DR site as per the approved solution document.
- The Selected Bidder shall adequately size the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels (cloud services) mentioned in the RFP and the application service levels. There should be sufficient headroom (at an overall level in the compute, network and storage capacity offered) available for near real time provisioning (as per the SLA) on a Pay-as-you-Go basis.
- The Selected Bidder shall provide
 - i. the details of the monitoring and management tools,
 - ii. solution for Helpdesk,
 - iii. the manpower deployment details at NOC and SOC,
 - iv. escalation matrix to be adopted,
 - v. the detailed BOQ for Compute, Network, Storage, Security, Backup, and all other components
 - vi. the WAN transformation plan
 - vii. High- and Low-Level Architectural Diagram of entire Setup
 - viii. High- and Low-Level Network Diagram
 - ix. other required details.
- The Selected Bidder shall provide Managed Security Solution & Services (MSS) as mentioned in **Table T.4 of Section T in SoW**, including all hardware, software, and storages as part of the solution. Next Generation Firewalls with UTM features at DC & DR must be provided.
- The Selected Bidder's Scope shall include the proposal for SAP Infra consolidation. SAP Application Servers/VMs should be hosted in GCC in such a way that all SAP client VMs (Development, Quality, Production) will be able to integrate/ communicate with each other and the HANA DB Cloud at near-zero latency.
- The Selected Bidder shall carry out the capacity planning in advance to identify & provision, where necessary, the additional capacity to meet the user growth and/ or the peak load requirements to support the scalability and performance requirements of the solution for the Contract Period. There should not be any constraints on the services. The final decision on capacity addition will be taken in consultation with GIC Re.
- The Selected Bidder shall ensure that all peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to devices, equipment, accessories, software, licenses, tools, etc. should also be provisioned according to the requirements of the solution.
- The Selected Bidder shall ensure that the proposed solution is working as intended and as per GIC Re's satisfaction post migration and implementation.
- GIC Re will not be responsible if the Selected Bidder has not provisioned some components, subcomponents, licenses, assemblies, and sub-assemblies, etc., as part of the bill of material in the

bid. The Selected Bidder shall have to provision the same to meet the solution requirements at no additional cost and time implications to GIC Re.

- The Selected Bidder shall ensure seamless near-zero latency east-west traffic flow between GCC and the other two (2) Clouds.
- The Selected Bidder shall carry out hardening of OS (Operating System), patch and other configuration management activity on all OS, DB, private cloud, and its related software, etc., (which is provided under this RFP) as per the requirement of GIC Re VAPT (Vulnerability Assessment & Penetration Testing)/ audit Observations during the Contract Period as per GIC Re's requirement. Selected Bidder shall undertake BIOS, OS, DB, hypervisor, other software, etc. upgrade whenever required by GIC Re or on recommendation from OEM (during Contract Period). GIC Re conducts VAPT and Information Security audit based on GIC Re's audit policy. The Selected Bidder needs to comply with the findings of the VAPT/ audit in terms of the hardware, software, OS, DB & applications provided under this RFP.
- The Selected bidder shall include a PERT (Project Evaluation and Review Technique) chart of proposed activities required to implement the project as part of Technical Bid Evaluation (**Annexure III**) submission. Once the PO is received, Selected Bidder shall submit the fully filled and detailed PERT chart, location-wise, within 14 days from the date of receiving the PO. The selected bidder shall submit weekly reports on the progress of the project and the status as on the scheduled date and actual date of each activity detailing any deviation from baseline PERT chart. The selected bidder shall take total responsibility for working out all macro and micro level details of the project plan and the requirements while responding to this RFP.
- The Selected Bidder must wipe out all data from existing hardware at the current DC & DR sites, after completing migration activity. The selected bidder should provide proof/certificate for wiping out all data from existing hardware.
- The Cloud services shall be available on pay as per usage model. The billing shall be done monthly/quarterly irrespective of Fixed, On- Demand or mixed model of the Cloud Service Provider. Selected Bidder to provide unit wise Rate Card for all Cloud service components (Compute, Storage, RAM, VMs, Backup, Security, etc.) for this purpose.

B. Deployment of VMs on GCC

- The GCC shall be hosted on an isolated cloud at the Selected Bidder's DC & DR sites, separate from other clouds.
- GCC shall only host Cloud services for Departments/ Ministries/ Agencies/ Autonomous Institutions/ Statutory Bodies/ Offices under Government of India or States or UTs or Local Governments or PSUs within India (herein after referred to as Government Departments).
- The space allocated for the GCC infrastructure should be clearly demarcated and identified as hosting Government Departments' projects. The demarcated and identified area shall not host any components other than those of Government Departments' projects.
- The infrastructure elements including physical server, physical storage (including backup storage) and network equipment in the GCC shall be dedicated only for the Government Departments. There shall be physical and logical separation (of space, servers, storage, network etc.) from the public and other cloud offerings of the Cloud Service Provider. However, these infrastructure elements can be shared (physically only) among the Government Departments within GCC only.
- The entire Network Path for each of GIC Re's applications/ VMs/ Servers shall be logically separate from that of other government departments.
- The Selected Bidder shall ensure seamless near-zero latency east-west traffic flow between GIC Re's GCC, SAP HANA Certified Cloud and Oracle DB Servers. VMs hosted in GCC must be able to communicate with the SAP HANA DB Cloud and Oracle DB Servers at very high throughput/ speed and Near-Zero Latency.
- The entire Network path shall be administered through a Firewall with secured VLAN zoning.
- The Selected Bidder shall administer the Firewall policy as per GIC Re's directions/ existing policy.
- With respect to monitoring tools, agents deployed on the VMs or otherwise, the monitoring tool(s)

may be shared provided there is logical segregation and controls built-in to ensure that the tools & deployed agents comply to the security policies and ONLY the events, performance threshold alerts and inventory data for the OS, DB, infrastructure, and Application is captured & sent by the deployed agents. The monitoring tools and deployed agents (in case of agent-based tools) shall not capture or send GIC Re's application and/ or user and/ or transaction data.

- Security solutions such as UTM, WAF, Anti-Virus, HIPS, Anti-DDoS, Anti-APT, AV, EDR, PIM/ PAM, DLP, etc. shall be deployed (as shared service) for securing applications and servers on GCC, SAP HANA & Oracle Clouds. The Selected Bidder shall deploy and manage EDR and DLP on GIC Re's Endpoints as well. Detailed List for MSS is provided in **Table T.4 of Section T in SoW**.
- The DR Solution shall be on Active (DC) – Standby (DR) mode. DR Deployment shall be automated (one-switch DR) for mission critical Apps/ VMs (list provided in **Annexures XIII & XIV**).

C. Infrastructure Analysis and Build

- Selected Bidder shall provide complete hardware & Software details at DC & DR site including following parameters
 - CPU Calculation
 - RAM Calculation
 - Disk Calculation
 - Network interface requirement
 - Network throughput requirement
 - Backup requirement
 - OS License Requirement
 - DB License Requirement
 - MSS License Requirement
 - SASE ZTNA EDS License Requirement
- Selected Bidder shall provide direct leased-line connections between the DC site and DR for replication.
- Selected Bidder shall provide dual MPLS connectivity from each of GIC Re's domestic branches to DC and DR (Hub-and-spoke Model). Traffic will be shared among the dual links through SD-WAN services. DC & DR will be Hub locations and GIC Re domestic Branches will be spoke locations. All application traffic should flow through these MPLS links.
- Selected Bidder shall provide dual Internet Leased Line connectivity from each of GIC Re's domestic branches/ spoke locations, DC & DR to Internet (local egress/ break-out). All web traffic should locally break-out to internet through these links from each branch.
- Selected Bidder shall size the bandwidth requirements as per table mentioned in **Annexure XII**. It is to be noted that GIC Re mandates for connectivity through established ISPs only.
- Selected Bidder shall implement and manage SD-WAN for entire Network Architecture.
- Proposed Solution should be compatible with IPv6, and Selected Bidder shall provide High-level architectural diagram showing different layers of solution like Internet & MPLS Connectivity, Network, Security, Compute, Hardware, Storage & Backup layers.
- Proposed solution should have IP schema depicted at high level with NATing to secure the applications directly getting exposed to Internet. Such applications facing public domain must be routed through WAF (Web Application Firewall).
- Selected Bidder shall provide Backup solution with different features, like snapshots of VMs, DB backup, incremental and full back up of all data, restoration of data in test environment as and when required. Backup schedule shall be as per GIC Re's IS Policy, which shall be provided to selected bidder.

D. Dynamic Scaling of Resources

- The initial sizing & provisioning of the underlying infrastructure (including the system software and hardware) shall be carried out based on the information provided in the RFP.
- Subsequently, the Selected Bidder shall scale up (or scale down) the resource requirements (compute,

memory, storage, bandwidth, backup, etc.) based on the growth in the compute load/ data load/ bandwidth/ backup load (during peak and non-peak periods / year-on-year increase) to support the scalability (up to 200% or for Contract Period) and performance requirements of the solution and meet the SLAs. There should not be any constraints on the services.

- There should be sufficient headroom (at an overall level in the compute, network, backup, and storage capacity offered) available for near real time provisioning (as per the SLA) during any unanticipated spikes in the user load.
- The scaling up/ scaling down must be carried out with prior approval from GIC Re. Change management Procedure must be followed for every change and GIC Re's approval must be taken.
- The Selected Bidder shall provide the necessary details including the sizing calculations, assumptions, current workloads & utilizations, expected growth/ demand and any other details justifying the request to scale up or scale down.
- For any changes to the underlying cloud infrastructure, hardware, software, etc. under the scope of the Selected Bidder, GIC Re shall get alerts/ notifications from the Selected Bidder, both as advance alerts and post implementation alerts. Monthly utilization reports for entire infrastructure (compute, storage, network, etc.) must be sent to GIC Re.

E. Ownership of Data/ VMs/ Software/ Licenses

- GIC Re shall retain ownership of all data & application licenses hosted on Selected Bidder's infrastructure and shall be able to retrieve full copies of these at any time (without any charges).
- GIC Re retains ownership of all virtual machine's templates, clones, and scripts/applications created for GIC Re's applications. GIC Re retains the right to retrieve full copies of these virtual machines at any time (without any charges).
- GIC Re retains ownership of loaded software/ application installed on virtual machines and any application or product that is deployed by GIC Re on the Hybrid Cloud Infrastructure.
- The Selected Bidder shall procure, implement, and manage licenses for all OS and DB (Windows, RHEL, Oracle (for non-SAP), MSSQL, etc.) for the entire infrastructure. These licenses should be on SPLA model and in the name of the Selected Bidder. Any audits by OEMs regarding GIC Re's usage of these licenses will fall on the Selected Bidder, and it will be their responsibility to assist and comply with the audit/ licensing requirements of OEMs.
- GIC Re will own the licenses of all its applications – SAP, non-SAP, etc. GIC Re will also own and deploy Oracle and HANA DB licenses for its SAP environment ONLY. The Selected Bidder shall manage these DBs (in addition to all the other DBs procured and installed by Selected Bidder in GIC Re's setup).
- All details of license ownership and management are provided in **Annexure XI**.

F. Compliances

- Selected Bidder shall adhere to the standards/ audit requirements/ regulation published (or to be published) or suggested by GIC Re or any standards/ regulator body setup/ recognized by Government of India and notified to the Selected Bidder by GIC Re as a mandatory standard.
- The Selected Bidder's cloud service offerings shall always remain Empaneled / complied with the MEITY guidelines & standards. Selected Bidder shall be responsible for the costs associated with implementing, assessing, documenting, and maintaining such Empanelment/ Compliances.
- The Selected Bidder's proposed DC & DR sites must be listed and valid under GCC section in the Audit Status Tab in below link for the Contract Period:
<https://www.meity.gov.in/content/gi-cloud-meghraj>
- Selected Bidder shall always remain adhered and complied to the prevailing guidelines issued by NCIIPC, RBI, CERT-In etc., from time to time.
- Selected Bidder shall facilitate surprise or planned DC & DR site visits by GIC Re, its auditors and/ or Regulators and comply with all recommendations derived from such visits.
- Selected Bidder shall neither prevent nor impede GIC Re/ auditors/ Regulator from meeting its respective regulatory obligations, nor from exercising its audit/ regulatory powers of conducting

inspection, investigation, obtaining information from the Selected Bidder.

- Selected Bidder shall provide access to all books, records, and information (relevant to this project) to GIC Re, its auditors and Regulators whenever required.
- Selected Bidder shall also assist GIC Re in fulfilling the requirements of the NCCC Project by CERT-In. This project involves setting up Honeypot sensors (2U Rack space) in GIC Re's Cloud Infrastructure, collecting SIEM logs from GIC Re's network and sending it to CERT-In through the public domain (4 public IPs).

G. Documentation

- Selected Bidder shall create and maintain all the necessary technical documentation, design documents, standard operating procedures, configurations required for continued operations and maintenance of cloud services.
- The documents which hold critical information, process, policies shall have to be approved by GIC Re before release.
- The Selected Bidder shall develop, maintain, update following documents as per GIC Re's requirements:
 - Details of inventory for Compute (RAM & CPU), Storage, Network, Security, etc. elements.
 - Details of the management, monitoring and helpdesk tools
 - The WAN connectivity plan
 - Business Continuity/ DR plan
 - Details of manpower deployment at NOC and SOC
 - Escalation matrix
 - Other details as desired by GIC Re.

H. Resource Management

- The Selected Bidder shall manage the instances of storage, compute instances (RAM & CPU), backup and network environments. This includes GIC Re owned & installed application & DB systems (SAP ECC, SAP HANA) and other system software (non-SAP applications) that are outside of the authorization boundary of the Selected Bidder.
- The Selected Bidder shall enable workflow based automatic switch over/failover between DC & DR.
- The Selected Bidder shall provide a webpage and associated Uniform Resource Locator (URL) that describes the following:
 - Service Level Agreements (SLAs)
 - Help Desk and Technical Support
 - Resources (Documentation, Articles/Tutorials, etc.)
 - Inventory

I. Operation Services

- Selected Bidder shall ensure the overall reliability and responsive operation all cloud services through both proactive planning and rapid situational response.
- Selected Bidder shall manage the compute (RAM & CPU), network, storage, server, and virtualization layers, to include performance of internal technology refresh cycles applicable to meet the SLAs.
- Selected Bidder shall ensure monitoring of performance, resource utilization and other events such as failure of service, degraded service, availability of the compute, network, storage, database systems, operating Systems, applications, including application access within the infrastructure.
- Selected Bidder shall prepare a comprehensive O&M plan for managing the cloud services and keep it updated.
- Selected Bidder shall ensure uptime and utilization of the cloud resources as per SLAs defined in this RFP.
- Selected Bidder is required to provision additional VMs/ compute/ storage/ network when the corresponding component utilization exceeds 80% in any Server/ VM/ Network.
- Selected Bidder shall manage the cloud infrastructure as per standard ITIL framework.

- Selected Bidder shall investigate outages, perform appropriate corrective action to restore the hardware, operating system, and related tools. Selected Bidder shall also share RCA report for every incident/ outage.
- Selected Bidder shall design and implement automated scaling processes for the entire Hybrid Cloud Infrastructure.
- Selected Bidder shall provide and implement tools and processes for monitoring the availability of assigned applications, responding to system outages with troubleshooting activities designed to identify and mitigate operational issues.
- Selected Bidder shall provide all administrative support for user registration, User ID creation, maintaining user profiles, granting user access, authorization, user password support, domain creation, domain management, OU & Group creation & maintenance, etc., for Active Directory & DNS services.
- Selected Bidder shall also perform housekeeping activities for all VM, servers, network, backup, etc., and ensure monitoring/ utilization alerts remain below threshold.
- Selected Bidder shall document and perform patch management for entire infrastructure appropriate to the scope of their control and/or provide self-service tools to perform patch management. Any required version/ Software/ Hardware/ OS/ DB upgrades, patch management etc. in the Hybrid Cloud Infrastructure shall be performed by the Selected Bidder for the entire Contract Period at no extra cost to GIC Re. Selected Bidder shall Generate Alerts well in advance on the upcoming patches via email and management portal.

J. Self Service Management/ Provisioning

- Self Service management/ provisioning focuses on capabilities required to assign services to users, allocate resources, and services and the monitoring and management of these resources.
- The Selected Bidder shall provide Self Service Provisioning Portal/ Basic monitoring tool/ Dashboard with two factors authentications via the SSL/TLS or SSH or through a web browser to remotely administer their virtual instances having fine-grained role- based access controls. The tool/ dashboard shall:
 - Enable GIC Re to provision virtual machines, storage, and bandwidth dynamically (or on-demand), on a self-service mode or as requested.
 - Enable service provisioning via online portal/ interface (tools).
 - Enable service provisioning via Application Programming Interface (API).
 - Enable secure provisioning, de-provisioning and administering [such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS) or Secure Shell (SSH)].
 - Support the terms of service requirement of terminating the service at any time (on-demand).
 - Make the Management Reports described in this RFP accessible via online interface. These reports shall be available for 7-year periods after being created.
- The Selected Bidder shall ensure that effective Remote Management features exist for all VM/ Servers with admin privileges so that issues can be addressed by GIC Re & third-party Application Admins in a timely and effective manner. This can be enabled via RDP for Windows VMs/ Servers and SSH access for RHEL VMs/ Servers over MPLS as well as through SASE ZTNA EDS Solution.
- The Selected Bidder shall provide for automatic monitoring of resource, compute, storage, network, backup, etc., utilization and other events such as failure of service, degraded service, etc. via service dashboard or other electronic means. The Utilization Monitoring tools shall have minimum following features:
 - Real time performance thresholds.
 - Real time performance health checks.
 - Real time performance monitoring & Alerts.
 - Historical Performance Monitoring.
 - Capacity Utilization statistics.
 - Cloud Resource Usage including increase / decrease in resources used during auto-scale.
- The Selected Bidder shall provide Trouble Ticketing via online portal/ interface (tools). All such

tickets shall be visible and manageable from the monitoring tool/ dashboard.

- The Selected Bidder shall provide Self Service Provisioning Portal/ Basic monitoring tool/ Dashboard with the ability to automatically provision services via a Web Portal (Self Provisioning), provide meter billing, to provide service assurance for maintenance & operations activities. Detailed user level or user group level auditing, monitoring, metering, accounting, quota, and show-back information is essential for the cloud platform to be offered.
- The Selected Bidder shall support maintenance of user profiles and present the user with his/ her profile at the time of login on the monitoring tool/ dashboard.

K. Data Handling & Management

- The Selected Bidder shall strictly maintain & manage isolation of GIC Re's data isolated from other clients in multi-tenant environment.
- The Selected Bidder shall provide tools and mechanism to GIC Re (or its appointed vendor/ agency) for configuring, scheduling, performing, and managing applications and other related activities (as and when required) of all the data including but not limited to files, folders, images, system state, databases, and enterprise applications through MPLS or SASE ZTNA EDS Solution.
- The Selected Bidder shall facilitate migration/ Transfer of data, either on demand or on termination of contract for any reason.
- The Selected Bidder shall provide and implement security mechanisms for handling data at rest and in transit. Advanced encryption to be used.
- The Selected Bidder shall manage data remanence throughout the data life cycle. The Selected Bidder must not delete any data at the end of the agreement (for a maximum of 90 days beyond the expiry of the Agreement, as per Exit Management Clause) without the express approval of GIC Re.
- When the Selected Bidder (with prior approval of GIC Re) scales down the infrastructure services, Selected Bidder is responsible for deleting or otherwise securing GIC Re's Content/ application/ data prior to VM deletion and in case deleted, shall ensure that the data cannot be forensically recovered. Prior to such VM deletion, a VM/ data backup must be taken and retained for 10 years.
- The Selected Bidder shall strictly maintain confidentiality of GIC Re's data. The Selected Bidder shall perform configuring, scheduling, performing, and managing back-ups and restore activities of all the data including but not limited to files, folders, images, system state, databases, and enterprise applications in an encrypted manner as per the defined policy.
- The Selected Bidder shall provide mechanism to transfer data back in-house either on demand or in case of contract or order termination for any reason. On expiration/ termination of the contract, Selected Bidder shall handover complete data in the desired format to GIC Re which can be easily accessible and retrievable.

L. User Administration (PIM/ PAM)

- The Selected Bidder shall implement Privilege Identity and Access Management (PIM/ PAM) that properly separates users by their identified roles and responsibilities, thereby establishing least privilege principles and ensuring that users have only those permissions necessary to perform their assigned tasks. Only admins designated by GIC Re are to be given privileged access.
- The Selected Bidder shall facilitate Administration of users, identities, and authorizations, effectively managing the root account, as well as any Identity and Access Management (IAM) users, groups, and roles they associated with the user account.
- The Selected Bidder shall implement multi-factor authentication (MFA) for the root account, as well as any Privileged Identity and Access Management accounts associated with it for cloud portal.

M. Cloud Resource and Network Traffic Monitoring

- Selected Bidder shall make provisions to monitor the network traffic in GIC Re's Hybrid Cloud landscape.
- Selected Bidder shall make provisions to analyze amount of data transferred (uploaded/ downloaded), via Internet Traffic through ILL or Application Traffic through MPLS, for each VM/ Server and

endpoints.

- Selected Bidder shall provide network information of cloud virtual resources.
- Selected Bidder shall make provisions to monitor latency between endpoints in each branch of GIC Re and VMs at DC and Internet over MPLS and ILL.
- Selected Bidder shall make provisions to monitor network uptime of each VMs and endpoints.
- Selected Bidder shall make provisions to monitor the uptime of all cloud resources. The report shall be in exportable form.
- Selected Bidder shall make provisions for resource (i.e., CPU, RAM, storage, disk, etc.,) utilization graphs of each VM. There shall be graphs of each disk partition and email alerts should be sent if any threshold of disk partition is breached.
- Selected Bidder shall make provisions to monitor the load of RHEL/ Windows/ DB servers and set threshold for alerts.
- Selected Bidder shall make provisions to monitor the running processes/ services of all servers. This will help GIC Re monitor processes consuming resources.
- Selected Bidder shall make provisions for setting alerts based on defined thresholds. There should be provision to configure different email addresses where alerts can be sent.
- Selected Bidder shall ensure that there should be historical data of minimum 6 months for resource utilization to resolve any billing/ audit disputes if any.
- Selected Bidder shall ensure that audit logs of all servers, OS, DB, network, scalability (horizontal and vertical), etc., are maintained for at least 6 months.
- Selected Bidder shall ensure that log of reaching thresholds used to trigger additional resources in auto provisioning are maintained for at least 3 months.
- Selected Bidder shall ensure that there are sufficient graphical reports of cloud resource utilization and available capacity.
- Selected Bidder shall provide utilization reports for Internet bandwidth (per User, per endpoint, per VM, etc.), load balancers etc.
- Selected Bidder shall monitor and manage all Oracle DBs'. The services shall include (but not limited to):
 - Monitor and manage Table Spaces and health and size of Table space and DB.
 - Monitor live and waiting session.
 - Monitor live processes.
 - Monitor pmon, smon, dbwr, lgwr, ckptr for availability of DB.
 - Monitor and manage Parameters like Redo Logs, redo log Buffer Size, Fixed Area Size, etc.
- Selected Bidder shall provide Monitoring & management of all network links (MPLS, ILL, P2P) proposed as part of this solution.
- Selected Bidder shall monitor parameters for continuous bandwidth utilization, latency, packet loss, jitter, etc.
- Selected Bidder shall provide solution for Monitoring Parameters Buffer Cache Size, Shared Pool Size, etc.

N. Cloud Computing Requirements

N.1. Provisioning of Virtual Machines (VM), Oracle & HANA DBs

1	The Selected Bidder shall do provisioning for required computing resources for hosting of all the required IT applications as listed in <u>Annexures XIII & XIV</u> and all future Applications that GIC Re may on-board. Virtual Machines shall be required to run the variety of workloads such as compute-intensive workload, memory-intensive workload, general-purpose workload, etc. The Selected Bidder shall deploy VMs on Server-Hardware having 1:2 Physical Core to vCPU ratio.
2	The Selected Bidder shall deploy, configure, and manage Oracle and HANA DBs at both DC & DR sites as per sizing mentioned in <u>Annexures XIII & XIV</u> . Selected Bidder shall also consider YoY growth while sizing for Contract Period.
3	The Oracle DB Servers must be deployed in separate Oracle DB Private Cloud, perfectly complying with Oracle Core based licensing requirements.

4	All Application and DB servers shall be deployed on enterprise class Type-I Hypervisor based Virtualized environments.
5	The HANA DB Servers must be deployed in SAP HANA Certified Cloud environment as per sizing provided in Annexure XIV .
6	The Selected Bidder shall ensure that VMs created on GCC are able to communicate at near-zero latency with the DB Servers on the Oracle and SAP HANA DB Clouds.
7	CPU (Central Processing Unit) shall be provided with a minimum equivalent processor speed of 2.4GHz. The CPUs shall support 64-bit operations.
8	GIC Re reserves the right to get the server landscape audited by any third-party auditor, if deemed necessary.
9	The VMs and DB Servers shall be capable of running different operating systems (RHEL, Windows etc.) with any of their variants/ versions.
10	The Selected Bidder shall monitor VM up/ down status and resource utilization such as RAM, CPU, Disk, IOPS and network.
11	GIC Re retains ownership of all VMs, Servers, templates, clones, and scripts/ applications created for GIC Re's applications & DBs.
12	The Selected Bidder shall deploy the entire Infrastructure in HA mode. The proposed setup must have the capacity to automatically reboot any VM & Server in another Host in case of Host Failure.
13	The Selected Bidder shall have provision for live migration of VMs to another physical Host and vice versa in case of predictive Host failure.
14	The Selected Bidder shall provide facility to configure required vCPU, RAM, and Disk, etc.
15	The Selected Bidder shall provision entire infrastructure with All-Flash/ SSD Storage only.
16	The Selected Bidder shall provide, configure, and manage NTP server/ services for entire GIC Re Hybrid Cloud Infrastructure and comply with all necessary audit requirements for the same.

N.2. Administration, Configuration & Training

1	Upon deployment of VMs & Servers, the Selected Bidder must take full administrator access and is responsible for performing additional configuration, security hardening, vulnerability scanning, application installation, troubleshooting, hardening, patch/ upgrades deployment, BIOS & firmware upgrade, DB patches/ upgrade, etc., as, and when required.
2	The Selected Bidder shall ensure Preparation/ Updating of the new and existing Standard Operating Procedure (SOP) documents on servers & applications deployment and hardening.
3	The Selected Bidder shall ensure Patching of VMs, Hypervisor, OS, DB, etc., on the next available patch management change window.
4	The Selected Bidder shall be setting up and configuring servers and applications as per configuration documents/ guidelines/ suggestions provided by GIC Re.
5	The Selected Bidder shall do Installation/ re-installation of the OS and its utilities, DB, and its utilities in the VMs and Servers.
6	The Selected Bidder shall do configuration and maintenance of File Systems of all DBs, perform housekeeping tasks, and perform all DB Administrator responsibilities.
7	The Selected Bidder shall make provisions to Monitor VM & Server up/ down status and resource utilization such as RAM, CPU, Disk, IOPS and network.
8	The Selected Bidder shall monitor availability of the Servers, VMs, OS & system software, DBs, and network.
9	The Selected Bidder shall ensure that VMs & Servers receive OS patching, health checking, Systematic Attack Detection, and backup functions.

10	The Selected Bidder shall arrange training for GIC Re personnel on proposed cloud platforms from OEM and Self-Service portal, with respective certifications.
N.3. Internal Storage Requirements of VMs & DB Servers	
1	The Selected Bidder shall provide scalable, redundant, dynamic cloud-based storage. The initial storage requirement for all VMs/ Servers are provided in Annexures XIII & XIV . The Selected Bidder must size accordingly, considering YoY growth for the Contract Period.
2	The Selected Bidder shall provide All-Flash/ SSD based block storage capabilities on- demand, dynamically scalable per request, for VM & Server instances, of arbitrary size ranging from 1 GB to multiple TBs. Once mounted, the block storage should appear to the virtual machine like any other disk.
3	The Selected Bidder shall enable GIC Re to add either block storage volume or file level storage block to cloud VM from provisioning portal.
4	There must be different disk Space options to allocated for VMs, Servers and file data as per the requirement of GIC Re.
N.4. Network Interfaces & Segmentation of VMs & DB Servers	
1	The Selected Bidder shall ensure that cloud VM & Server network is both IPV4 & IPV6 compatible.
2	The Selected Bidder must ensure that all the cloud VMs & Servers are zoned in different network segments (VLANs) as per GIC Re's requirements. The Selected Bidder must ensure that the VMs in GCC are able to communicate at near zero/ sub-millisecond latency with the DB Servers on the Oracle and SAP HANA DB Clouds through specified ports.
3	The Selected Bidder shall provide Private static IP addresses for all the VMs & DB Servers.
4	The Selected Bidder shall ensure the VMs & Servers provisioned should have minimum 4 no's of 10G vNIC and should be scalable to 25G or 50G each.
5	The Selected Bidder should ensure near-zero/ sub-millisecond latency between all VMs & Servers across the 3 Clouds (GCC, HANA & Oracle) within GIC Re's setup.
N.5. Security of VMs, Servers & Endpoints	
1	All VMs & Servers should be firewall protected and come under the scope of Managed Security Services (MSS).
2	All VMs & Servers should have Host & Network based Security Software.
3	All VMs & Servers should have DLP & Server AV.
4	All Endpoints, of each GIC Re branch, should have EDR (Endpoint Detection & Response) and DLP (Data Leak/ Loss Prevention) features/ solution installed.
5	The Selected Bidder shall deploy a Sandboxing/ Anti-Ransomware tool/ solution for the entire infrastructure. All network traffic (North-South & East-West) shall be examined by this solution and then only will propagate into the network.
6	The Selected Bidder shall provide Identity and Access Management (PIM/ PAM) for managing access to GIC Re users.
7	The Selected Bidder shall perform Hardening & patch management of all VMs, Servers, OS, DB, underlying infrastructure, etc.
8	The Selected Bidder shall perform management of the OS & DB processes and log files of the VMs & Servers.
9	The Selected Bidder shall provide Cloud services that support auditing with features such as what request was made, the source IP address from which the request was made, who made the request, when it was made, login attempts, login failure, software installation attempts, security logs, and so on.

O. Managed Services

O.1. Backup & Restoration	
1	The Selected Bidder shall provide Disk-Based Backup-as-a-Service for entire GIC Re Hybrid Cloud Infrastructure. The Services must be sized as per GIC Re's current Backup schedule and considering growth for the Contract Period. All Backups must be encrypted as per Industry standards.
2	The Selected Bidder shall provide backup solution (Disk based backups), covering but not limited to daily, weekly, monthly, quarterly, and annual backup functions (full volume and incremental) for VM, DB, File system, data and software maintained on the servers and storage systems using Enterprise Backup Solution.
3	The Selected Bidder shall cover (but not limited to) Backup & Restoration of VM images, Operating System, Applications, Databases and File system etc.
4	The solution must have the capability to copy or clone VMs & Servers for archiving, troubleshooting, restoration drill and testing. The Selected Bidder shall perform an Image backup of VM & Servers or support the ability to take an existing running instance or a copy of an instance and export the instance into GIC Re's required format. Entire VM, Server, DB, File System, data, etc., backup must be available to GIC Re.
5	In case of suspension/ decommissioning of a running VM/ Server, the VM/ Server shall still be available for reactivation for a period of 3 months (or more if specified by GIC Re) without having to reinstall or reconfigure the VM/ Server.
6	In case of suspension/ decommission beyond a reasonable time, all the data within VM/ Server shall be immediately deleted/ destroyed and certify to GIC Re that the data has been destroyed as per stipulations and shall ensure that the data cannot be forensically recovered.
7	The Selected Bidder shall configure, schedule, monitor and manage backups of all the data including but not limited to files, images, and databases as per the policy/procedure/plan finalized by GIC Re. The Backup Policy and final schedule will be shared with selected Bidder after RFP.
8	The Selected Bidder shall also perform Administration, tuning, optimization, planning, maintenance, and operations management for backup and restore.
9	The Selected Bidder shall propose cloud-based solution for backup or use a SaaS based/ Third Party Software which shall deployed on VMs & Servers.
10	There shall be a Long-Term Storage option of enforcing WORM (Write Once, Read Many) policy for sections of data that requires the same.
11	The Selected Bidder shall ensure that the solution supports de-duplication at backup server/ host level so that only changed blocks travel through the network to backup devices.
12	The Selected Bidder shall make provision for scheduled file system checks to ensure data integrity.
13	The Selected Bidder shall perform Restoration Drill/ testing quarterly with the permission of GIC Re. The selected bidder must ensure integrity of the data returned during a restore by verifying the block data read with a check sum of the data.
14	The Selected Bidder shall ensure that the backup solution supports 256-bit AES encryption for data at rest and data-in-flight during replication. The backup solution should also support retention lock feature which ensures that no data is deleted accidentally.
15	The Selected Bidder must use a simple file system structure that keeps track of the head of the log to avoid overwriting older data and thereby reduce the chances of data corruption.

16	The Selected Bidder shall provide Real-time monitoring, log maintenance and automated backup reports daily for all VM/ Servers. The backup solution shall provide prompt problem resolution in case of failures in the backup processes and reinitiate such failed backups till successful completion.
17	The Selected Bidder shall make provisions, if required, to shift the backup to GIC Re 's required location on HDD/ USB in retrievable form.
18	The Selected Bidder shall ensure prompt execution of on-demand backups & restoration of VMs, Servers, volumes, files systems and full DBs whenever required, and retain them as per GIC Re 's suggestion.
19	The Selected Bidder shall also perform Redo/ archive log backups of all SAP & DMS Servers. It shall be the collective duty of the Database and Backup Teams of Selected Bidder to rebuild the databases of such servers using the redo/ archive logs in case of any data corruption without suffering any data loss.
20	The Selected Bidder shall perform Real-time monitoring, log maintenance and reporting of backup status on a regular basis.
21	The Selected Bidder shall ensure that all latest and long-term backups taken by current/ outgoing Service Provider must be migrated to the new setup, retained for 10 years and retrievable/ restorable anytime on demand.
22	The Selected Bidder shall make provisions for an offsite/ secondary disk-based backup for audit compliance. Backup data from DC must be copied to another facility of the Selected Bidder (offsite: except DC & DR) monthly. The report and location for the same must also be shared with GIC Re monthly.
23	The backup service must provide following capabilities: Compression: Support compression of data at source before backup Encryption: Support at least 256-bit encryption for data at rest and data-in-flight Alert: Support email notification on backup job's failure File exclusion: Ability to exclude specific files, folders, or file extensions from backup Deduplication: Provide deduplication capabilities A Secondary copy of Backups should be stored in such a way that disaster at either DC or DR or both should not result in loss of backups (offsite).

Indicative Backup plan

#	Backup Type	Backup Frequency	Retention
1	Incremental	Daily	7 Days
2	Full	Weekly	1 Month
3	Full	Monthly	3 Months
4	Full	Yearly	7 Years
5	Transaction/ Archive logs	Every 1 Hour for Production, 3 Hours for Others	1 Week

O.2. Managed Services – Active Directory & DNS

1	The Selected Bidder shall migrate & manage GIC Re 's Active Directory and DNS in its entirety.
2	The Selected Bidder shall maintain and manage GIC Re 's main domain, sub-domains, Domain Controller, Additional Domain Controllers, etc., current and future. This includes the domains(sub-domains) of GIC Re 's foreign branches, which are part of GIC Re 's AD forest.
3	The Selected Bidder shall perform 24*7*365 monitoring of all availability parameters on Domain controllers, Replication & Time Sync, AD Services monitoring, AD Sites.
4	The Selected Bidder shall perform daily health checks. GIC Re must receive reports based on resource utilization, event logs and critical errors based on alerts. All such alerts must be resolved by Selected Bidder.

5	The Selected Bidder shall manage FSMO Roles & Domain Global Catalogue based on alerts and Service Requests raised by GIC Re.
6	The Selected Bidder shall manage replication of AD & DNS to DR Site.
7	The Selected Bidder shall create, remove, and manage sites, domains & subnets as and when required by GIC Re through service requests.
8	The Selected Bidder shall perform AD Object Management such as creation, removal and modification of Users, groups, and OU as and when required by GIC Re through service requests.
9	The Selected Bidder shall perform Group Policy Management such as group policy creation, removal, modification as and when required by GIC Re through service requests.
10	The Selected Bidder shall perform Event Management such as Configuring Event Viewer for AD events, Review Event logs for errors and warnings, Enabling and reviewing DC Audit logs as and when required by GIC Re through service requests.
11	The Selected Bidder shall backup AD & DNS as per Backup Policy & schedule.
12	The Selected Bidder shall be able to restore deleted objects from AD, perform Schema Management and domain creation/ removal as and when required by GIC Re.
13	GIC Re must be notified via phone or email in case of any issues (based on alerts) on any of the above and the Selected Bidder must resolve the issues.

O.3. Managed Services – Windows OS

1	The Selected Bidder shall create new VMs/ Servers with any variant/ version of Windows OS in GIC Re's Hybrid Cloud Infrastructure.
2	The Selected Bidder shall migrate and manage all Windows OS instances (existing and new) in GIC Re's Hybrid Cloud Infrastructure.
3	<p>The Selected Bidder shall perform 24*7*365 monitoring of the following in all Windows VMs & Servers:</p> <ul style="list-style-type: none"> o Availability related parameters o Server reachability from Bidder's tools o Disk space threshold o Scheduled job monitoring o CPU Threshold o Memory Threshold o Critical services o Antivirus updates o Patch updates o Ports o Others
4	The Selected Bidder shall perform health checks, Business readiness checks and checks on Critical processes on all Windows VMs & Servers on daily basis and on basis of service requests (SR) raised by GIC Re.
5	The Selected Bidder shall schedule Automated scripts as and when required by GIC Re or as part of the bidder's activities.
6	The Selected Bidder shall manage Configuration and Parameters of all Windows VMs & Servers.
7	<p>The Selected Bidder shall perform Patch Management of all Windows VMs & Servers with prior approval from GIC Re. These shall include (but not limited to) installation of:</p> <ul style="list-style-type: none"> o Microsoft OS Service packs o Microsoft Windows Security patches o Windows Version Upgrade o Microsoft Hot fixes o other Microsoft software

8	The Selected Bidder shall perform Disk Management of all Windows VMs & Servers by fixing disk space problems by backing up (if required) and deleting files, increasing disk size by allocating disks/ volumes, perform defragmentation on file systems, etc., based on alerts or up on receiving SR from GIC Re.
9	The Selected Bidder shall perform all Change Management on Windows VMs & Servers by creating and following change management procedure document. All Changes must be performed after prior approval from GIC Re.
10	The Selected Bidder shall perform VM/ Server Maintenance (based on alerts or SR from GIC Re) by analysing and fixing problems due to Excess swap memory, Physical memory, CPU & RAM utilization.
11	The Selected Bidder shall perform functions given below related to Problem Management of all Windows VMs & Servers (based on alerts or SR from GIC Re): o Monitor, record and resolve all operating system problems o Carry out comprehensive problem analysis and share RCA reports with GIC Re o Start/stop services/process and restart servers to provide workarounds
12	The Selected Bidder shall perform File System (FS) Creation & Management (based on alerts or SR from GIC Re) by creating NTFS or FAT32 file systems, copying/ moving existing file/ folder to new file/ folder.
13	The Selected Bidder shall perform File & Folder Access Management (based on alerts or SR from GIC Re) by giving access to files/ folders, sharing level permissions to local windows users (Read/ Write/ Modify), etc. All such access reports must be shared with GIC Re on demand.
14	The Selected Bidder shall perform Service Trend Analysis and analyse the utilization of resources in peak hours and off-peak hours. Monthly Utilization reports must be sent to GIC Re.
15	The Selected Bidder shall perform and facilitate all sorts of Audits on Windows VMs & Servers (including AD) like below and send monthly reports to GIC Re: o System security- password strength, users' permissions o System Access – login attempts, failures, FS access o AV events o Windows service packs o Unauthorized application/services usage/ installation
16	The Selected Bidder shall perform OS hardening of all VMs & Servers and share the hardening policy with GIC Re if required.

O.4. Managed Services – RHEL & JBOSS EAP

1	The Selected Bidder shall create new VMs/ Servers with any variant/ version of RHEL OS in GIC Re's Hybrid Cloud Infrastructure.
2	The Selected Bidder shall migrate and manage all RHEL instances (existing and new) in GIC Re's Hybrid Cloud Infrastructure.

3	<p>The Selected Bidder shall perform 24*7*365 monitoring of the following in all RHEL VMs & Servers:</p> <ul style="list-style-type: none"> o Availability related parameters o Server reachability from Bidder's tools o Disk space threshold o Scheduled job monitoring o CPU Threshold o Memory Threshold o Critical services o Antivirus updates o Patch updates o Ports o Others
4	<p>The Selected Bidder shall perform health checks, Business readiness checks and checks on Critical processes on all RHEL VMs & Servers on daily basis and on basis of service requests (SR) raised by GIC Re.</p>
5	<p>The Selected Bidder shall perform scheduled job management of all planned/ scheduled activities, like below, in all RHEL VMs & Servers:</p> <ul style="list-style-type: none"> o Scheduling jobs in Cron o Automated scripts o Timely log rotation o Backup system configuration o Sync/ replication
6	<p>The Selected Bidder shall perform Configuration Management by tracking the configuration items of all RHEL VMs & Servers for purpose of locating corruptions and necessary remediation to be done. The Selected Bidder shall then Manage (Modify/Delete) the OS related configurations in concurrence with GIC Re.</p>
7	<p>The Selected Bidder shall perform Patch Management of all RHEL VMs & Servers with prior approval from GIC Re. These shall include (but not limited to) installation of:</p> <ul style="list-style-type: none"> o RHEL Patch Updating – Monthly o Critical patches – Immediately after the notification and acceptance from GIC Re. o RHEL Version upgrade – based on SR from GIC Re
8	<p>The Selected Bidder shall perform Log Management of all RHEL VMs & Servers regularly:</p> <ul style="list-style-type: none"> o Monitor all the systems logs for any events (warnings and exceptions) and notify to GIC Re for further actions if GIC Re's interaction is needed. o Troubleshooting the systems based on messages and security logs o Periodic log rotation (Weekly/Monthly as per GIC Re's policy)
9	<p>The Selected Bidder shall perform and facilitate all sorts of Audits on all RHEL VMs & Servers like below and send monthly reports to GIC Re:</p> <ul style="list-style-type: none"> o System security- password strength, users' permissions o System Access – SUDO access, login attempts, failures, FS access o AV, SIEM events o Unauthorized application/services usage/ installation
10	<p>The Selected Bidder shall perform User Management and be responsible for entire user lifecycle (based on alerts or SR raised by GIC Re) across all RHEL VMs & Servers. This will include (but not limited to):</p> <ul style="list-style-type: none"> o User Creation/ Deletion o Define password policies, password resets o User Permission & access o User quota management o Direct Root access will not be shared, instead SUDO access will be provided.

11	<p>The Selected Bidder shall handle the complete management of disk (based on alerts or SR raised by GIC Re) on all RHEL VMs & Servers. This will include (but not limited to):</p> <ul style="list-style-type: none"> o Initializing disks o Maintaining disk health o Managing disk organization o Addition/ Removal of disks o Raid configuration o LVM Configuration and Management
12	<p>The Selected Bidder shall ensure that the system resources are being effectively and efficiently used to meet the goals on all RHEL VMs & Servers by performing the following activities (but not limited to):</p> <ul style="list-style-type: none"> o Pro-active monitoring of OS o Swap memory tuning o RAM utilization monitoring o CPU utilization monitoring o Disk utilization monitoring o User/ access alerts o Notification of alarms/ alerts to GIC Re
13	<p>The Selected Bidder shall perform the following functions related to Problem Management of all RHEL VMs (based on alerts or SR from GIC Re):</p> <ul style="list-style-type: none"> o Monitor, record and resolve all operating system problems o Carry out comprehensive problem analysis and share RCA reports with GIC Re o Start/stop services/process/ restart servers and work with OEM to provide workarounds
14	<p>The Selected Bidder shall perform File System (FS) Creation & Management (based on alerts or SR raised by GIC Re) of all RHEL VMs & Servers. This includes (but not limited to):</p> <ul style="list-style-type: none"> o Creation of ext3, ext4, zfs, xfs file systems o Encryption and Decryption of Files o Extending and Reducing the Logical Volumes. o Fix disk space problems by backing up (if required) and deleting files in concurrence with GIC Re o Manage/ Modify FS access o Share access reports
15	<p>The Selected Bidder shall perform File & Folder Access Management (based on alerts or SR from GIC Re) by giving access to FS, permissions to users (Read/Write/Modify), etc. All such access reports must be shared with GIC Re on demand.</p>
16	<p>The Selected Bidder shall perform Service Trend Analysis and analyse the utilization of resources in peak hours and off-peak hours. Monthly Utilization reports must be sent to GIC Re.</p>
17	<p>The Selected Bidder shall perform all Change Management on all RHEL VMs & Servers by creating and following change management procedure document. All Changes must be performed after prior approval from GIC Re.</p>
18	<p>The Selected Bidder shall perform OS hardening of all VMs & Servers and share the hardening policy with GIC Re if required.</p>
19	<p>The Selected Bidder shall support & manage all instances of JBOSS EAP in GIC Re's Infrastructure.</p>

O.5. Managed Services – Database (DB Administration)

1	<p>The Selected Bidder shall do provisioning for required Database Servers and Database administrator services for GIC Re Applications. GIC Re uses MSSQL, SAP HANA & Oracle DBs and Selected Bidder must manage all instances of these 3 DBs in GIC Re's Hybrid Cloud Infrastructure.</p>
---	--

2	The Selected Bidder shall offer the Database services that makes it easy to set up, operate, and scale a relational database in the cloud.
3	The Selected Bidder shall provision licenses on SPLA Subscription model and deploy/ install all instances of Oracle & MSSQL DB in non-SAP Servers. The License and installation of Oracle & SAP HANA DBs in SAP Servers will be provided and done by GIC Re. Detailed list provided in <u>Annexure XI</u> .
4	The Selected Bidder shall manage all Oracle, HANA & MSSQL DBs in entire GIC Re Infrastructure (both SAP & non-SAP Servers).
5	The Selected Bidder shall support latest versions of all major database like MS SQL, HANA, Oracle, etc.
6	The Selected Bidder shall support & manage asynchronous replication of the primary database to secondary database (and vice versa) in Oracle DB Servers to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. The replication all DBs (including HANA) in VMs must be automated and replication of all DBs in Servers (non-SAP Oracle) can be in active-standby mode.
7	The Selected Bidder shall provision & support read replicas that make it easy to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads.
8	The Selected Bidder shall support a manual failover of the DB instance running on Oracle Cloud Servers from primary to a standby replica. Failover of all other DBs (VM & HANA) must be automated in DR.
9	The Selected Bidder shall support the needs of DB workloads that are sensitive to storage, performance, and consistency in random access I/O throughput.
10	The Selected Bidder shall support creating more than one in-DC and across DC replicas within India per DB instance for scalability or disaster recovery purposes.
11	The Selected Bidder shall support enhanced availability and durability of all DB instances, especially for production workloads.
12	The Selected Bidder shall support creating a DB backup (including Redo/ Archive logs), as per Backup Schedule/ Policy or on-demand from GIC Re and restoring the DB instance from the backup to a specific date and time.
13	The Selected Bidder shall perform monitoring of performance and health of all DBs.
14	<p>The Selected Bidder shall perform following Database support services 24*7*365:</p> <ul style="list-style-type: none"> o Installation, configuration, maintenance of all DBs (Cluster & Standalone). o License provisioning of all MSSQL and non-SAP Oracle DBs. o Regular health check-up of all DBs. o Regular monitoring of CPU & Memory utilization of all DB servers. o Alert log monitoring & configuration of the alerts for errors. o Space monitoring for DB tablespaces, Index fragmentation monitoring and rebuilding. o Performance tuning of DBs, Troubleshooting, root cause analysis and identification of problem area. o Partition creation & management of DB objects, Archiving of DB objects on need basis. o Patching, upgrade & backup activity and restoring the DB backup as per defined interval. o Schedule/review the various backup and alert jobs. Batch Job Management as per the application requirement. o Setup, maintain and monitor the DB replication/ Physical standby and Assess IT infrastructure up-gradation on need basis pertaining to all DBs o DB User Account Management o Application DBA/ System / End User accounts – Create/ Modify/ Drop o Provide the access – Create/ Select/ Insert/ Update/ Drop/ Alter access o DB Administration o Database, Table space and indices Management o Space and Storage Group Management

	<ul style="list-style-type: none"> o Database Instance Management, restart/ shutdown instances, kill sessions, etc. o Maintain parameter/ System settings o Facilitate/ Assist GIC Re in DB migration activities, in conjunction with application support teams o Manage DB groups, connectivity issues, etc.
15	The Selected Bidder shall be able to rebuild all DBs using redo/ archive logs in case of any data corruption without suffering any data loss.

O.6. Managed Services – Storage

1	The Selected Bidder shall do provisioning & management of required Storage for hosting of all GIC Re applications, VMs & Servers.
2	The Selected Bidder shall provide scalable, dynamic, and redundancy-based storage. The Selected Bidder shall offer Block/ File Object level storage to use with compute instances in the cloud.
3	The storage array should support hardware-based data replication at the array controller level across all models of the offered family.
4	The Selected Bidder shall provide All-Flash/ SSD storage media to provide the throughput, IOPS, and low latency needed for entire GIC Re Hybrid Cloud Infrastructure.
5	The Selected Bidder shall provide consistent near-zero latency performance between 2.5-7.5 milliseconds at any scale.
6	The Selected Bidder shall provide all application and database storage on high-speed disks (minimum 5 IOPS/ GB) for better performance.
7	The Selected Bidder shall allow block sizes from 1 GB to multiple TBs to be provisioned by GIC Re from self-service provisioning portal.
8	The Selected Bidder shall support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm.
9	The Selected Bidder shall support read after write consistency (each read and write operation is guaranteed to return the most recent version of the data).
10	The Selected Bidder shall provide storage management tools to cater dynamically scalable storage requirements of GIC Re.
11	<p>The Selected Bidder shall facilitate following storage services:</p> <ul style="list-style-type: none"> o Storage Administration o LUN management-LUN provisioning and deletion, LUN mapping to the host o RAID group creation o SAN Switch & vSAN management, SAN switch configurations (zoning, masking, etc.) o Controller configuration o License management o Firmware upgradation in coordination with OEM
12	<p>The Selected Bidder shall perform Fault Management for entire storage which shall include (but not limited to):</p> <ul style="list-style-type: none"> o Response to alerts generated by storage or problems reported by GIC Re o Troubleshooting, root cause analysis (RCA) and identification of problem area o Resolution of problems through configuration changes/ re- installations/ replacements within the given architecture and design. o Run diagnostic tool as guided by OEM vendors. o OEM Product support. o Escalate hardware failures to hardware vendor. o Assist hardware vendor to Identify problem area (by log collection & reboot)

13	<p>The Selected Bidder shall perform Performance Management for entire storage which shall include (but not limited to):</p> <ul style="list-style-type: none"> o Monitor hardware resources through SAN tool. o SAN performance tuning. o I/O benchmarking. o Storage space and switch ports capacity management o 24*7*365 monitoring of performance parameters o Auto alerts and notification to performance degradation, threshold violation, etc. o Trouble shooting & root cause analysis for incidents/ faults o Identifying bottlenecks and suggesting de-bottlenecking solution
14	<p>The Selected Bidder shall perform Operational Support for entire storage which shall include (but not limited to):</p> <ul style="list-style-type: none"> o Log Storage: Store critical logs in shared Syslog server for retention period of 90 days o Configuration backup: Take incremental configuration backup daily for retention period of 90 days o Restoration of configuration when required o Trouble ticket logging, update, and closure o Replication Setup checks

O.7. Managed Services – Load Balancer

1	The Selected Bidder shall deploy a Load Balancer to distribute the TCP, UDP, HTTP, HTTPS, etc. traffic across many computing resources within the same site to increase the responsiveness and availability of all applications.
2	The Selected Bidder shall do the necessary sizing of load balancing requirements considering both current and future network and compute sizing of GIC Re Infrastructure.
3	The Selected Bidder shall provide secure, hardened, redundant (hardware or software) based Load balancer services.
4	<p>The Selected Bidder shall perform Administrative Management which shall include (but not limited to):</p> <ul style="list-style-type: none"> o User and Password Control o Check and maintain access control o Routine connection tests
5	<p>The Selected Bidder shall perform Change & Configuration Management for load balancer which shall include (but not limited to):</p> <ul style="list-style-type: none"> o IP Configuration o VLAN configuration (No ACL support on Routed/ VLAN interfaces) o Trunk port configuration o High Availability Configuration o Load Balancing SSL o Content Switching
6	<p>The Selected Bidder shall perform Fault Management for load balancer which shall include (but not limited to):</p> <ul style="list-style-type: none"> o Response to alerts generated by systems or problems reported by GIC Re o Troubleshooting, root cause analysis (RCA) and identification of problem area o Resolution of problems through configuration changes/ re- installations / replacements o Escalate hardware failures to hardware vendor o Assist hardware vendor to Identify problem area (by log collection & reboot)

7	The Selected Bidder shall perform Performance Management for load balancer which shall include (but not limited to): o 24*7*365 monitoring of performance parameters o Auto alerts and notification to performance degradation/ threshold violation o Trouble shooting & root cause analysis for incidents/ faults o Identifying bottlenecks and suggesting de-bottlenecking solution
8	The Selected Bidder shall perform Operational Support for load balancer which shall include (but not limited to): o Log Storage: Store critical logs in shared Syslog server for retention period of 90 days o Configuration backup: Take incremental configuration backup daily for retention period of 90 days o Restoration of configuration when required o Trouble ticket logging, update, and closure, etc.

P. Disaster Recovery (DR) Site

P.1. Disaster Recovery (DR) Solution	
1	The Selected Bidder is responsible for Disaster Recovery Services to ensure continuity of operations in the event of failure of primary DC. The Selected Bidder shall design and document an efficient DR solution in lines with the requirements of GIC Re and as per the RPO and RTO requirements.
2	The Selected Bidder shall provide DR as a service for the Applications, VMs, and DB Clouds, etc. as mentioned in Annexures XIII & XIV . The Solution must be able to seamlessly redirect GIC Re application traffic from all branches (domestic & foreign)/ spoke locations to the proposed DR site Infrastructure in a semi/ fully automated manner in case of any disruptions/ disaster at DC.
3	The Selected Bidder shall make provisions for required VMs, DB Servers at DR Site. The Selected Bidder shall analyse the existing infrastructure, applications, and any other relevant details before designing the DR Solution. The DR Solution shall be on Active (DC) – Standby (DR) mode. The Selected Bidder shall provide details of resources that will be deployed to implement the DR solution and justify how the resources will be sufficient to meet the requirements, including the RTO and RPO requirements.
4	The Selected Bidder shall make provisioning of requisite software, Business application, VM, OS, DB, etc., licenses and other required monitoring software/ tools for IT setup at DR site, as per Annexures XIII & XIV . GIC Re may add more applications, VMs, Servers, OS, DBs, etc., to the DR site in the future. The Selected Bidder shall make suitable provisions for such scale-up/ growth during the Contract Period.
5	The Selected Bidder shall perform installation, Migration and configuration of compute, OS, DB, Storage, Network, VMs/ Servers and enforce replication Mechanism for all requisite Applications/ VMs. The application environment must be installed and ready for use at DR site.
6	The Selected Bidder shall undertake installation and configuration of any other specialized applications/ software solution/ Hardware solution required for the setup and functioning of DR Setup.
7	The Selected Bidder shall offer switchover and switchback of individual Servers/ VMs/ Applications/ Components instead of entire system, as part of the services. The Servers/ VMs/ Applications/ Components at DR must function exactly as they do at DC Site.
8	The Selected Bidder shall only invoke the DR site when a disaster is declared by GIC Re or during planned DR Drills, upon prior approval from GIC Re. Users must only be allowed to access the IT applications/ VMs/ Servers at DR site when such a situation arises.

P.2. RPO & RTO

1	The service parameters to be met by the DR solution focus on the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO), which in business terms define the 'Interruption to Service' and 'Loss of Data' respectively. The RTO will be calculated from the time of “declaration of a disaster” up to the time by which all the applications are made fully operational & end users are able to access these applications & carry out the business operations. Recovery point objective (RPO) is the maximum acceptable amount of data loss after an unplanned disaster/ disruption, expressed as an amount of time.
2	The Recovery Time Objective (RTO) shall be less than or equal to 60 minutes (1 Hour) to enable business operations & The Recovery Point Objective (RPO) should be less than or equal to 15 minutes.
3	The Selected Bidder shall offer dashboard to monitor RPO and RTO.

P.3. Replication

1	The Selected Bidder shall adequately do the sizing of DC-DR replication links and commission them with (1+1) redundancy, to meet the RTO and the RPO requirements. A preliminary sizing has been provided by GIC Re in the Bandwidth Details List in Annexure XII . The Selected Bidder can propose a different bandwidth with proper justification.
2	All DR specified DBs shall be replicated on an ongoing basis and shall be available in full (100% of the Primary DC) as per required RTO/ RPO and designed replication strategy.
3	GIC Re currently requires a 25% capacity DR. However, this may be scaled up to 100% any time, if required. The Selected Bidder must consider this during DR sizing. There shall be asynchronous replication of data between Primary DC and DR. Any lag in data replication must be clearly visible in dashboard and alerts of same must be sent to GIC Re.
4	The Selected Bidder shall be responsible for providing/ facilitating replication tools/ software/ processes for Databases, Active Directory, Web Servers, application, VMs, Servers, etc., for seamless replication from DC to DR and vice versa to meet RPO and RTO requirements. The Selected Bidder shall mention details of these tools/ software in their solution document.
5	The Selected Bidder shall provide detailed operating manuals/ procedure documents for entire DR replication.
6	The Selected Bidder shall provide details of replication mechanism for (but not limited to) the following solutions: o OS o DBs o Servers o VMs o Active Directory/ LDAP/ DNS

P.4. DC-DR Failover & Restoration - DR Drills/ Actual Disaster

1	The Selected Bidder shall clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for complete switchover to DR in the BCP/ Procedure document. The Selected Bidder shall also define the access mechanism of all users from spoke locations to DR site during disaster/ drills in the solution document and BCP.
2	The failover from primary DC to DR should be done through a proper DR announcement process which should be documented as part of BCP planning. In the event of a disaster, GIC Re's Setup at proposed DR site will become the Primary system.
3	The DR site must be available (with GIC Re's systems & data) on-demand basis within the defined RTOs and RPOs. Users of all branch/ spoke locations of GIC Re must be able to connect to the Selected Bidder's proposed DR Site directly during disaster/ drills, through ILL (over SASE ZTNA EDS Solution or VPN).

4	During DR drills, the Selected Bidder shall demonstrate the fulfilment of SLAs at load of 100% users with 60% concurrency.
5	Application data and application states must be replicated between DC & DR so that when an outage occurs, failover to the surviving data center can be accomplished within the specified RTO. The installed application & database instances must be usable.
6	During the switch from DC to DR or vice-versa (during disaster/ drills), it should be as per the given RPO. The Selected Bidder shall provide workflow-based switchover/ failover facilities (during DC failure & DR Drills). The switchback mechanism shall also be workflow based. The Selected Bidder shall also provide a tool/ mechanism for GIC Re to trigger DR switchover, for example a “one-click DR”. The Selected Bidder shall perform all necessary development and configuration of any additional scripts for successful working of DR.
7	The DB, Security, storage, OS, etc. capacity & licenses must be sized as per current sizing (Annexures XIII & XIV) and future growth as well. The Selected Bidder shall scale up the entire setup (including Bandwidth) at DR as per GIC Re's requirements, based on rate cards. Users must be routed seamlessly from DC site to DR site.
8	Restoration provides an easy process for copying updated data from the DR server back to the DC server. Whenever main DC will be recovered and operational, the data from DR system to DC systems should be synchronized. Once this data is synchronized and verified, the switchback from DR system to DC system should be done. In that case all users will be accessing systems of main DC, post successful switchback.
9	The Selected Bidder shall provide detailed DR activity plans which will contain steps/ procedures to switch over services to DR site and vice-versa (DR to DC) in the event of disaster at DC site.
10	In case of failover to DR site (once disaster is declared) within the defined RTO, the SLA would not be applicable for RTO period only. Post the RTO period, SLA would start to apply and should be measured accordingly.
11	The Selected Bidder shall partner/ coordinate with respective applications/ product support vendors on GIC Re's side to bring the applications up and running at DR site, support DR in event of disaster/ Drills or for performing periodic maintenance & upgrade activities.
12	The Selected Bidder shall conduct DR drills twice per annum, wherein the Primary DC must be deactivated, and complete operations shall be carried out from the DR Site. The pre-requisites of DR drill must be carried out by The Selected Bidder and GIC Re jointly. The Selected Bidder must formulate and design the exact process of the DR drill, in consultation with GIC Re and its application support team, in such a way that all elements of the system are rigorously tested, while the risk of any failure during the drill is minimized. The process must be documented by the Selected Bidder as part of the disaster recovery plan (DRP). The Selected Bidder shall plan the activities to be carried out during the mock drill and issue a notice and a POA (Plan of Action) to the department at least 15 working days before such drill. The Selected Bidder shall provide a detailed DR Drill report, with RPO/ RTO achieved during the drill, after each planned Drill activity.
13	During the DR drill, the Selected Bidder must arrange the full DR team with sufficient resources and expertise and complete the activity under the supervision of senior resources for co-ordination. The Selected Bidder shall develop appropriate policy, procedure & checklists in line with ISO 27001 & ISO 20000 framework for failover and fall back to the appropriate site.
P.5. DR as a Service	
1	Provision for managed services for the entire DR facility must be provided. The Selected Bidder shall provide continuous maintenance activities to support the DR site.

2	The Selected Bidder shall provide support for all server maintenance activities. This would include periodic health check, on-demand troubleshooting, repairs, part replacement etc. from certified vendors. ITIL processes named problem, change, incident & configuration management procedures will be followed by the Selected Bidder at DR site.
3	The Selected Bidder shall have proper escalation procedure and emergency response in case of failure/disaster at DC.
4	Any activities not mentioned here but required for the implementation, operation, and maintenance and monitoring of DC and DR sites shall be carried out by the Selected Bidder. The solution provided by the Selected Bidder shall meet all the service level requirements.
5	The Selected Bidder shall perform RPO monitoring, reporting and event analytics and other activity associated with operations and management of DR plan and Implementation for the DR solution.
6	The Selected Bidder shall provide a monitoring tool with dashboard showing RPO, RTO, changeover facility etc.
7	The date, time, duration, and scope of each drill shall be decided mutually between GIC Re and the Selected Bidder. Extreme care must be taken while planning and executing DR drills to ensure that there is no avoidable service interruption, data loss, or system damage at DC.
8	To demonstrate how the application fails over when the primary site goes down. The testing should include the: o Uninterrupted replication to DR servers. o Lag in replication due to any unforeseen errors. o Process of recovering from lags if any. o Data integrity test of DR servers.
9	The Selected Bidder shall be responsible for Devising and documenting the DR policy discussed and approved by GIC Re. GIC Re reserves the right, on its own or via a third-party auditor, to conduct overall testing at any point of time for the services delivered by the Selected Bidder.
10	The Selected Bidder shall configure all the components and sub-components for end-to-end user access to all applications/ VMs/ services at the DR site, through ILL (using SASE ZTNA EDS Solution).
11	The Selected Bidder shall be responsible for bringing the VMs/ applications/ DBs to login level in case of disaster/ DR drills.
12	The solution must be able to perform application-level recovery scalable to site level recovery based on the impact of the disaster.
13	In case of reverse replication, since the DR site would be acting as main site, all the necessary support (same as DC site) to run the environment must be provided by the Selected Bidder.
14	Reverse Replication is necessary and envisaged when the DR site is acting as the main site. The solution must ensure consistency of data in reverse replication till the operations are not being established at the Cloud site. The RPO would be applicable in reverse replication also. The entire data should be made available for restoration at Primary DC after switchback.

P.6. BCP for GIC Re Infrastructure

1	The Selected Bidder shall define and submit (as part of the solution), a detailed approach for “Business Continuity Planning”; this should clearly delineate the roles and responsibilities of different teams during DR Drills or actual disaster; further, it should define the parameters at which “disaster” would be declared.
2	The Selected Bidder should have a practicing framework for business continuity planning and plan development which has been established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements.

3	The Selected Bidder should practice Business continuity and security incident testing at planned intervals or upon significant organizational or environmental changes.
4	Incident response plans must be developed by the Selected Bidder which shall involve impacted customers (tenant) and other business relationships and represent critical intra-supply chain business process dependencies.

Q. SD-WAN with MPLS, ILL & P2P - Implementation & Management

Q.1. Network Architecture - MPLS, ILL & SD-WAN	
1	The Selected Bidder shall design the underlaying network with Dual MPLS HUB-&-SPOKE Model, with DC and DR Sites as Hubs and GIC Re Branches as Spokes. All these Spoke locations must communicate with each other and with DC & DR via different Private VLANs. Furthermore, the Selected Bidder must provide Dual ILL connectivity for local internet break-out at each branch of GIC Re. The application traffic shall flow through the dual MPLS links and web/ internet traffic shall flow through the dual ILLs at each location. The SD-WAN solution shall be an overlay/ orchestration layer on this and manage the entire network architecture. The Bandwidth details per branch are mentioned in Annexure XII .
2	The Selected Bidder shall implement and manage SD-WAN solution with centrally managed WAN edge devices (to be referred to as CPEs hereinafter) placed in branch offices, DC & DR sites to establish logical connections among the CPEs using the underlying physical WAN infrastructure. These logical connections should create secure paths across multiple WAN connections and carriers, such as MPLS, hybrid Internet leased lines, etc. SD-WAN solution should dramatically simplify the complexity associated with management, configuration, and orchestration of WANs. CPEs may be physical or virtual devices implementing SD-WAN functionality in software (network function virtualisation (NFV)).
3	The Selected Bidder shall provide self-service capabilities, as part of the solution, which gives access to GIC Re for monitoring and designing policies of the SD-WAN network. The Selected Bidder shall design and deploy policies across the entire network as per Industry best practices & GIC Re's requirements.
4	The Selected Bidder shall provide a solution which supports distributed cloud gateway architecture to facilitate the communications between all MPLS sites & Public Internet through ILL.
5	The proposed SD-WAN solution should have the following minimum features (not limited to): <ul style="list-style-type: none"> o Application visibility and Analytics o Centralized Orchestration & Policy Management o Transport Independent Overlay Solution o Application Aware Routing & Application Prioritization o Performance based App Aware Routing & Load Sharing o Segmentation & Dynamic Topologies o Application Based QoS o Local Internet Break out o Path Brownout o Security & Encryption o Managed service offering o Self Service Portal for reporting & service requests
Q.2. SD-WAN Core Components - Overlay Network	
1	Each CPE must be capable of dynamically establishing fully meshed encrypted overlay paths to every other CPE, across multiple different WAN services: MPLS, Internet Leased Line, etc.
2	The solution must support dynamic optimal direct site-to-site remote routing (spoke-to-spoke model) and/ or any-to-any.

3	The overlay paths established amongst the CPEs must support: o Transport of unicast, multicast, and broadcast traffic o The ability to run routing protocols: OSPF v2 and v3, BGP; for IPv4 and IPv6; etc.
4	The design shall be such that only the WAN IP addresses of the CPEs at each branch locations need to be known for establishing the overlay network.
5	The locations must be able to access Microsoft 365 & all other internet-based applications, which GIC Re is using currently/ or may deploy in future, over Internet directly through ILLs (local breakout). In case both ILL links go down at any branch, internet traffic should still be accessible via MPLS through DC, until the ILLs are restored.
6	All edge devices/ CPEs and WAN must comply with GIC Re's/ Regulator's periodic audit requirements.
7	During the period of contract GIC Re may add additional MPLS and/ or ILLs at some locations and the Selected Bidder must add all such links to the SD-WAN and suitably configure the CPEs.

Q.3. SD-WAN Core Components - Dynamic Load Sharing based on Business and/ or Application Policies

1	CPEs must be able to load balance traffic across multiple WAN paths based on load balancing algorithms efficiently using all available WAN bandwidth (MPLS & ILL).
2	The solution must be able to dynamically control data packet forwarding decisions by looking at application type, performance, policies, path status, etc. and route all traffic accordingly towards DC (internal application traffic through MPLS) and Internet (M365, browsing, etc. traffic through ILL).
3	The solution must be able to monitor the network performance - jitter, packet loss, bandwidth and delay and make decisions to forward critical applications over the best performing path based on the defined application policy.
4	The solution must respond to measured performance changes (degradation) in addition to link and node state changes (up/ down) and adjust application forwarding accordingly.
5	The solution must be able to prioritize real time traffic over other traffic and adjust forwarding policies based on GIC Re's requirements.
6	The solution must have application awareness with capability of deep packet inspection of traffic to identify and monitor applications' performance to determine what traffic is running across the network to tune the network for business-critical services, resolve network problems and to help ensure that critical applications are properly prioritized across the network.
7	The solution must be able to monitor application and internet usages of individual users over the network and provide reports for the same, as and when required.
8	CPEs must be able to identify and classify applications, including application encrypted traffic. Identification and classification of all application (both current and future) types must be supported by the solution.

Q.4. SD-WAN Core Components - Security & Encryption

1	All site/ spoke location traffic must be encrypted when transported over WAN transport links: Internet leased line, MPLS network, etc., protecting Data Confidentiality and Integrity.
2	The encryption must be done as per IPsec standards using AES with 128bit keys or higher coupled with Internet Key Exchange Version 2 (IKEv2) or a set of equivalent or higher standards.
3	The use of encryption should not limit the performance or availability of applications hosted at DC or over Internet and should be transparent to end users.

4	The proposed SD-WAN solution should have stateful security features, like L3/ L4 filtering, Zone-Protection for network, DDoS Protection, SSL Inspection, etc., for network isolation in the CPE along with other SD-WAN features. The solution and its features must also be patched and updated by the Selected Bidder at regular intervals.
5	The solution should have inbuilt Next Generation Firewall (NGFW) features, like L7 Application-level filtering, URL-filtering, SSL Inspection/ decryption, etc. All the features should be enabled on all CPEs without addition of any other separate hardware or licenses.
Q.5. SD-WAN Core Components - Centralized Management, Monitoring & Configuration	
1	The Selected Bidder must provide a Centralized management solution which uses unified platform for network service provisioning, monitoring and assurance, change and compliance management.
2	The centralized management solution must have web-based GUI.
3	The solution must support zero-touch provisioning/ plug-n-play for new/ future branches of GIC Re.
4	The solution must support end-to-end real-time flow visualization for the application paths for identifying issues and taking corrective actions.
5	All network-wide configurations shall be from the centralized management solution.
6	All application forwarding policies shall be configured from the centralized management solution/ application.
7	The centralized management solution shall have NMS capabilities and must support network wide visibility for all the CPEs, networks and GIC Re endpoints. The NMS should be configured to monitor all the links terminated on the CPEs irrespective of the type of link (internet leased line, MPLS, etc).
8	The solution must be able to collect and aggregate traffic statistics for all WAN paths (MPLS & ILL). Traffic statistics include path utilization, application specific utilization and path performance.
9	The solution must support device health monitoring for all the devices within the solution scope.
10	The solution must store historical traffic and performance information for at least three (3) months to assist with trouble analysis, traffic forecasting and SLA compliance.
11	The solution must support email-based alarm to notify the administrators and GIC Re in case of any device/ link fault or network performance degradation.
Q.6. SD-WAN Core Components - Monitoring, Reports & Analytics	
1	The Selected Bidder shall provide 24*7*365 remote proactive monitoring service of the entire ILL & MPLS based SD-WAN network from their own NOC by specialized technical team to ensure that the services are always operational end-to-end.
2	The Selected Bidder shall provide availability reports on monthly basis and ensures that proactive notification is provided to GIC Re in case of any network element (ILLs, MPLS, P2P, SD-WAN CPEs, etc.) failure.
3	Managed Services shall include (but not limited to) providing up/ down status reporting, malfunction alarms/ alerts, fault monitoring, incident management, patch management, performance management, change management (including device configuration, backups, and log reporting, changing faulty device, etc.), escalation, and resolution; 24*7*365 network monitoring; and online portal-based device/ network availability performance reporting.
4	Bidder shall provide quote for rate card for additional internet link management, in case GIC Re procures additional internet link at any of the locations. Internet link procured by GIC Re shall be part of monitoring scope.
5	The solution must provide Real & historical time series log event reporting.

6	The solution must provide Traffic usage/ protocol anomaly detection reports.
7	The solution must provide Ad-hoc and scheduled reports as per GIC Re's requirements.
8	The solution must provide Predefined and custom report templates.
9	The solution must support report export formats like csv, pdf, xls(x), email notifications, etc. The solution should also have provision to integrate with SMS gateway.
10	The solution must provide Traffic reports per site: availability, bandwidth usage per access circuit, bandwidth usage per application, user, latency, packet loss, QoS per access circuit/ link etc.
11	The solution must provide Firewall reports: top rules, zones, source, destination by IP/ domain name/ geo location, ports, protocols, session duration, QoS, DDoS, NAT events, pool utilization and Flood detection, etc.
12	The solution must provide Application reports: Top Applications usages, User wise usage, Top URLs, Top Bandwidth Consuming Applications, Top Sources, Top Destinations, Site based Application usage analysis report, Top sites, Top Sites over time, Site availability over time, Total Availability, etc.

Q.7. SD-WAN Core Components - User Interface

1	The solution must provide detailed dashboard & reports on network performance parameters like utilization, packet loss, jitter, latency, availability etc., and security of all the transport media/ links terminated (including media proposed to be terminated during the period of contract) on the CPE. The dashboard access should be provided to admin users of GIC Re as and when required.
2	The solution must provide Dashboard views for SD-WAN, security, CPE functionality, links, etc.
3	The solution must provide visualization using charts, real-time views, maps, grids, etc.
4	The solution must provide drilldown support to analyse data instantly for a given time range, detect trends and anomalies, etc.
5	The solution must provide HTTP/ HTTPS Web-based interface.

Q.8. SD-WAN Core Components - Other Specifications

1	The Selected Bidder shall provide any other hardware/ software/ license required to complete the solution/ achieve functionality.
2	During the Contract Period, GIC Re may add/ delete/ replace applications, links, security policies, etc. Accordingly, the Selected Bidder shall carry out necessary configuration changes in the Solution/ network, as and when required by the GIC Re.

Q.9. SD-WAN Core Components – Customer Premise Equipment (CPE)

1	All the hardware supplied by the Selected Bidder should be appliance based, rack-mountable, from the same OEM and must be with all related accessories, power cables, mounting kit, etc.
2	The Selected Bidder shall terminate multiple internet transport media/ Links (MPLS, ILL) on the CPEs as required by GIC Re.
3	The Selected Bidder shall size the Minimum Capacity of the Proposed CPEs as per Bandwidth (MPLS & ILL) and user details of each branch/ spoke locations as provided in <u>Annexure XII</u> .
4	All SD-WAN CPEs must be capable of terminating 2 ILLs and 2 MPLS links on immediate basis. GIC Re may add additional links based on business requirement. The Selected Bidder shall provide SD-WAN CPEs to support the scale of throughput and minimum 2 additional WAN interfaces.
5	The Selected Bidder shall provide all the software and licenses required to meet the tender specifications from day one (1).

6	SD-WAN subscription/ license should be based on the bandwidth of links terminating on the devices and not on the CPE capacity. As and when GIC Re upgrades the bandwidth, the SD-WAN subscriptions/ license should also be upgraded as per the contracted rate.
7	The CPE(s) must have inbuilt Next Generation Firewall (NGFW) feature from day one (1).
8	Proposed SD-WAN CPE must be available as virtual appliance in case the DC and DR require a virtual implementation. Necessary VMs can be sized and used from GIC Re's Hybrid Cloud Infrastructure. The Selected Bidder shall provide the details of sizing parameters for the SD-WAN CPE virtual appliance.
9	SD-WAN CPE virtual appliance should be compatible with major cloud service providers (e.g., AWS, Azure, Google, etc.).
10	In case of failover of any transport media or CPE, the connectivity should be automatically established with the alternate transport media or CPE without any delay/latency. Resolution of transport media and CPE should be as per SLA. Each Branch/ spoke location of GIC Re must have 2 CPEs (redundancy).
11	GIC Re should be able to use bandwidth from all the transport media/ Links (MPLS & ILL) terminating on single CPE or multiple CPEs at each location.
12	The Selected Bidder shall configure local breakout from each branch/ spoke locations for internet-based applications access, like M365, browsing, or any other cloud services, etc., through ILLs as per GIC Re's requirements during the period of contract.
13	The Selected Bidder shall assist GIC Re in configuring the local/ private vLANs in each branch/ spoke location and ensure the network connectivity (MPLS & ILL) for all endpoints and servers.

Q.10. SD-WAN Core Components - Last Mile (ILL, MPLS, P2P)

1	DC & DR Sites
i	The Selected Bidder shall provide last miles (ILL, MPLS, P2P) at DC and DR sites on wired media with redundancy. The primary and backup should be extended from two different Telecom Service Provider devices/ POPs and the backup link should be from different Telecom Service Provider in case of bidder terminating the backup link on different POP.
ii	The primary and backup should be in active-active mode and should be available always for load balancing through SD-WAN.
iii	Bidder shall provide 80 Mbps or higher point-to-point (P2P) link between DC & DR for replication for maintaining required RPO (15 minutes) & RTO (1 Hour), mentioned in <u>Annexure XII</u> .
2	Spoke/ Branch Locations
i	The Selected Bidder shall provide ILL and MPLS links for all GIC Re branches/ spoke locations on wired media with redundancy. The primary and backup should be extended from two different Telecom Service Provider devices/ POPs and the backup link should be from different Telecom Service Provider in case of bidder terminating the backup link on different POP.
ii	The primary and backup should be in active-active mode and should be available always for load balancing through SD-WAN.
iii	Location wise bandwidth and link details provided in <u>Annexure XII</u> .
iv	The ILL & MPLS links at all locations must be scalable to support higher bandwidth requirements during the period of contract. Rate cards must be provided for the same.
v	The Selected Bidder shall provide connectivity with minimum number of “hops” for all links.
vi	All the POPs from where the MPLS & ILLs links are provided must have redundancy of equipment, links, power systems, backhaul connectivity, etc.

vi i	<p>The Selected Bidder shall ensure that major security features (including those mentioned above) against attacks as mentioned below are implemented in their network:</p> <ul style="list-style-type: none"> o Protection against all kinds of attacks including DDOS attacks, SYN attacks, smurf attacks etc. o Protection against all kinds of spoofing like VPN spoofing/ IP spoofing etc.
Q.11. SD-WAN Core Components - VPN (for GIC Re Foreign Offices & Roaming Users)	
1	GIC Re's foreign offices are located at London and Kuala-Lumpur. These offices access internal applications hosted at DC/ DR through site-to-site (IPsec) VPN. The Selected Bidder shall provide a similar setup for these 2 foreign branches and enable connection to these locations by making necessary configurations for the site-to-site VPN at both end Firewalls, as required. GIC Re may require additional site-to-site VPN connectivity, during the Contract Period, for connectivity to new/ existing foreign offices. The Selected Bidder must provide rate cards for such connections. These VPN connections must be managed by the Selected Bidder for the entire Contract Period.
2	The Selected Bidder shall enable VPN access for roaming users to connect to the DC and DR in the proposed solution. This will be required in addition to SASE ZTNA EDS Solution and for 50 Users. This number must also be scalable as and when required.
3	The Selected Bidder shall provide necessary licenses required for establishing VPN connectivity to foreign offices (site-to-site/ IPsec) & 50 roaming users (Software VPN with tokens).
4	The Selected Bidder shall provide dedicated hardware or use DC & DR SD-WAN CPEs to enable remote access VPN for foreign offices (site-to-sit/ IPsec) & roaming users (software with token).
Q.12. SD-WAN Core Components - Network Migration	
1	The Selected Bidder shall be responsible for migrating all branch/ spoke locations from existing MPLS Network to ILL & MPLS based SD-WAN network .
2	The Selected Bidder shall build a migration calendar in discussion with GIC Re for migrating branch/ spoke locations to the new SD-WAN (ILL & MPLS) Network.
3	The Selected Bidder shall clearly specify required downtime for migration along with migration calendar. Downtime for migration shall be approved & provided by GIC Re during non-business hours.
4	The Selected Bidder shall ensure smooth migration to the ILL & MPLS based SD-WAN Network. In case of any migration failures, bidder shall rollback the configuration to old network immediately and coordinate with GIC Re for application testing within the approved downtime window.
Q.13. SD-WAN Core Components - Bandwidth (ILL, MPLS, P2P)	
1	The Selected Bidder shall dedicate (1:1) bandwidth (ILL & MPLS) for GIC Re at each branch/ spoke/ hub location and on dedicated ports. The ILLs must be available in full duplex mode (for e.g. - On a 2 Mbps circuit, 2 Mbps sending and 2 Mbps receiving should be possible simultaneously).
2	The Selected Bidder shall provide a Network which supports access control list (ACL) Support, SNMP & v2 support Network Time Protocol Version 4 (NTPv4), Syslog, Ping, Trivial File Transfer Protocol (TFTP), Secure Shell version 2 (SSHv2) and Internet Protocol version 4 & 6 (IPv4 & IPv6).
3	The Participating Bidders are expected to do a site survey for feasibility and for positioning of the terminating equipment. They should clearly inform about the equipment that will be deployed with its physical, electrical and any other related information.
4	The Selected Bidder shall arrange required Rights of way permission from Local Corporation/ Municipalities/ authorized agency for road cutting, digging, and laying of fibre/ copper cables.

5	The Selected Bidder shall do all internal cabling till CPEs at all locations for successful commissioning of the required MPLS & ILLs. The Selected Bidder shall assist GIC Re in connecting the internal vLANs at each location to the CPEs and establishing connectivity successfully. The Selected Bidder shall provide all required cables for connecting to the CPEs.
6	All network equipment shall support Packet Filtering, TCP spoofing, IPv4 & IPv6 both and other industry standard protocols and security features (as mentioned above).
7	Table in Annexure XII lists bandwidth required for each location. The Selected Bidder may suggest improved alternatives.

R. ZTNA Solution for Remote Users

R.1. SASE ZTNA EDS Solution	
1	The Selected Bidder shall procure, supply & implement licenses for SASE ZTNA EDS Solution for 100 users as per the commercial format in Annexure IV . GIC Re may procure additional licenses as per rate fixed in Annexure IV anytime during the Contract Period.
2	The Selected Bidder shall migrate the current SASE ZTNA EDS Solution and manage the setup for the Contract Period.
3	The Selected Bidder shall plan, design, integrate, implement, rollout updates, manage the solution for the Contract Period. If some components are missed out or not properly sized, onus is on the Selected Bidder to supply/ replace it without any cost to GIC Re.
4	The Selected Bidder shall ensure that during implementation phase, the performance, security, etc. of the entire network setup is not compromised. The Selected Bidder shall ensure the SASE ZTNA EDS Solution is able to host both thick and thin client Applications of GIC Re.
5	The Selected Bidder shall migrate the SASE ZTNA EDS Solution connector pair from the current setup to both the proposed DC & DR sites. The connectors need to be deployed in high Availability (2 VMs). It is recommend creating a new connector when you have reached 100 applications on a single connector pair. The 2 VMs must be replicated over to the DR site as well.
6	The Selected Bidder shall provision the access and support for Applications as mentioned in Annexure XI for 100 users. For GIC Re admins, RDP/ SSH sessions must be provided to approximately 90 VMs (all VMs in GIC Re Infrastructure, whichever is more). The admin IDs (for Both Linux & Windows servers) will be provided to the Selected Bidder. Any new VMs and Applications provisioned during the Contract Period must also be included in the solution scope. The Selected Bidder shall add any new applications/ VMs to the SASE ZTNA EDS Solution portal in the future.
7	The Selected Bidder shall make provisions for thick client apps, Web Based Apps & RDP/ SSH access-based configurations, as per the details mentioned in Annexure XI .
8	The Selected Bidder shall configure Multi Factor Authentication OR two factor authentications for all the applications listed as per Annexure XI , which would be either Email/ SMS or TOTP (Authentication token) based MFA.
9	The Selected Bidder shall make provisions for Single Sign on for the applications listed in Annexure XI . SSO will allow GIC Re users to authenticate with the SASE ZTNA EDS Solution once to gain access to all their applications, without having to log in again to each application individually. SSO can be implemented by using the solution's own Identity Provider.
10	The Selected Bidder shall manage the Active Directory Integration during the implementation phase. Thereafter, any requests/ incidents related to the integration/ implementation must be addressed by the Selected Bidder.
11	The Selected Bidder shall install the SASE ZTNA EDS Solution clients on workstations of designated users for accessing thick client application access such as SAP GUI etc. for the following supported OS - Microsoft Windows 7, Windows 10, Windows 11 Home/Pro/Enterprise editions, Apple macOS 10.12 Sierra, macOS 10.13 High Sierra, macOS 10.14 Mojave, or macOS 10.15 Catalina and future versions.

12	The Selected Bidder shall use the Solution's IdP (Identity Provider) to authenticate SAML and Single sign-on (SSO) authentication for GIC Re applications.
13	The Selected Bidder shall deploy SASE ZTNA Solution's security agent on all designated systems/ workstations, like Office Desktops and Home Laptops/ Desktops for WFH/ roaming users. All components of the SASE ZTNA Solution must be deployed on all systems that remote users will be using to access GIC Re applications.
14	The Selected Bidder shall deploy Security Connector pair in the GIC Re's DC & DR sites, which act as hub for all spoke/ branch locations (including foreign branch users). Enterprise Security Connector pair will be VMs that must be deployed to block malicious traffic and record information about machines in GIC Re network.
15	The Selected Bidder shall provide all necessary details on the VM and Network Requirements. Changes in Network & Firewall must be carried out by the Selected Bidder to allow the SASE ZTNA Solution connector's private IP address to reach the application on configured port numbers.
16	The Selected Bidder shall make provisions for email alerts & One-time report sharing with GIC Re team, as SASE ZTNA Solution security policies will be in "Monitor" mode for the first few days of deployment, during that duration the relevant triggers will be analysed & a detailed report will be prepared which needs to be reviewed by Selected Bidder & GIC Re team, post which the controls will be moved to "Block" mode. The reports will then have to be regularized on a particular frequency as per the final recommendations.
17	Selected Bidder to assist GIC Re team for deployment of SSL/ Wildcard Certificates for Application/ IdP URLs.
18	The Selected Bidder shall deploy connector by using the provided private IP addresses inside the Local Area Network (LAN). The connector should run close to internal applications, possibly in the same subnet as the application, and be able to communicate with the application over specified port.
19	The Selected Bidder shall create a Dial-out access to the Internet on TCP port 443. The connector must reach the Enterprise Application Access service over the internet. This communication is carried out over an open TCP port 443, and only needs outbound connectivity (outbound traffic only).
20	Selected Bidder shall make provisions for access to the applications. The port and protocol must be accessible in the LAN.
21	The Selected Bidder shall document the detailed solution architecture, design, traffic flow etc. and provide the same to GIC Re as soon as the solution is implemented and Live.
22	The Selected Bidder shall provide on demand and pro-active 24*7*365 remote support for the SASE ZTNA EDS Solution.
23	The Selected Bidder shall submit escalation matrix and keep GIC Re informed, if any changes take place in the designed solution.
24	The Selected Bidder shall provide/ implement/ apply all product updates, upgrades & patches free of cost during Contract Period. The Selected Bidder shall inform GIC Re about all release/ version change of patches/ upgrades/ updates of hardware/ software/ OS/ middleware etc. as and when released by the OEM.
25	The Selected Bidder shall ensure that all upgrades/ changes at the DC-DR end (Server OS & DB Versions, Application version, network, etc.) must also be compatible with the solution during the Contract Period.
26	The Selected Bidder shall participate and comply with various audits, regulatory requirements and certifications conducted by IRDAI, other agencies and various legal entities.
27	The Selected Bidder shall deploy Unified threat protection security policy using the solution for all GIC Re's roaming/ WFH employees. Selected Bidder needs to do the Initial policy configuration for GIC Re's environment.

28	Currently, SASE ZTNA EDS Solution is already deployed in GIC Re environment with 2 connectors (VMs) and all applications/ VMs configured. The Selected Bidder shall migrate the solution with these connectors and shall continue to manage the setup post migration (with license for 100 users).
----	--

S. Hardware Upgrades/ Software Updates/ Patch Management

- The Selected Bidder shall perform upgrades & patch management of entire infrastructure. Any required version/ Software, Hardware upgrades, patch management etc. in GIC Re's Hybrid Cloud Infrastructure Sites will be done by the Selected Bidder for the entire Contract Period.
- Application Patch Updating (except AD & DNS, which bidder must do) will be done by GIC Re team.
- The Selected Bidder shall document all upgrade & patch management related activities.
- The Selected Bidder shall ensure to Generate Alerts well in advance on the upcoming patches via email and management portal.

T. Managed Security Services (MSS) & Security Operations Centre (SOC)

T.1. Cloud Security Requirements	
1	The Selected Bidder shall implement and manage complete end-to-end security solutions, as part of SOC as a service, for GIC Re's environment. The solution and its components must cover GIC Re's Network, VMs, Servers, systems, and endpoints at every branch/ spoke location. The Selected Bidder shall be responsible for any breach in security or any security incidents and the onus of mitigating all such risks shall lie with the Selected Bidder.
2	The Selected Bidder shall ensure complete security requirements for the entire GIC Re Hybrid Cloud Infrastructure (GCC, HANA Cloud, Oracle Cloud, etc.) hosting with suitable security arrangements through SaaS model (Security/ SOC as a Service) as per Meity, IRDA, etc., guidelines. The Selected Bidder shall provide end-to-end security services to meet IT security challenges for the infrastructure based on the proven frameworks and security best practices. It is vital for complete security that the processes and technology which shall support the Information Security function are proven and adhere to standards.
3	The security operations shall be centralized, structured, and coordinated and shall be responsive resulting in effective threat prevention and detection helping the deployed Hybrid Cloud solution to be secure from attackers. The Information Security functions shall respond faster, work collaboratively, and share knowledge more effectively. The proposed Hybrid Cloud solution shall have multiple security layers to secure the infrastructure from threats.
4	The Selected Bidder shall ensure that there is a set of IT security management processes and tools to ensure complete security of GIC Re Hybrid Cloud solution. An IT security policy, framework, and operational guidelines as per ISO 27001, 27017, 27018 & PCI-DSS must be maintained & implemented by the Selected Bidder.
5	All the security management processes, tools and usage shall be well documented in security policy and the security best practices to be followed to maintain IT security.
6	Data shall not leave the Indian boundaries and data residing within Cloud shall not be accessed by any entity outside the control of GIC Re.
7	Security services shall support audit features such as what request was made, possibly the source IP address from which the request was made, who made the request, when it was made, and so on.

8	<p>The Selected Bidder shall execute the below listed (but not limited to) service activities:</p> <ul style="list-style-type: none"> o Integration, configuration & management of security solutions of all Servers, VMs, systems, endpoint devices from GIC Re's branch/ spoke locations and DC-DR with the SIEM solution. o Data/ log aggregation from all security systems and devices (servers, endpoints, VMs, network devices, etc.). o Correlating, Analysing and responding on all security incidents. o Monitoring different events on 24*7*365 basis. o Intimating GIC Re about security risk and incidents and taking all required actions. o Monthly Reporting on all incidents. o All Security Log Retention for 6 months. o Studying, investigating and mitigating anomalies/ incidents. o SOC as a Service for all servers, endpoints, VMs, network devices, etc., in GIC Re's Hybrid Cloud Infrastructure.
9	<p>SOC as a Service shall cover all GIC Re systems, servers, VMs, etc. at DC & DR and all endpoints at GIC Re Branch/ spoke locations. The Selected Bidder shall monitor and manage all SOC components (as mentioned in Table T.4) and cover below aspects (but not limited to):</p> <ul style="list-style-type: none"> o Correlation and security monitoring o Analytics o Alerting o Dashboards o Compliance o Log Retention o Incident response o Threat Intelligence o User and Entity Behaviour Analytics (UEBA) o Artificial Intelligence & Machine Learning (AI & ML) o Real time Threat Hunting & detection
T.2. SOC Controls	
1	<p>Secure Access Control: The solution shall include mechanisms for defining and controlling user access to the operating system environment and applications. Best practices from enterprise security including password strength, password aging, password history, reuse prevention etc. must be followed for access control.</p>
2	<p>Authorization Control: A least-privilege concept such that users are only allowed to use or access functions for which they have been given authorization shall be available.</p>
3	<p>Logging: Logs must be maintained for all attempts to log on (both successful and unsuccessful), any privilege change requests (both successful and unsuccessful), user actions affecting security (such as password changes), attempts to perform actions not authorized by the authorization controls, all configuration changes etc. Additionally, the access to such logs must be controlled in accordance with the least privilege concept mentioned above, so that entries may not be deleted, accidentally or maliciously.</p>
4	<p>Hardening: All unnecessary packages must be removed and/or disabled from the system. Additionally, all unused operating system services and unused networking ports must be disabled or blocked. Only secure maintenance access shall be permitted, and all known insecure protocols shall be disabled.</p>
5	<p>Malicious Software Prevention: Implementation of anti-virus software on Servers and EDR on endpoints must be performed by the Selected Bidder, and other malicious software prevention tools shall be supported for all applications, servers, data bases, etc.</p>

6	<p>Network Security:</p> <ul style="list-style-type: none"> o The network architecture must be secure with support for UTM, Next Generation Firewall (NGFW) and encryption. The system shall also configure host-based firewalls. o Cloud services shall provide a web interface with support authentication to access and manage the resources deployed in cloud and provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing.
7	<p>Log Monitoring and Correlation: All Servers/ sub systems/ network devices/ appliances/ endpoints as proposed shall have capability and throw logs to the log server. The Logs and events generated by VMs, applications, DB, network, endpoints, security component/ devices of the system shall be monitored. The Selected Bidder must provide a Security information and event management (SIEM) solution for the same which shall be capable to analyse logs from all these sources and provide various security alerts, events, logs generated from various IT infrastructure (Hardware/Software) components. The Selected Bidder shall ensure the IT security compliance and therefore monitor the threats/ logs generated by various equipment's/ sub systems.</p>
8	<p>The Selected Bidder shall store all logs (event, security, etc.) for minimum 6 months. Also, Selected Bidder shall scale the storage if the existing storage space is full.</p>

T.3. SOC Administration

1	<p>The Selected Bidder shall provide 24*7*365 managed services for the entire security stack protecting GIC Re's environment. The Selected Bidder shall be responsible for managing configuration and patch management, vulnerability scanning, protecting data in transit and at rest, managing credentials, identity, and access management etc. The activities include:</p> <ul style="list-style-type: none"> o Appropriately configure the security groups in accordance with the Security policies. o Regularly review the security group configuration and instance assignment to maintain a secure baseline. o Secure and appropriately segregate/ isolate data/ application traffic by functionality using DMZs, subnets etc. o Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorized activity. o GIC Re conducts quarterly vulnerability scanning and penetration testing of its systems. The Selected Bidder shall comply with all the observations/ recommendations of all such audits. o Review the audit logs to identify any unauthorized access to GIC Re's systems. o The protection from unauthorized usage, detection of intrusions, reporting as required and proactive prevention actions are to be provided by Selected Bidder. o Service Component Administration. o User and Password Control. o Check and maintain access control. o Routine connection tests. o Change & Configuration Management. o IP, Port, Zone Configuration. o Firewall policies, IPsec VPN, SSL VPN configuration. o NAT, PAT configuration. o Antivirus/ IPS Signature update, when released by OEM. o Fault Management. o Response to alerts generated by systems or problems reported. o Troubleshooting, root cause analysis (RCA) and identification of problem area. o Resolution of problems through configuration changes/ re-installations/ replacements. o Escalate hardware failures to hardware vendor. o Assist hardware vendor to Identify problem area (by log collection & reboot). o Log Storage: Store critical logs in shared Syslog server for retention period of 180 days. o Configuration backup: Take incremental configuration backup daily for retention period of 90 days and Restoration of configuration when required.
---	--

	<ul style="list-style-type: none"> o Trouble ticket logging, update, and closure. o Managing configuration and security of Demilitarized Zone (DMZ) Alert/ advise department about any possible attack/ hacking of services, unauthorized access/ attempt by internal or external persons, ransomware, malware, etc and take necessary actions during such attacks/ events.
2	Incident Response - The Selected Bidder shall have policies and procedures in place for timely detection of vulnerabilities within organizationally owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. The Selected Bidder must also have policies and procedures in place to ensure timely and thorough incident management, as per established IT service management policies and procedures. The Solution shall be complied with ITIL (Information technology Infrastructure library) standards.
3	Governance & Risk Assessment - The Selected Bidder shall have organizational practices in place for policies, procedures and standards for application development and service provisioning as well as design, implementation, testing, use, and monitoring of deployed or engaged services in the cloud.

T.4. SOC Components

1	The Selected Bidder shall implement, configure, and manage all components mentioned in table below for GIC Re Environment.
2	The components must be sized for GIC Re's current Servers, systems, VMs, network, endpoints, etc. Growth during the Contract Period must also be considered during sizing. The Selected Bidder shall provide requisite licenses for all components for entire environment (DC, DR & Endpoints). The Selected Bidder shall provide rate cards for licenses/ units of each component for scaling up in the future.
3	GIC Re is in the process of procuring M365 E3 with Defender Plan 2 (as a separate Project). The Selected Bidder shall ensure that the MSS proposed as part of this project must integrate with the security features of M365 E3 with Defender Plan 2. Any overlap of below components must be highlighted to GIC Re.

MSS Components

#	Service/ Tool/ Solution	Remarks	Sizing
1	SIEM	Current SIEM (with only 70 log sources) throughput is 3500 Peak EPS.	The Selected Bidder shall size SIEM & SOAR for entire GIC Re Infrastructure and provide rate card for scaling up/ out. All other SOC components must be integrated with SIEM/ SOAR/ MSS.
	SOAR	Security Orchestration & Automation.	
2	IPS	Host & Network IPS	The Selected Bidder shall size properly for entire Network & Endpoints & Servers and provide rate card for scaling up/ out. Endpoint count provided in Annexure XII .
3	NGFW	Next Generation Firewall with UTM	The Selected Bidder shall size properly and provide rate card for scaling up/ out.
4	PIM/ PAM	Privilege & identity Access management solution	The Selected Bidder shall size properly and provide rate card for scaling up/ out.
5	Cloud WAF	Web Application Firewall for Public Applications	Currently needed for 5 Public Applications only and provide rate card for scaling up/ out.

6	DLP	Network DLP	The Selected Bidder shall size properly for entire Network & Endpoints & Servers and provide rate card for scaling up/ out. Endpoint count provided in <u>Annexure XII</u> .
		Endpoint & Server DLP	
7	Data Classification	For Endpoints, Servers & Network DLP	The Selected Bidder shall size properly and provide rate card for scaling up/ out.
8	Proxy	Cloud Proxy for all outgoing traffic	The Selected Bidder shall size properly and provide rate card for scaling up/ out.
9	EDR	Endpoint Detection & Response For all Endpoints	The Selected Bidder shall size properly for all endpoints and provide rate card for scaling up/ out. Endpoint count provided in <u>Annexure XII</u> .
10	Server Security	Anti-Virus for All Servers & VMs	The Selected Bidder shall size properly and provide rate card for scaling up/ out.
11	Cloud Sandboxing	Ransomware Protection for entire network	The Selected Bidder shall size properly and provide rate card for scaling up/ out.
12	Cloud DDoS	DDoS Protection for entire Network, with pooled mitigation for DC & DR	The Selected Bidder shall size properly and provide rate card for scaling up/ out.

U. Migration Approach

U.1. Migration Pre-Requisites	
1	The Selected Bidder shall support end-to-end migration from existing environment to the new environment.
2	The Selected Bidder shall assess the current environment to determine which workloads and applications are critical to GIC Re.
3	The Selected Bidder shall identify all users and stakeholders that would be impacted by the migration.
4	The Selected Bidder shall identify and understand the business processes and governance processes that are associated with current environment (both applications & infrastructure).
5	The Selected Bidder shall provide Application Management Services, in coordination with GIC Re's application support vendors, during migration period.
6	The Selected Bidder shall be required to understand the complete Application landscape to provide application related supports. The smooth running, data consistency, performance, etc., of all Applications shall be responsibility of the Selected Bidder.
7	The Selected Bidder shall understand the decomposition of applications & identification of common functions and services that can potentially be migrated, and identification of potential shared services. The Selected Bidder shall perform comprehensive analysis and understanding of the current environment, that incorporates considerations for security such as data sensitivity, legal or other regulatory issues, disaster recovery, etc.
U.2. Migration Planning	

1	<p>The Selected Bidder shall carry out comprehensive planning for migration of the application suite and data, including developing the migration roadmap, identifying the constraints and inhibitors to cloud migration, etc. The migration plan must have:</p> <ul style="list-style-type: none"> o The configuration proposed to fulfil day-1 requirements with the explicit understanding that during the duration of the contract these nominal profile requirements will change o Migration Tools, software, applications, scripts, and associated licenses must be planned and documented. o Procedures and documentation to be developed for migration of applications and data & content including re-development/ additional development that may be required. o Plans for co-existence of non-GCC and GCC architectures after migration. o Communication, change management, and training needs. o Cloud governance for post-implementation. o Test Plans/ Scenarios for verifying successful migration. o Detailed Risk Management Plan that will identify potential risks, set out possible mitigation approaches, and identify specific tasks the Selected Bidder shall undertake to help avoid all risks connected with the Migration.
---	---

U.3. Migration Procedure

1	<p>The Selected Bidder shall perform application and data migration based on:</p> <ul style="list-style-type: none"> o Complete architectural understanding of the existing applications and processes necessary for successful migration of the applications and data as well as continued operation and maintenance of the services. o Analysis of the interdependencies such as application dependencies and affinities to servers, server configurations, etc. o Dependencies between applications and DBs.
2	<p>The Selected Bidder shall provision the necessary compute & storage infrastructure on the GIC Re Hybrid Cloud Infrastructure (GCC & non-GCC), including the underlying licenses, to host the entire Application Suite that meet or exceed the day -1 minimum capacity.</p>
3	<p>The Selected Bidder shall setup the Development, Quality, Production and Disaster Recovery Environments by provisioning the necessary compute, storage, network & license infrastructure on the GIC Re Hybrid Cloud Infrastructure (GCC & non-GCC) to host the entire Application Suite. The migration shall also include the migration of underlying data & files from the current live DBs, storage in DBs, storage on the cloud, DB & data Backups, etc.</p>
4	<p>The Selected Bidder shall configure external connections (physical or logical) between the existing and proposed infrastructures, required to upload live Applications & DBs, historical backups, File system data and VM images to the new/ proposed environment.</p>
5	<p>To enable easy migration, GIC Re may consider up-gradation of OS & DB to latest versions available in market. The Selected Bidder shall perform all such necessary upgradation, in coordination with GIC Re's application support vendors.</p>
6	<p>GIC Re may consider deploying new Applications in the new environment during migration. The Selected Bidder shall perform all necessary activities to facilitate such requirements.</p>
7	<p>The Selected Bidder shall configure, manage, deploy, and scale the entire system and network on GCC & non-GCC Clouds.</p>

U.4. Migration Monitoring & Management

1	<p>The Selected Bidder shall manage (including project managing), coordinate and plan all aspects of migration.</p>
2	<p>The Selected Bidder shall proactively identify, monitor, and manage any significant risks or issues in relation to migration.</p>
3	<p>The Selected Bidder shall provide regular progress reports to GIC Re.</p>

4	The Selected Bidder shall provide and keep updating a list of all Migration Deliverables and Milestones, including acceptance status, the estimated time to completion, days overdue, planned completion date, and actual completion date and comments, as well as a report identifying the status of all Milestones.
5	The Selected Bidder shall provide and keep updating a list of all unresolved issues related to the execution of the Migration Plan, along with due dates, priority, responsible party, and an assessment of the potential and actual business impact and impact to the Migration Plan.
6	The Selected Bidder shall provide status of the any risks, including those identified in the Risk Management Plan, as well as the steps being taken to mitigate such risks.

V. Help Desk

- The Selected Bidder must provide multiple support options catering to the varying levels of support requirements (e.g., toll free number, ticket, chat, and forum) for GIC Re.
- GIC Re team shall be periodically visiting the DC & DR sites on quarterly basis or as and when required. Selected Bidder shall make convenient & secure provisions for at least 3 GIC Re personnel to access the Hybrid Cloud Infra and meeting with Selected Bidder personnel part of the NOC & SOC support services.
- The Selected Bidder must have Fire-proof space (with Lock & Key). If required Selected Bidder shall allow to store GIC Re's items, equipment, etc. Fireproof space should be under 24 x 7 under CCTV monitoring.
- The Selected Bidder shall ensure availability of at least one dedicated support person having 5+ years of experience in Coordinating & Managing services (NOC+SOC+TELECOM) for the Hybrid Cloud Infrastructure in GIC Re's premises during the entire duration of the contract.

W. Maintenance & Support of implemented Cloud

- The Selected Bidder shall be responsible for providing 24*7*365 days' support to the infrastructure from the date of issuance of operational acceptance by GIC Re, ensuring Uptime and utilization of the cloud resources as per SLA's defined in this RFP. In the event of a disaster at DC site, activation of services from the DR site is the responsibility of the Selected Bidder.
- GIC Re performs VAPT Audit every quarter through third-party Auditors. The Selected Bidder must update/ patch the system in response to any adverse findings in the report, without any additional cost to GIC Re.
- The Selected Bidder is required to provision additional resources (VMs, Servers, compute, storage, network, etc.) when the utilization exceeds 80%.
- The Selected Bidder shall develop appropriate policy, checklists in line with ISO 22301, ISO 27001 & ISO 20000 framework for failover and fallback to the appropriate DR site.
- The Selected Bidder support team shall Interface with the technical team of The Selected Bidder on behalf of GIC Re for all activities including monitoring the reports (e.g., usage, security, SLA, etc.), raising (or escalating) tickets/ incidents and tracking the same to resolution
- On expiration/ termination of the contract, The Selected Bidder shall handover complete data, VMs, Servers, etc. in the desired format to GIC Re which should be easily accessible and retrievable.

6. PERFORMANCE/ SLA MANAGEMENT

The Selected Bidder's project manager shall submit to GIC Re in the first week of the calendar month, a performance report, which shall document the performance with respect to the service levels during the previous month. These reports will form the basis for the monthly & quarterly reviews for the Service level metrics and or addition/ changes to the schedule. SLAs shall be measured monthly.

The purpose of this clause is to clearly define the levels of service which shall be provided by the Selected Bidder to GIC Re during the Contract Period. This clause, as specified below, is applicable to the Data Center and the Disaster Recovery sites and all services as described in Scope of Work. However, the same shall be measured independently for each site and service.

- a) The Selected Bidder shall provide GIC Re with methodologies/ tools to demonstrate ability to meet the performance requirements stated in the proposed contractual SLAs. A ticketing tool, for creating/ managing incidents & service-related requests, must be provided as mentioned in Scope of Work. The tool must have a dashboard to monitor all open & closed tickets.
- b) **Service Availability & Helpdesk Support:**
- The Selected Bidder shall provide on demand 24*7*365 support as defined in Scope of Work.
 - The Selected Bidder shall provide a 24*7*365 Helpdesk Support Center to handle fault reporting, trouble ticketing and related enquiries during the Contract Period.
 - Incident tickets can be logged at any time via email/ ticketing tool/ call/ SMS.
 - Service requests can be logged at any time via email/ ticketing tool/ call/ SMS.
 - List of all such Incidents & Service Requests (both open & closed) must be available for GIC Re's perusal at any time either via reports or dashboard.
- c) **Incident Management:**
Incident refers to any event/ abnormality/ action in the functioning of the Data Center equipment/ component/ specified services that may lead to disruption in normal operations of the services to GIC Re or access to any applications, VMs, servers, network, etc.
While Creating an Incident Ticket either via tool/ email, it shall be necessary to provide a summary and details of the incident. The category and incident priority fields must also be set.
Incidents will be categorized as follows:
- Users not able to access desired services/ components/ applications/ network from any branch/ spoke location (including foreign branches).
 - Quality of access i.e., speed/ latency of network, performance of servers, etc., are poor/ not up to mark.
 - Other outage/ disruption related incidents.
- Every Incident/ Event that is not resolved within the agreed timeline will be considered as breach of SLA attracting liquidated damages as per the **Liquidated Damages clause (Clause 24)** in **Annexure V**.
- d) **Service Request (SR) Management:**
Service Request management is for any changes to the environment, inclusion of new VMs/ applications/ functionalities, patch updating, Scaling up or down, removal of unnecessary VMs/ applications/ functionalities, DR Drills, etc. Within the ticketing tool, GIC Re should be able to create a Service Request. When creating a Service Request, it will be necessary to provide a summary, details of the service, the timelines for completion, and any other details (if applicable).
The Service Request is categorized as follow:
- Creation/ provisioning of new VMs/ Servers.
 - Scaling up/ down of components like compute/ network/ storage, etc.
 - Patch/ version upgrade of any kind.
 - Removal/ Decommission of VMs/ Servers.
 - User access management: adding/ removing users, change in access to applications/ servers/ networks.
 - Requests related to reports & dashboard.
 - Other new change or service-related requests
- The service request type will be resolved as per the agreed timeline between GIC Re and Selected Bidder. Every Service Request that is not resolved within the agreed timeline will be considered as breach of SLA attracting liquidated damages as per the **Liquidated Damages clause (Clause 24)** in **Annexure V**.
- e) The Selected Bidder should develop procedures and tools for performance measurements including, but not limited to, the following:
- Quality of work: defect rate, re-work rate
 - Response time
 - Service fulfilment rate
 - User Satisfaction (GIC Re)
- f) **Uptime:** Uptime shall mean the time-period for which the specified services/ components with specified technical and service standards are available to GIC Re. Uptime, in percentage, of any component (Non-IT & IT) can be calculated as:

Uptime = { 1 - [(Downtime) / (Total Time – Maintenance Time)] } * 100

- g) **Downtime:** Downtime shall mean the time for which the specified services/ components with specified technical and service standards are not available to GIC Re and excludes the scheduled outages planned for the DC & DR.
- h) **Response Time:** Response time refers to how quickly Selected Bidder's support team will acknowledge with suggested solution to an issue being raised as ticket, email, or other methods with subsequent status updates in email/ tool dashboard.
- i) **Resolution Time:** Resolution Time shall mean the time taken, after the incident has been reported at the helpdesk, in resolving (diagnosing, troubleshooting, and fixing) or escalating (to the second level or to respective OEMs/ Selected Bidders, getting the confirmatory details about the same from the Selected Bidders and conveying the same to GIC Re) the service-related troubles. A resolution time refers to how long it takes from the time an issue/ ticket is logged/ created until it is fully resolved.
- j) All times are from the beginning of the occurrence of the event when logged. Thus, in an emergency, a response is required in fifteen minute's time from the raising of incident and solution must be provided, and the problem has also to be solved within 45 minutes of the occurrence of the event. Penalties associated with missed deadlines are provided in **Clause 24** of **Annexure V**.
- k) The Incident and Service Requests shall include Hosting Service/ Component disruption of any kind, such as (but not limited to):
- Core business process cannot be carried out till SR/ Incident is resolved.
 - Applications/ VMs/ network cannot be accessed from branches/ spoke locations.
 - Unavailability of routers/ SD-WAN CPEs/ network devices and users unable to access the network (MPLS, ILL, etc.).
 - Security or disruptive incident or service request related event of any kind.
 - Incident/ Service Request has serious impact on critical tasks and no workaround is available.
 - Delay in provisioning/ update of VM/ Server/ Network/ backup/ any other component, etc. which impacts business processes.
 - System/ VM/ network/ solution cannot function as designed or installed.
 - Compliance timeline is affected due to pending SRs.
 - Isolated incident or SR of any kind.
 - Degraded performance and/ or is difficult to use (network/ servers, etc.).
 - SRs related to general information, service, or consultation.
 - SRs related to Backups, Version enhancements, scaling VMs/ network up or down, etc.
 - SRs related to Report enhancements.
 - Any other Incident or Service Request raised by GIC Re.

The Severity, Response & Resolution Time will be monitored as per the Proposed Service Level Matrix given below:

Priority/ Severity	Impact	Response Time	Resolution (including Response) Time
Emergency/Very High/ Critical	Entire organization/ majority users (>300) are affected.	15 minutes	1 hour
High	Multiple users (>200) or departments are directly affected.	30 minutes	90 minutes
Medium	Medium number or medium group of users (>100) are directly affected.	30 minutes	4 hours
Low	Small number or small group of users (<100) are directly affected.	30 minutes	8 hours

7. IMPORTANT DATES

Event / Activity	Date / Time
Release of Request for Proposal (RFP)	22 nd March 2022

Last Date for receipt of Queries from Bidders through e-mail*	4 th April 2022
Pre-Bid Meeting	5 th April 2022
Last Date for Submission of e-Tender Bids	22 nd April 2022, 01:00 PM
Opening of Prequalification and Technical Bids	22 nd April 2022, 01:00 PM
Presentation by individual Bidders	Date will be intimated by email.
Opening of Commercial Bids	To be intimated to the Technically Qualified Bidders and published on website

*Queries are to be submitted at E-mail: itmg@gicofindia.com (No queries will be accepted on telephone or through any means other than e-mail.) and clarifications on queries will be uploaded on the GIC Re website www.gicofindia.in after last date of receipt of queries. The queries are to be submitted by the bidders in the format given below:

#	Page No.	Clause from the RFP	Amendment/ Clarification desired in the clause

SECTION – II: INSTRUCTIONS/ GUIDELINES TO BIDDERS

1. **BINDING TO ALL - TERMS & CONDITIONS**

The Bidders are advised to submit the bids strictly based on the terms and conditions and specifications contained in this RFP including amendments, if any, issued by GIC Re prior to the date of submission of the Bids. The formats prescribed in this RFP should be scrupulously followed by the Bidders. Bids that do not comply with the terms and conditions hereof or are incomplete are liable for rejection. The Bidder must take due care and caution in this regard. Since the nature of this procurement is such that the order cannot be split, hence, the whole order will be awarded to a single Bidder only.

2. **PRE-QUALIFICATION CRITERIA (PQC)**

The Bidders must upload PQC online as mentioned in **Annexure II**. The template and required documents must be filled and uploaded by all Bidders.

3. **METHOD OF BID SUBMISSION**

The Bidders are required to submit their respective bids as per the instructions given in **Annexure I**.

- a) All Bids are to be submitted online on the website <https://gicre.eproc.in> as e-tenders (herein referred to as bids/e-tenders). No bid shall be accepted off-line. The bids shall be received only “online” on or before the scheduled date and time of bid submission.
- b) The bids received after the specified date & time for receipt of bids shall not be considered.
- c) Pre-Qualification criteria (PQC) is to be uploaded online as per **Annexure II**. Further, On request original documents should be produced failing which the bid/e-tender is liable for rejection.
- d) Technical Bids as per **Annexures III & XV** and other documents sought along with the technical bid are to be uploaded online.
- e) Commercial bid as per **Annexure IV** is to be submitted online.
- f) Undertaking by the Bidder as per the **Annexure IX** shall be made on the letter head of the Bidder’s company, duly signed by authorized official along with the seal of body corporate and shall be uploaded online.
- g) The Successful Bidder shall submit the Performance Bank Guarantee (PBG) as per the **Annexure VI**.
- h) A self-signed and stamped scanned copy of EMD deposit through NEFT/RTGS or Bank Guarantee from any of the commercial bank as stipulated in Section-II Point 3 below should be uploaded on the E-procurement portal.
- i) In the e-tender system, after uploading the bid, the Bidder need not send any documents (hard copy) to the tender inviting authority before opening of technical bid/price bid. If required, after opening of bid, the authenticity of the uploaded documents would be verified by the tender inviting authority. As such on request original documents should be produced failing which the bid/ e-tender is liable for rejection.

4. **EARNEST MONEY DEPOSIT (E.M.D.)**

- Every Bidder, except those eligible for EMD waiver as mentioned in Section-II Point 4, shall submit non-interest bearing EMD of ₹ 2,00,00,000/- (Rupees Two Crores only).
- The Bidder must deposit Earnest Money Deposit in the form of the RTGS/ NEFT into the account of “General Insurance Corporation of India” as per details given below.

Sr. No.	Details of Bank Account	
1.	Name of Beneficiary	General Insurance Corporation of India
2.	Type of Account	Current

3.	Account Number	001020100010245
4.	Name of the Bank	Bank of India
5.	Name of the Branch	Churchgate, Mumbai
6.	Address of Branch	Eros Building, Churchgate, Mumbai – 400020
7.	MICR Code No.	400013014
8.	IFSC Code No.	BKID0000010

- The RTGS/ NEFT transaction should have been done at least 2 days before the final submission of the bid.
- The EMD will not carry any interest.
- No previous dues of the Bidder shall be adjusted towards the above transaction of EMD.
- Micro and Small Enterprises (MSEs) as defined in MSE Procurement Policy issued by Department of Micro, Small and Medium Enterprises (MSME) or as registered with the Central Purchase Organization or the concerned Ministry or Department are exempted from payment of EMD. For availing such exemption Bidder must submit the current relevant certificate.
- The Bidder shall use RTGS/NEFT transaction for this RFP only, otherwise his bid will be rejected.
- The account from which the EMD amount is to be deposited/transferred should be in the name of Bidder/authorized person of the Bidder who has digitally signed the bid.
- Refund of EMD, in respect of unsuccessful Bidders, will be made to that specific account only from which the EMD was received and within two weeks of tender result declaration.

Forfeiture of EMD

The EMD submitted by the Bidder will be forfeited in the following circumstances–

- a) if the Bidder withdraws the bid after acceptance by GIC Re; or
- b) if the Bidder withdraws the bid before the expiry of the Bid validity period; or
- c) if the Bidder Violates any of the provisions or the terms and conditions of the Bids.
- d) If the Bidder alters its Bids during the Bid Validity Period
- e) In case of the successful Bidder, if the Bidder fails to furnish the Service Level Agreement, Reciprocal Non-Disclosure Agreement, Integrity Pact, Code of Integrity, Deed of Indemnity and/or Performance Bank Guarantee in accordance with provisions, terms, and conditions of this RFP.

Refund of EMD

- a) EMD of the successful Bidder shall be refunded after delivery and verification of all the system/equipment and execution of Service Level Agreement (SLA), Reciprocal Non-Disclosure Agreement (NDA), Deed of Indemnity, Integrity Pact and Performance Bank Guarantee ('PBG').
- b) In case of unsuccessful Bidders, EMD would be refunded after final selection of successful Bidder.
- c) In case of rejection of e-tender/ unsuccessful e-tender, the EMD will be refunded to the Bidders after intimation of rejection of e-tender.

5. PREFERENCE TO MICRO AND SMALL ENTERPRISES (MSEs)

This shall be strictly in terms of the mandates of the Public Procurement Policy for Micro and Small Enterprises (MSEs) Order, 2012.

- a) For this clause, Micro and Small Enterprises ("MSEs") shall be as defined by The Micro, Small and Medium Enterprises Development Act, 2006 (as amended from time to time).
- b) MSEs shall be given the tender document free of cost.
- c) MSEs shall be exempted from payment of earnest money deposit (EMD) subject to furnishing of relevant valid certificate for claiming exemption.
- d) A purchase preference of 100% of the project will be awarded to any MSE bidder quoting within

price band of L1+15 (fifteen) percent by bringing down their price to L1 price.

- e) A purchase preference of 100% of the project will be awarded to MSE bidder, owned by Schedule Caste (SC)/ Scheduled Tribe (ST) entrepreneurs, quoting within price band of L1+15 (fifteen) percent by bringing down their price to L1 price. For this clause, MSEs would be treated as owned by SC/ST entrepreneurs in the following cases:
 - i. In case of proprietary MSE, proprietor(s) shall be SC/ST.
 - ii. In case of partnership MSE, the SC/ST partners shall be holding at least 51% (fifty-one percent) shares in the unit.
 - iii. In case of Private Limited Companies, at least 51% (fifty-one percent) share shall be held by SC/ST promoters.
- f) MSE's must, along with their bid, provide proof of their being registered as MSE (indicating the terminal validity date of their registration) for the item tendered, with any agency mentioned in the notification of the Ministry of Micro, Small and Medium Enterprises (Ministry of MSME) as well as of being owned by SC/ST entrepreneurs.
- g) MSEs shall be given relaxation as far as prior turnover is concerned.
- h) MSEs shall be given relaxation as far as prior experience is concerned.

6. SPECIAL CONDITIONS FOR STARTUPS

- a) For the purpose of this clause an entity shall be considered a Start Up in the following cases:
 - i. Up to ten years from the date of its incorporation/ registration.
 - ii. If its turnover for any of the financial years has not exceeded ₹ 100 (Rupees One Hundred) crores.
 - iii. It is working towards innovation, development, improvement of products or processes or services or if it is a scalable business model with high potential of employment generation or wealth creation.
- b) Provided further that to obtain benefits, a start-up so identified under the above definition shall be required to be recognized as Start Up by the Department for Promotion of Industry and Internal Trade.
- c) Startups shall not be eligible for any kind of relaxation as far as quality or technical specifications mentioned in the RFP are concerned.
- d) Startups shall be given relaxation of 3 crores as far as prior turnover is concerned.
- e) Startups shall be given relaxation of 1 year as far as prior experience is concerned.

7. OPENING OF PRE-QUALIFICATION AND TECHNICAL BID

Bidder should follow the server time being displayed on Bidder's dashboard at the top of the tender site, which shall be considered valid for all actions of bid preparation, bid submission, bid opening etc., in the e-tender system.

The encrypted bids received will be decrypted and opened online, on the scheduled date and time at the address (mentioned in the covering page of this RFP) in the presence of those Bidders who have submitted the bid and wish to remain present. The Bidders are required to send their representative/s who is/are vested with powers to take decision. The authorized representative should bring a letter on Bidder's letterhead authorizing him/her to attend the bid-opening. Without this letter, he/she may not be allowed to attend the bid-opening meeting. After evaluation of bid, all the Bidders will get the information regarding bid status. Thereafter, a system generated email confirmation will be sent to all Bidders. The Bidders can check information regarding the status of their bids and ranking on e-procurement portal.

8. PROCEDURE FOR PROCESSING THE BIDS

- a) Documents containing Pre-Qualification and Technical bids would be opened on the specified date and time.
- b) Technical bids will be evaluated of only those Bidders who have met the Pre-Qualification criteria.
- c) The documents submitted by the Bidders would be evaluated by the Technical Sub Committee of GIC Re. Bidders will be scored on the parameters defined in **Annexures III & XV**. Bidders will

be scored out of a total of 100 marks and the ones scoring above 75 will qualify for commercial bid opening.

- d) Commercial bids would be opened of only those Bidders who have been qualified in technical bid. The authorized Signatory of shortlisted Bidders who wish to remain present for financial bid opening should bring a letter on Bidder's letterhead authorizing him to attend the financial bid opening. The time, place and the date would be intimated to the shortlisted Bidders later.
- e) Commercial bid with the lowest cost will be identified as the successful Bidder. If for any reason, the Bid of any Successful Bidder(L1) is rejected, GIC Re may at its discretion: -
 - i) Consider the next lowest Financial Bid(L2)
 - ii) Annul the bid process or
 - iii) Take any such measure as may be deemed fit in the sole discretion of GIC Re
- f) In Commercial bid, if a Bidder quotes 'NIL' charges/ consideration, the bid shall be treated as unresponsive and will not be considered/shall be rejected.
- g) Any efforts made by the Bidder to influence GIC Re in the evaluation/ contract award decision, may result in the rejection of the bid.
- h) In case of any wrong calculations or mathematical errors, if the bid opening committee suggests corrections and the Bidder does not accept it, the bid shall be rejected.
- i) Bids received after the specified date and time of receipt, shall not be considered.
- j) Any bid incomplete in any respect or deviating from the specified format would not be considered. This procedure is subject to changes and the procedure adopted by GIC Re for opening the bids shall be final and binding on all the parties.

9. REJECTION OF BIDS

The e-bids are to be rejected due to any of the following reasons: -

- a) If it is received after the expiry of the due date and time.
- b) If it is not accompanied by the requisite EMD.
- c) If the bid is conditional.
- d) If it is not in conformity with the instructions mentioned herein.
- e) If it is incomplete including non-furnishing of the requisite documents.
- f) Any quotation or billing linked to GIC Re's Assets and/or Revenue will disqualify the Bidder.
- g) If there is canvassing/ lobbying/ influence regarding short listing, status etc. of any kind, GIC Re reserves the right to reject any or all the bids submitted by a Bidder without assigning any reasons whatsoever and the decision of GIC Re would be final and binding. GIC Re reserves the right to cancel the tender process partly or fully at its sole discretion at any stage without assigning any reason to any of the participating Bidders. GIC Re also reserves the right to re-issue or re-commence the entire bid process without the Bidders having the right to object. Any decision of GIC Re in this regard shall be final, conclusive, and binding on the Bidders.

10. BID VALIDITY PERIOD

Bid should be valid for acceptance for a minimum period of at least **90 (Ninety) days** from the date of opening of bids. The validity may be extended by mutual consent. Bids with lesser validity period would be rejected.

11. DEBARMENT FROM BIDDING

- a) A Bidder shall be debarred from further bidding under the same or future procurements if he has been convicted of an offence—
 - i. under the Prevention of Corruption Act, 1988; or
 - ii. the Indian Penal Code or any other law for the time being in force, for causing any loss of life or property or causing a threat to public health as part of execution of a public procurement contract.
- b) A Bidder debarred under sub-section (i), or any successor of the Bidder shall not be eligible to participate in a procurement process of GIC Re for a period not exceeding three years commencing

from the date of debarment.

12. CLARIFICATION OF BIDS, SHORTFALL OF INFORMATION/ DOCUMENTS

During evaluation and comparison of bids, GIC Re may, at its discretion, ask the Bidder for clarifications on the bid and/or shortfall information/documents. The request shall be given in writing by registered/ speed post/ email, asking the Bidder to respond by a specified date, and mentioning therein that, if the Bidder does not comply or respond by the date, his bid will be liable to be rejected. Depending on the outcome, such bids will be rejected or considered further. It is however, clarified that no post-bid clarification at the initiative of the Bidder shall be entertained.

13. SERVICE LEVEL AGREEMENT AND PERFORMANCE BANK GUARANTEE

The successful Bidder shall enter into a detailed Service Level Agreement (SLA) with GIC Re as per draft given in **Annexure V** within 30 days from the receipt of notification of award of the contract. However, GIC Re reserves the right to alter/ vary/ amend/ modify all or any of the terms set out in the said draft Agreement before the same is signed.

The successful Bidder shall at its own expense provide a Performance Bank Guarantee (PBG) to GIC Re at the rate of **3%** of the total Commercial bid value for performance guarantee within 14 days from the receipt of notification of award of the contract from GIC Re, which shall be an unconditional, irrevocable, and continuing PBG from a scheduled commercial bank acceptable to GIC Re, payable on demand, for the due performance and fulfillment of the ensuing contract. PBG should be submitted in the format given in **Annexure VI**. GIC Re reserves the right to amend/ modify/ delete all or any of the terms set out in the draft PBG before the same is delivered. The PBG should remain valid for a period of 60 days beyond the date of completion of all contractual obligations of the successful Bidder including warranty obligations. The PBG shall be invoked in the event of breach of the ensuing contract documented in the said SLA by the successful Bidder. On reduction of value of PBG owing to such invocation, the successful Bidder shall forthwith replenish/restore the PBG to its original value within 15 days starting from the date of such breach.

14. INTEGRITY PACT

The Bidders that desire to bid against this RFP, shall compulsorily sign an Integrity Pact with GIC Re to be monitored by the INDEPENDENT EXTERNAL MONITORS (IEMS). IEMS would review independently and objectively whether and to what extent Bidders have complied with their obligations under the Integrity Pact. This project will be reviewed by following Independent External Monitors-

- a) Dr. Atanu Purkayastha
- b) Mr. Umakant Lal

The said Integrity Pact can be downloaded from the 'Media - Downloads – Policies and Guidelines' link on the website <https://www.gicofindia.com/>. The Bidder should submit Integrity Pact Agreement signed by the authorized representative of Bidder with office seal on a non-judicial stamp paper of INR 100/-. The Agreement will be counter- signed for and on behalf of GIC Re after opening of the Pre-Qualification and Technical bid.

15. CODE OF INTEGRITY

No official of GIC Re or a Bidder shall act in contravention of the codes which includes

- a) Prohibition of:
 - making offer, solicitation or acceptance of bribe, reward or gift or any material benefit, either directly or indirectly, in exchange for an unfair advantage in the procurement process or to otherwise influence the procurement process.
 - any omission, or misrepresentation that may mislead or attempt to mislead so that financial or other benefit may be obtained, or an obligation avoided.
 - any collusion bid rigging or anticompetitive behavior that may impair the transparency, fairness, and the progress of the procurement process.

- improper use of information provided by the GIC Re to the Bidder with an intent to gain unfair advantage in the procurement process or for personal gain.
- any financial or business transactions between the Bidder and any official of the GIC Re related to this RFP or execution process of contract, which can affect the decision of GIC Re directly or indirectly.
- any coercion or any threat to impair or harm, directly or indirectly, any party or its property to influence the procurement process.
- obstruction of any investigation or auditing of a procurement process.
- making false declaration or providing false information for participation in a procurement process or to secure a contract.

b) Disclosure of conflict of interest:

The Bidder participating in a bidding process must not have a Conflict of Interest. A Conflict of interest is a situation in which a party has interests that could improperly influence that party's performance of official duties or responsibilities, contractual obligations, or compliance with applicable laws, rules, and regulations.

A Bidder may be in conflict of interest with one or more parties in the bidding process if, including but not limited to:

- Have controlling partners/shareholders in common; or
- Receive or have received any direct or indirect subsidy from any of them; or
- Have the same legal representative for purposes of the bid; or
- have a relationship with each other, directly or through common third parties, that puts them in a position to have access to information about or influence on the bid of another Bidder, or influence the decisions of the procuring entity regarding the bidding process; or
- The Bidder participates in more than one bid in a bidding process.

c) Disclosure by the Bidder of any previous transgressions made in respect of the provisions of sub-clause (i) with any entity in any country during the last three years or of being debarred by any other procuring entity.

In the event that GIC Re, after giving a reasonable opportunity of being heard comes to the conclusion that a Bidder, has contravened any of the above, it may take appropriate measures including removing the Bidder's name from the list of registered suppliers, rejecting the bids of the Bidder, taking other punitive actions such as cancellation of contracts, banning and blacklisting, debaring the Bidder or any of its successors, from participating in any procurement process undertaken by GIC Re, for a period not exceeding two years, or action in Competition Commission of India, and so on.

All Bidders are required to abide with the above Code of Integrity and shall sign and submit a declaration in this respect in the format attached as **Annexure X**.

16.COMPLIANCE WITH INFORMATION SECURITY POLICY

The selected Bidder shall follow the Information Security Policy of GIC Re. In case the selected Bidder is found to be in violation of the said policy, GIC Re reserves the right to terminate the contract in addition to any other remedies for breach, injunctive relief, and indemnity as per the contract and the applicable laws.

17.NON DISCLOSURE AGREEMENT

The Successful Bidder shall sign Non-Disclosure Agreement (NDA) as per **Annexure VII** with GIC Re for the entire Contract Period to maintain and protect the confidentiality of data and information. The Bidders will treat data and information about the GIC Re, obtained in the execution of this e-Tender including any business, technical or financial information, in strict confidence and will not reveal such information to any other party.

18.DEED OF INDEMNITY

The Successful Bidder shall execute and furnish to GIC Re a Deed of Indemnity as per **Annexure**

VIII.

19. GENERAL TERMS

- a. The contract shall be in force for the Contract Period, i.e., total period including implementation & migration phase plus 5 years from the date of Go-Live declared by GIC Re. However, the contract can be extended further as mutually decided by GIC Re and the selected Bidder.
- b. If at any point of time, the services of the successful Bidder are found to be non-satisfactory then the contract will be terminated, giving notice in advance as mentioned in Service Level Agreement.
- c. Correct technical information of the service being offered must be filled in. Filling up of the information using terms such as “OK”, “Accepted”, “Noted”, “As given in Brochure/ Manual” “negotiable”, “to be discussed” is not acceptable. GIC Re may treat such bids as not adhering to the guidelines and as unacceptable.
- d. The Bids and all supporting documents submitted by the Bidder as part of the RFP responses shall become the property of GIC Re.
- e. Amendments/Corrigendum in the RFP, if any, would be hosted on our website and Central Public Procurement Portal (CPPP).
- f. GIC Re reserves the right to -
 - Add, modify, relax, or waive any of the conditions stipulated in this RFP whenever deemed necessary.
 - To reissue the RFP
 - Cancel/ withdraw the RFP process at any stage without assigning any reasons thereof
- g. The Bidder must submit the bid document online well in advance before the prescribed time to avoid any delay or problem during the submission process.
- h. It is construed that the Bidder has read all the terms and conditions before submitting the bid.
- i. GIC Re will not be held responsible for any technical snag or network failure during on-line bidding.
- j. It is the Bidder’s responsibility to comply with the system requirement i.e., hardware, software, and internet connectivity at Bidder’s premises to access the e-tender website. GIC Re shall not be liable to the Bidders for any direct / indirect loss or damages incurred by them arising out of incorrect use of the e-tender system or internet connectivity failures under any circumstances.
- k. In case of any technical assistance on bid preparation/submission, login, registration, etc., kindly contact the following team: -

Contact and Follow-up team:

HELPDESK NUMBERS ARE OPEN BETWEEN 1000 HRS to 1800 HRS IST		
(MONDAY TO FRIDAY (Excluding GIC Re HOLIDAYS))		
Contact Nos. and email IDs for helpdesk officers		
Dedicated email	gicresupport@c1india.com (Please email your issues before your call helpdesk. This will help us serving you better.)	
Global support number	+91-22-66865600	
Dedicated helpdesk for GIC Re Suppliers		
Name	Email	Phone Numbers
Ujwala Shimpi	ujwala.shimpi@c1india.com	+91-124-4302000 Ext: 114
Saranraj Naicker	saranraj.naicker@c1india.com	+91-124-4302000 Ext: 110
Escalation Level		
Fairlin Jivin	fairlin.jivin@c1india.com	+91-124-4302000 Ext: 112
Steven Crasto	steven.crasto@c1india.com	

- l. In case of any tender-related queries, kindly contact us at: -

General Insurance Corporation of India, ITMG Department, 1st Floor, Suraksha,
170, J. Tata Road, Churchgate, Mumbai-400020

Phone: +91-22-2286 7162, 7115, E-mail: itmg@gicofindia.com

20.PRICE

- a) Price quoted shall be in Indian Rupees (INR) only.
- b) The price quoted by the Bidder should be exclusive of applicable taxes like Goods & Services Tax (GST). GST as applicable will be paid additionally on actuals. GIC Re would be entitled to deduct TDS as applicable while making payments according to the Indian taxation rules.
- c) There shall be no escalation in the prices once the prices are fixed and agreed to by GIC Re and the successful Bidder. But any benefit arising out of any subsequent reduction in the prices due to reduction in duty & taxes after the prices are fixed should be passed on to GIC Re.

21.SCHEDULE & PAYMENT TERMS

The stipulated delivery schedule and payment terms is as per terms of the SLA: -

- a) The Selected Bidder shall complete the implementation and migration from current DC and DR sites to proposed DC & DR sites within **16 weeks** of acceptance of the Purchase Order (PO). The new Setup/ environment must be end-user ready and fully live/ functioning within **16 weeks** of acceptance of PO.
- b) One-time charges would be paid as per Commercial bid (**Annexure IV**) on completion of all activities as per Scope of work, to the satisfaction and sign-off from GIC Re.
- c) Recurring charges would be paid at the end of each quarter, on receipt of invoice, thereafter for the duration of the Contract Period.

22.LIQUIDATED DAMAGES

In the event of delay in performance and/or non-performance and/ or breach of any of the terms of the contract, GIC Re will be entitled to liquidated damages as per SLA (**Annexure V**).

23.TERMINATION OF CONTRACT

GIC Re shall have the unilateral right to terminate any agreement/contract(s) formed between GIC Re and the successful Bidder(s) as per "Termination Clause" of annexed Service Level agreement.

24.DISASTER RECOVERY SUPPORT

The successful Bidder is expected to manage DR Site at GIC Re in the System Landscape with fail-over provision to servers at GIC Re's Disaster Recovery site.

25.INTELLECTUAL PROPERTY RIGHTS

All plans, drawings, specifications, designs, reports, software configuration, customized materials used to provide the services (for such items as source code, object code, user manuals and documentation) other documents prepared by the successful Bidder for GIC Re under this contract shall become and remain the property of GIC Re. The Selected Bidder may retain a copy of such documents, but shall not use anywhere, without taking permission, in writing, from GIC Re, and GIC Re reserves right to grant or deny any such request.

26.SUB-CONTRACTING

Neither the contract hereunder nor any part thereof shall be sub-contracted or assigned by the selected Bidder without the specific written consent of GIC Re. If such consent is granted, the selected Bidder shall ensure that the sub-contractor complies with all the requirements of this RFP and the contract, and the selected Bidder shall remain liable to GIC Re for all acts and omissions of the sub-contractor as if they were acts and/or omissions of the selected Bidder himself.

27. BIDDER'S UNDERSTANDING OF THE RFP

In responding to this RFP, the Bidder accepts the full responsibility to understand the RFP in its entirety, and in detail, including making any inquiries to GIC Re as necessary to gain such understanding. Bidder accepts sole responsibility regarding any mistake as to fact pertaining to the services sought, and GIC Re shall have the sole discretion to cancel the award to the Bidder who is at material variance with the object of this RFP. Such disqualification and/or cancellations shall be at no fault, cost, or liability whatsoever to GIC Re.

28. GOOD FAITH STATEMENT

All information provided by GIC Re in this RFP is offered in good faith. Individual items are subject to change at any time. GIC Re makes no certification that any item is without error. GIC Re is not responsible or liable for any use of the information or for any resulting claims.

29. PUBLICITY

Any publicity by the selected Bidder in which the name of GIC Re is to be used should be done only with the explicit written permission of GIC Re.

30. ANTI FRAUD AND CORRUPTION

It is the GIC Re's policy to require that GIC Re as well as the Bidders observe the highest standard of ethics and propriety during the procurement process, execution of the contract, the contract duration and thereafter (hereinafter referred to as the 'Contract Cycle').

Definitions:

In pursuance of this policy, the GIC Re defines, for the purpose of this provision, the terms set forth below as follows:

- (1) "Corrupt Practice" means the offering, promising, giving, receiving, or soliciting, directly or indirectly, anything of value, either tangible or intangible, which a person is not entitled to, to influence or which has the potential to influence the action of an official during the Contract Cycle.
- (2) "Fraudulent Practice" means the following:
 - i. a misrepresentation or omission of facts or submission of fake or forged documents in order to influence any component of the Contract Cycle.
 - ii. an intentional act of commission or omission designed to deceive, resulting in GIC Re suffering a loss and/or the perpetrator achieving a gain.
- (3) "Collusive Practices" means a scheme or arrangement whether formal or informal, between two or more Bidders, with or without the knowledge of the GIC Re, designed to establish prices at an artificial, noncompetitive levels or which affects submission or non-submission of bids.
- (4) "Coercive Practices" means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in a procurement process or affect the contract cycle.

Misdemeanor for this purpose shall include Corrupt, Fraudulent, Collusive and Coercive practices which shall carry meanings as per the definitions above.

Measures to be taken by the GIC Re:

- (1) GIC Re will be within its rights to terminate the contract with the selected Bidder for any Misdemeanor during the Contract Cycle, ban/blacklist/debar the Bidder from this and further procurements and the like.
- (2) GIC Re will be within its rights to take any other action against the Bidder deemed appropriate as per the terms of this RFP, the ensuing SLA as well as the law of the land.

Measures to be taken by the Bidders:

- (1) The Bidder shall during the entire Contract cycle, comply with the provisions of the Anti- Fraud Policy of GIC Re and not commit any Misdemeanor.
- (2) The Bidder shall procure the compliance with the above obligations (as mentioned in a.) from its associated persons, officers, employees, agents, subcontractors, or independent contractors as may be used for the fulfilment of its obligations under this RFP and the ensuing SLA during the entire Contract cycle.

The Bidder undertakes that the Bidder shall be responsible to GIC Re for the Misdemeanors and non-compliance of the Anti-Fraud Policy committed by the above-named persons during the entire Contract cycle.

- (3) If the Bidder gains knowledge of any conduct by any of its associated persons, officers, employees, agents, subcontractors, or independent contractors which constitutes a Misdemeanor or non-compliance of the Anti-Fraud Policy, or if it has reasonable suspicion of the existence of such conduct, it shall immediately inform GIC Re of such knowledge and if requested by GIC Re, provide information it may reasonably require regarding such conduct.

31.COMMUNICATION

Verbal communication shall not be effective unless formally confirmed in writing by GIC Re. In no case shall verbal communication govern over written communication.

Bidder's queries related to this RFP are to be directed via e-mail to:

E-mail : itmg@gicofindia.com

Telephone: 022-22867124/116

Queries shall include, but are not limited to:

- a) Questions concerning this RFP: Questions must be submitted in writing via the email address provided and be received before the last date for receipt of Queries from Bidders as mentioned in section I under important dates.
- b) Errors and omissions in this RFP and enhancements: Bidders shall bring to notice of GIC Re any discrepancies, errors, or omissions that may exist within this RFP. With respect to this RFP, Bidders can recommend to GIC Re any enhancements that might be in the best interest of GIC Re. These recommendations must be submitted via e-mail and be received before the last date for receipt of Queries from Bidders as mentioned in section I under important dates.

GIC Re will make a good-faith effort to provide a written response to all queries. Written responses will be uploaded on GIC Re Website (<https://www.gicofindia.com>).

32.NON-CONFORMITIES BETWEEN FIGURES AND WORDS:

In the event, non-conformities/errors are observed in responsive Bids between the quoted prices in figures and in words, it shall be taken care of in the manner indicated below:

- a) If, in the price quoted, there is discrepancy between the unit price and total price (which is obtained by multiplying the unit price by the quantity), the unit price shall prevail, and the total price corrected accordingly.
- b) If there is an error in a total corresponding to the addition or subtraction of sub-totals, the sub-totals shall prevail, and the total shall be corrected; and
- c) If there is a discrepancy between words and figures, the amount in words shall prevail.
- d) Such a discrepancy in an offer shall be conveyed to the Bidder asking him to respond by a target date and if the Bidder does not agree to GIC Re's observation, the Bid shall be liable to be rejected.

33.NO AGENCY:

- a) The relationship between the Parties shall be that of independent contractor and contractee. Nothing in this RFP constitutes any fiduciary relationship between GIC Re and the selected Bidder/the selected Bidder's Team or any relationship of employer employee, principal and agent, or partnership or joint ventures, between GIC Re and the selected Bidder.
- b) Neither Party shall have any right or authority either express or implied to bind the other Party in any manner whatsoever except as agreed under the terms of any ensuing Agreement or to assume or create any obligation or responsibility on behalf of the other.
- c) GIC Re has no obligations to the selected Bidder or the selected Bidder's Team except as stated in this RFP.
- d) The selected Bidder shall comply with all laws, rules, and regulations applicable to the services being procured hereunder and all applicable laws, rules, and regulations to which it may be subject

from time to time.

- e) However, if due to any deeming fiction or if the law otherwise provides for a situation where GIC Re may be held vicariously or otherwise liable for acts of selected Bidder, the selected Bidder shall protect, indemnify and hold harmless GIC Re in respect of any losses, costs, damages whether direct or indirect arising out of the failure, omission or non-observance of any laws, rules or regulations which it was expected to comply with hereunder or any act of the selected Bidder which as a reasonable man, it should not have committed.

34.CONTRACT VARIATIONS

- a) The selected Bidder agrees that the requirements given in the RFP and the ensuing contract are broad requirements and are in no way exhaustive and guaranteed by GIC Re.
- b) GIC Re at any time by written Change Order may change the scope of work of this RFP and the ensuing contract, including the specifications, statement of work, number, and design criteria of any of the components thereof, delivery dates/timing of submission of reports, personnel inputs, timing of an activity or output.
- c) If any such change has cost or time implications for the selected Bidder, GIC shall adjust price and delivery schedules equitably through a further written Change Order, on the written request of the selected Bidder. The selected Bidder further understands and agrees that if any such change entails any reduction in the scope of work, then the cost and/or time benefits shall be passed on to GIC Re through a mutual Change Order in writing.
- d) The selected Bidder shall not make any change in the scope of work of this RFP and the ensuing contract without the prior written approval of GIC Re.
- e) The selected Bidder further understand and agree that any alteration, variation or addition in the scope of work necessitated by amendments and/or additions to any laws, rules or regulations before the time of award of the contract or during the currency of the contract shall not be considered a subject of a Change Order, provided that the nature of the mandate introduced by the law, rule or regulation is of such a nature that its non-inclusion, exclusion or alteration would render the subject matter of the procurement infructuous or expose GIC Re to the risk of non-compliance with applicable laws, rules or regulations.
- f) All such contract variations carried out via Change Orders shall be recorded in the form of an amendment to the SLA.
- g) Provided that any upward revisions and/or additions to the Scope of Work of this RFP, consequent to errors, omissions, ambiguities, discrepancies in the specification, etc., of the RFP which the selected Bidder had not brought to GIC Re's notice at the time of the Bids shall not constitute a Change Order and such upward revisions and/ or additions shall be carried out by the selected Bidder without any time and cost implications to GIC Re.

35.GOVERNING LAW AND JURISDICTION

- a) The validity, construction and performance of this RFP and the ensuing contract shall be governed by and construed in accordance with the laws of India.
- b) Subject to the provisions of the Arbitration clause, if any, contained in the ensuing contract, the Parties agree to submit to the exclusive jurisdiction of a court of competent jurisdiction at Mumbai, India and to comply with all requirements necessary to give such court the jurisdiction.

36.RIGHT TO AUDIT

GIC Re reserves the right to conduct an annual audit of the Selected Bidder's services to determine whether the activities are being performed as required by the RFP and as agreed in the contract.

37. ADHERENCE TO STATUTORY OBLIGATIONS/ COMPLIANCE WITH LAWS

The Selected Bidder shall adhere and comply with all the applicable laws of land and rules, regulations and guidelines prescribed by various regulatory, statutory and Government authorities of India.

38. NO LEGAL RELATIONSHIP

No binding legal relationship shall exist between any of the Bidders and the GIC Re until the execution of a Service Level Agreement.

39. CANCELLATION OF TENDER PROCESS

GIC Re reserves the right to reject any bid at its sole discretion at any stage without assigning any reason. GIC Re further reserves the right to cancel the tender process partly or fully at its sole discretion at any stage without assigning any reason to any of the participating Bidders. The GIC Re further reserves the right to re-issue or re-commence the entire bid process without the applicants having the right to object. Any decision of the GIC Re in this regard shall be final, conclusive, and binding on the Bidders.

40. VERIFICATION OF DOCUMENTS

Documents and/ or reports submitted by the Selected Bidder shall be verified as per Standard Operating Procedure (hereinafter referred to as 'SOP') dated 02-02-2016. Notwithstanding anything contained anywhere in this RFP or the ensuing Agreement, non-compliance as per SOP norms will result in termination of contract or imposition of appropriate liquidated damages for any penalties imposed on / damages suffered by GIC Re, either pecuniary or otherwise. The said SOP can be downloaded from the website of GIC Re.

ANNEXURE I E-TENDER PROCESS

1. Bidder Registration:

- a) This RFP (non-transferable) covering eligibility requirements, technical specifications, terms & conditions and other relevant information/data or documents required may be obtained by interested and eligible prospective Bidders by downloading from the GIC Re website i.e., <https://www.gicofindia.com> and CPPP Portal from **22nd March 2022**.
- b) Bidders are required to enroll on GIC Re e-Procurement portal by <https://gicre.eproc.in>. Enrolment on the GIC Re e-Procurement portal is free of charge.
- c) During enrolment / registration, the Bidders should provide the correct/true information including valid email-id & mobile no. All the correspondence shall be made directly with the/ Bidders through email-id provided.
- d) As part of the enrolment process, the Bidders will be required to choose a unique username and assign a password for their accounts.
- e) For e-tendering process, Bidder should possess valid Digital Signature Certificate (Class III Certificates with signing & encryption copy) which can be obtained from M/s Sify Technologies Ltd./ TCS/ nCode/eMudra or any Certifying Authority recognized by CCA India on eToken Smart Card.
- f) Upon enrolment on GIC Re e-Procurement portal for e-tendering, the Bidders shall register their valid Digital Signature Certificate (DSC) with their profile.
- g) Only one valid DSC should be registered by a Bidder. Bidders are responsible to ensure that they do not lend their DSCs to others which may lead to misuse and should ensure safety of the same.
- h) Bidders can then log into the site through the secured login by entering their user ID password and the password of the DSC / eToken.

Note: Those Bidders who have already enrolled in the e-Procurement portal are not required to follow step 1.

2. Preparation of Bids by Registered Bidders:

- a) For preparation of bid Bidders shall search the RFP from published RFP list available on web site and download the complete e-tender document and should consider corrigendum if any published before submitting their bids.
- b) Any clarifications, if required, may be obtained through the contact details given under Section II point 19(k).
- c) Bidders should keep the bid documents ready in advance that are needed to be submitted as indicated in the RFP document in PDF format only.
- d) Bidder shall go through the RFP carefully to understand the documents required to be submitted as part of the bid. Any deviation from the terms and conditions of the RFP may lead to rejection of the bid.

3. Submission of Bids by Bidders:

- a) Bidder should log into the site well in advance for bid submission so that he/ she uploads the bid in time i.e., on or before the bid submission time.
- b) Bidder should deposit the EMD as per the instructions specified in the RFP on or before the last date & time mentioned in the RFP, otherwise the uploaded bid will be rejected. The Bidders claiming exemption as a MSME/NSIC registered unit shall upload the scanned copy of valid MSME/NSIC registration confirming as manufacturer of e-tendered item.
- c) While submitting the bids online, the Bidder shall read the terms & conditions of RFP and accept the same to proceed further to submit his/her bid.
- d) Bidder shall digitally sign and upload the required bid documents one by one as indicated in the RFP according to specified cover.

- e) Bidders shall note that the very act of using DSC for downloading the RFP and uploading their offers is deemed to be a confirmation that they have read all sections and pages of the RFP without any exception and have understood the complete RFP and are clear about the requirements of the RFP.
- f) Bidders shall submit their bids through online e-tendering system to the Competent Authority well before the bid submission end date and time (as per Server System Clock). The Competent Authority will not be held responsible for any sort of delay, or the difficulties faced during the submission of bids online by the Bidders.
- g) Bidder should follow the server time being displayed on Bidder's dashboard at the top of the e-tender site, which shall be considered valid for all actions of requesting, bid submission, bid opening, etc. in the e-tender system.

ANNEXURE II PRE-QUALIFICATION CRITERIA

GIC Re will evaluate proposals, and select the Bidder based on following criteria:

#	Criteria	Documents to be provided
1	The Bidder should be a company registered under the Companies Act, 1956/ 2013.	Certificate of Incorporation
2	The Bidder should have had an average annual turnover of Rs. 50 Crores in the last three financial years i.e., 2018-19, 2019-20 & 2020-21 from Data center services. This must be the individual company turnover and not that of any group of companies.	Copy of Audited Balance sheet for the financial years i.e., 2018-19, 2019-20 & 2020-21 should be submitted.
3	The Bidder should have positive Net Worth as per the last audited financial report.	Copy of Audited Balance sheet for the financial years i.e., 2018-19, 2019-20 & 2020-21 should be submitted.
4	The bidder should have earned profit in at least 2 of the last 3 audited financial years (2018-19, 2019-20 & 2020-21).	Audited annual account or auditor certificate should be submitted.
5	The Bidder should be an established Data Center Services provider and should have been in the business of Co-location and managed-Hosting services and Managing DCs for a period of at least 5 years as on 31.03.2021.	Work Orders confirming year and area of activity, or Memorandum and Articles of Association.
6	a) The Bidder should have provided DC or DR Managed or co-hosting facility to at least 5 Companies at their DC sites in India. b) The Bidder should have at least 1 operational Government Community Cloud client from Central/ State/ PSU departments during the time of bid submission. c) The Bidder must have experience of providing DC or DR Managed or co-hosting facility in their data center for at least 2 clients from any Central Govt/ State Govt/ Semi-Govt/ PSU organization.	Copy of work/ purchase orders or client certificates.
7	a) The Bidder's Data Center must have at least 3 customers hosting SAP primary or DR landscapes. b) The Bidder should also have hosted SAP HANA-certified solution for at least 1 customer.	Copy of Purchase orders.
8	The proposed DC & DR sites must be Tier III or Higher certified from uptime institute/ Rated 3 or higher certified from TIA 942.	Copy of certification from the bidder for the proposed DC & DR sites.
9	The proposed DC & DR sites must be certified for below: 1. ISO 27001 2. ISO 20000-1 3. IS 1893:1984	Copy of certification from the bidder for the proposed DC & DR sites.
10	The proposed DC & DR sites must be owned by the bidder. No Partnership/ Consortium bidding is allowed. In the case of leased premises, the unexpired lease period must be available for at least another 7 years from the date of the RFP.	Self-attested Proof of ownership. In the case of Lease, a copy of the Self-Attested Lease Agreement is to be submitted. Complete address of proposed sites to be provided.

11	Location of the facility and setup (Primary Data Center and Disaster Site): a) Primary Data Center setup location for Managed Hosting facility should be in Mumbai/ Navi Mumbai only. b) Disaster Recovery Site should be in a different seismic zone other than the Data Center within India.	Undertaking/ declaration on bidder letter head with the details of the proposed addresses of DC & DR duly attested, signed, and stamped to be submitted.
12	The Bidder must be empaneled with MEITY for GCC. The Bidder shall provide documents of evaluation by MEITY/ audit by STQC, and the bidder should be certified for hosting Government Community Cloud (GCC).	Bidder and proposed DC & DR sites must be listed and valid under GCC section in the Audit Status Tab in below link: https://www.meity.gov.in/content/gi-cloud-meghraj
13	The Bidder is required to enter into an Integrity Pact Agreement with GIC Re.	Bidders must download, dully fill, sign and submit the Integrity Pact Agreement from the 'Media-Downloads-Policies and Guidelines' link on the below website: https://www.gicofindia.com
14	The Bidder should not have been blacklisted by any department or institution or undertaking of the Government of India and the Government of Maharashtra.	Declaration in this regard by the authorized signatory on behalf of the bidder on the company letter head. (As per Annexure IX)

Pre-Qualification Criteria Template (to be filled and submitted/ uploaded by Bidders):

1.	Name of Organization:		
2.	Address (including telephone numbers and email-id)		
3.	Name of the official in charge of this bid with phone / mob. Nos.		
4.	Type of organization: (Pvt. Ltd. / Public Ltd)		
5.	Year of establishment (Certificate of Incorporation attached) Ref.: Pre-qualification - 1	Yes <input type="checkbox"/>	No <input type="checkbox"/>
6.	Work Orders confirming year and area of activity and Memorandum and Articles of Association attached. Ref.: Pre-qualification - 5	Yes <input type="checkbox"/>	No <input type="checkbox"/>
7.	Client References. Hosting DC & DR for non-govt./ govt. clients and GCC (Copy of Work orders/ Client certificates) Ref.: Pre-qualification - 6	Yes <input type="checkbox"/>	No <input type="checkbox"/>
8.	Client References. Hosting SAP & SAP HANA primary or DR landscape (Copy of Purchase orders attached). Ref.: Pre-qualification - 7	Yes <input type="checkbox"/>	No <input type="checkbox"/>
9.	Whether ISO 20000-1 certified. (Copy of certification attached) Ref.: Pre-qualification – 9	Yes <input type="checkbox"/>	No <input type="checkbox"/>
10.	Whether ISO 27001 certified. (Copy of valid certificate attached) Ref.: Pre-qualification – 9	Yes <input type="checkbox"/>	No <input type="checkbox"/>

11.	Whether IS 1893:1984 certified. (Copy of valid certificate attached) Ref.: Pre-qualification – 9	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
12.	Average annual turnover during the last three financial years Ref.: Pre-qualification - 2 & 3 (To be supported by auditor's Certificate)		Year 1	Year 2
		Turnover		
		PAT		
13.	Certified Professionals (Please specify other certifications, if any) Ref.: Pre-qualification – 8	Certification	No of employees	
		CDCP		
		PMP		
		CBCP		
		BCCE		
14.	Whether bidder has been declared ineligible for corrupt practices or blacklisted with any Govt. Agencies. (Self-Declaration as per <u>Annexure IX</u> attached) Ref.: Pre-qualification - 14	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
15.	Whether the bidder has the following certifications. Ref.: Pre-qualification – 8	TIA 942	Yes <input type="checkbox"/>	No <input type="checkbox"/>
		ASHRAE	Yes <input type="checkbox"/>	No <input type="checkbox"/>
16.	Whether bidder has own carrier neutral DC built and operated complying with Tier III or higher standards. Ref.: Pre-qualification - 8	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
17.	The Bidder should be same for both DC and DR site. Bidding by a consortium in this regard is not allowed. (Self-attested proof of ownership or lease with address of proposed sites) Ref.: Pre-qualification – 10	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
18.	Data Center Locations (other than Mumbai) Ref.: Pre-qualification - 11	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
19.	Relevant and adequate details of the Security arrangements at the Data Center location and Managed Hosting facility (Primary and Disaster Recovery Site) to be provided Ref.: Pre-qualification - 8	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
20.	Relevant and adequate details of the power supply and electricity arrangements to be provided for both Primary and Disaster Site. Ref.: Pre-qualification - 8	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
21.	Whether bidder is OEM / Partner of OEM for Hardware proposed.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
22.	Whether bidder has submitted Integrity Pact.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

	Ref.: Pre-qualification - 13		
23.	Whether Bidder provides SLA of 99.99% uptime for Managed hosting services	Yes <input type="checkbox"/>	No <input type="checkbox"/>
24.	Details of previous job, if any, done for GIC Re		

Declaration:

- 1) All the information provided by me/us herein above is correct
- 2) I/We have no objection if enquiries are made about the work listed by me/us in the accompanying sheets/annexure.
- 3) I/We have read all the terms and condition of bid and the instructions, and these are acceptable to me/us.

Signature:

Name & Designation of the Authorized Signatory:

Official Seal:

Date:

Place:

Note for Bidders:

- Bidders must provide supporting documents for all the pre-qualification criteria listed above. Bids which do not pre-qualify based on the above criteria will be summarily rejected.
- The documents, as listed above, must be of the same Bidder.
- On request, original documents should be produced failing which the bid is liable for rejection.
- GIC Re will evaluate the documents submitted to decide if the Bidder pre-qualifies. Mere submission of documents will not pre-qualify any Bidder.
- Bidders must upload above documents online as per **Annexure II**. All undertaking shall be duly signed and Stamped by Authorized signatory of the Bidder Firm.
- Bidders must submit Integrity Pact Agreement signed by the authorized representative of the Bidder with office seal on a non-judicial stamp paper of INR 100/-. The Agreement will be counter-signed for and on behalf of GIC Re after opening of the pre-qualification and technical bids of the e-tender.
- The Selected Bidder is required to sign agreements and submit the same to GIC Re (Non - Disclosure Agreement, Service Level Agreement, Deed of Indemnity, Performance Bank Guarantee).

ANNEXURE III TECHNICAL BID EVALUATION

A Bidder Experience & Expertise Rating			
#	Parameter	Description	Max Score
1	Experience in DC services	Experience of the bidder in providing Data Center services with requirements like SOW of this RFP and including managed hosting services to large clients. Specific experience in managing or hosting mission critical applications or SAP/ SAP HANA application landscape.	20
2	Testimonials from Customers	Testimonials on Satisfactory Service from at least 5 Customers/ Clients are to be provided. Marks will be given based on: <ul style="list-style-type: none"> customer satisfaction level penalties invoked for failure to meet RPO / RTO ability to meet change in resources/ requirements on time and satisfactorily. GIC Re will contact the customers/ clients to ascertain the above parameters. Client contact details must be provided.	20
3	Data Center infrastructure	Size in terms of number of Data Centers, total sq. ft. of area, number of clients whose applications are being hosted, Number of years of operation in India etc.	10
4	Robustness of existing Data Center and Disaster Recovery site infrastructure	Robustness of the Data Center in terms of building management system, security operations center, network operations center, electrical room, raised flooring, power backup, smoke detection, fire detection & suppression, precision air-conditioning, false ceiling, video surveillance systems, access logs, dedicated security personnel, biometric secured access to personnel and clients, percentage uptime etc.	10
5	Bill of material (BOM) provided for Complete setup	Sizing and price of current setup as per <u>Annexures XIII & XIV</u> including licenses and services and rate cards.	10
6	Qualification and competence of Key Staff.	Consultants with specialized skills and access to technologies related to assignment. Details of resources to be associated with this project must be provided.	10
7	Project plan	<ul style="list-style-type: none"> Proposed solution approach and Work Plan Implementation Methodology. PERT Chart must be provided. Detailed BOM with Complete Sizing considerations for GCC, Oracle, SAP HANA, SD-WAN (NOC) & MSS (SOC), etc., components must be provided. Additional value propositions. 	20
TOTAL			100

DC-DR Site Rating			
B			
#	Parameters	Bidders Response (Y/N)	Bidders Comments/ Details of Proof attached.
1	The facility should be either owned by bidder or on lease with unexpired lease duration of 7 years as on date of RFP.		
	a) Owned/ Leased but exclusive Data Centre building		
	b) Owned/ Leased but shared with multiple tenants		
	c) The bidder to submit Annexure II along with documents.		
2	Age of Building		
	a) Less than 10 years		
	b) More than 10 years		
3	The Data Centre facility building should be away from hazardous chemical materials, LPG storage areas, chemical go-downs and other storage facilities meant for dangerous commodities.		
4	The proposed Data Center building should not be in low lying and flood/ natural disaster-prone areas.		
5	The structural strength of the proposed building should have been certified and latest report to be available. The report should not be more than one year old. (Copy of report/ certificate to be attached)		
6	The proposed building should be covered under comprehensive insurance on ongoing basis including risk related to earthquake, floods, fire, lightning, terrorist attacks etc. (Copy of last year and current year insurance report to be attached.) (Yes/ No)		
7	The bidder proposed site should have following compliance/ certifications: (Copy of the relevant certifications for proposed sites)		
	a) NFPA 70 & 75		
	b) IS 1893:1984 seismic Compliance		
	c) TIA 942 compliance		
	d) PCI DSS		
	e) ISO 20000 & 27001		
	f) ISO 9001		
8	g) Compliance to ASHRAE Standards		
	The bidder to provide space with CCTV cameras, smoke & fire detectors, etc., in both DC & DR sites.		
9	Freight Lift - The data center should have high-capacity freight lift for ease of movement of servers and high-density network devices.		
10	The doors for the server room, communications room, and other critical areas should be fire rated for minimum 2 hours.		
11	The server room area should have a raised floor height of minimum 2ft.		
12	The server hall height from raised floor to false ceiling should be at least 10ft.		
13	The false flooring in server hall should be fire resistant and tiles should be made up of Calcium Silicate/ anti-static material.		
14	The Data Centre Site/ server hall area must have microprocessor-based system to detect water leakage.		

15	The Data Centre site should have electronic rodent control systems with operability on varied frequency range.		
16	All the Building Management system (BMS) activities are to be controlled centrally in a room specifically to be used for BMS activities. The bidder should manage the BMS activities on a 24*7*365 basis.		
17	There should be sufficient power backups in place for running the Building Monitoring system in the event of power outage.		
18	Each component of data center must allow concurrent maintenance without disruption to supply of services to data halls or support areas.		
19	The Data Centre should have load bearing capacity of 1000Kg/ Sq. m.		
20	Two independent power suppliers/ substations/ Grid Level redundancy each capable of supporting the site independently, in line with Tier 3 or above certification requirements. (Details of power arrangement to be submitted)		
21	The incoming supplies from alternate power suppliers/ sub-stations must be arranged as at least N+1, each entering the site from diverse paths, and each terminated in separate fire- resistant enclosures. Whether the utility power enter the site via overhead or underground conduits and/or ducts? (Details to be submitted)		
22	Diesel Tanks (for generators) - The data center should have high-capacity diesel tanks for ensuring 48-hour power backup with contracts for fuel supply on demand.		
23	Generators should be capable of providing power for 48 hours or continuously even during refilling.		
24	The entire failover mechanism to DG should be automatic, with power supply from the transformer as the primary source and automatic switchover to DG set as a secondary source without any disruption.		
25	Comprehensive Power Audit in the last two years/ Record of past incidents.		
26	The design for cooling infrastructure at the data center should be in lines with standard guidelines to support high density cooling needs.		
27	Redundant CRAC/ cooling units to facilitate High density cooling needs.		
28	The bidder should be able to provide Auto Transfer Switch (ATS) for single power input systems.		
29	Biometric Access to the common entry to the Server room/ Server Hall area should be available.		
30	The offered space should not be on top floor or ground Floor.		
31	a) Physical Security: i) Security guards should be deployed on a 24*7*365 basis. ii) Security guards should be deployed to screen visitors at the entry to the premises. iii) Security guards to be deployed at the entry of server rooms, to check the identity of the persons visiting the server rooms and make entry of the details of the visitor in register.		
	b) Bidder Employees & other customers: i) Visitors must declare the laptop and any storage device they are carrying to restricted areas (e.g., Data Center, Server rooms, etc.). These details must be verified at the time of exit. ii) Bidder employees must always carry photo identity cards. iii) Visitors must be classified according to the function they perform.		

	iv) Prior permission must be sought for visits by any Customer officials/ Auditors. Visitor badge must be provided. v) Separate registers for each customers/ vendor must be placed to note the movement of their employees. Visitors' sign-in registers must be placed and reviewed daily. vi) A list of bidder employees, authorized to enter the server room, must be placed with the security personnel manning the floor housing the server room.		
	c) Material Movement: i) Incoming/ outgoing packages must be inspected to prevent unauthorized movement of materials. ii) Incoming/ outgoing hardware must require disclosure and approved security clearance (gate pass).		
	d) The server room should have access control mechanisms like numeric pads, swipe cards, biometric, etc. to enable access.		
32	The server room area entrance and exit should be accessible using the proximity card (access control) with biometric access.		
33	The racks in server room area must be of 42U size with horizontal and vertical cable managers and the bidder to provide inter-rack cabling using patch panels, cross connects to communication area, cable managers for structured cabling, redundant power strips, earthing for each rack etc.		
34	The bidder should be able to provide space in the same server hall contiguous to the proposed area for scaling up, at the contracted rate during the period of contract.		
35	UPS must be configured in redundant mode i.e., N+1 (at least). (Details of UPS arrangement to be submitted)		
36	Two separate power paths from the UPS to be provided to the server/ network communication room.		
37	The proposed server area must be well covered in the smoke & fire detection and suppression system using systems like VESDA, FM 200/FE 227, NOVEC 1230, etc.		
38	There must be CCTV monitoring for surveillance of the server hall area. The CCTV surveillance should cover GIC Re's & GCC Server/ Rack area and other critical areas. The CCTV cameras should cover in row view of both front & back side of the racks row, within GIC Re's server area. The CCTV camera should cover the entry & exit to the GCC server area.		
39	The temperature in the server hall should be maintained at 21 +/- 2-degree C.		
40	The humidity at the data center should be maintained at 50 % +/- 5% RH.		
41	Availability of 3 phase, 4 wire power system in sever hall area.		
42	The Server room area must be provided with Water Leak detection system and fire alarm system.		
43	Air Quality in the data center site must be of severity level G1 (mild) as per ISA - 71.04.		
44	Activities to be recorded, logs and the archival should be kept for at least 90 days: a) CCTV recording kept for more than 3 months b) CCTV recording kept for less than 3 months		
45	The bidder must be able to share the video monitoring data in case required by GIC Re.		

46	Entry & Exit to DC and server rooms must be restricted and monitored and must also be in CCTV surveillance coverage.		
47	Telecom junction box, multiplexers of various service providers: at least Bharti, Tata, Sify, BSNL/MTNL, Reliance, etc., to be available in and around the building. Details of service providers whose MUXs are available at site(s) to be submitted.		
48	The Bidder must provide redundant telecom links for GIC Re's network and extend the links terminated by the link service provider on the junction box till the server room where GIC Re's setup will be located.		
49	Bidder must ensure fibers from multiple providers are fed to the site from three independent channels in ring connectivity.		
50	99.99% Uptime on monthly basis is required for the bidder Data center.		
51	Audit reports of proposed DC & DR sites must be available as and when required by GIC Re.		
52	Bidder shall provide and perform all cabling required for GIC Re's Hybrid Cloud Infrastructure to be hosted in the Data Centre.		
53	Bidder shall cover the entire Scope of Work in their bid submission and presentation.		
54	The bidder should provide staging/ storage area for at least four to six weeks for any material.		
55	Staging area should be preferably close to the server rooms and have all facilities like, redundant power, LAN connectivity, telecom, etc.		
	a) Staging area in same floor		
	b) Staging area in different floor		
56	The bidder should provide off-site drop off and pickup facility for backup tapes/ disks, if required.		
57	Critical Services like power, UPS, Genset etc. are managed by:		
	a) Own dedicated staff of the bidder		
	b) These maintenance services are Outsourced to third party		
58	The proposed Data Center should have multi layers of physical security:		
	a) Site Perimeter (Public Zone)		
	b) Perimeter Security (Reception Zone)		
	c) Facility control (Operating Zone)		
	d) Server Hall (high security Zone)		
	e) Details of security arrangements in the Data Center to be submitted.		

C	Presentation by Bidders		
#	Evaluation of Bidders Presentation		Marks
1	Project organization, Project plan & Execution Methodology		15
2	Understanding of Scope of work.		15
3	Articulation of migration strategy		15
4	Risk Mitigation Plan.		5
	Total		50

D	Client Reference					
#	Organization	Name of Person	Contact Details			
			Designation	Landline No.	Mobile No	Mail id
1						

2						
3						

E	Scheme of Marks/ Technical Score (TS) Calculation	
#	Technical proposal Evaluation	Maximum Score
1	Bidder Experience & Expertise Rating	100
2	Technical Bid Compliance as in <u>Annexure XV</u> .	150
3	DC-DR site Rating	200
4	Presentation by Bidders	50
Total (Marks out of 500)		500
TS for each Bidder (Marks out of 500*100)/500		

- Technical Bids receiving **Technical Score (TS)** greater than or equal to a score of **75** (cut-off marks) will be eligible for consideration in the subsequent round of commercial evaluation.
- Any other information that will facilitate GIC Re's evaluation of the Bidder's capability to successfully implement & manage the project must be provided.
- Bidders shall identify what they believe are the primary characteristics that differentiate them from others in the market and explain why they believe they are uniquely positioned to work successfully with GIC Re. In this context, describe any experience in working with Insurance or Reinsurance organizations, Financial Institutions, or other entities.

ANNEXURE IV COMMERCIAL BID

RFP for Hosting and Management of GIC Re Hybrid Cloud Infrastructure

Commercial Bid Submission:

- 1) Bidders shall submit the commercial bids in the below mentioned tabular formats.
- 2) Bidders shall submit detailed Bill of Materials (BOM) with proper sizing for GCC, Oracle, SAP HANA, SD-WAN (NOC) & MSS (SOC), etc., components as part of their Technical Bid Evaluation Submission (**Annexure III**).
- 3) Bidders may add more rows, for other components, as required, in the same format.
- 4) Qty provided is for current setup size as per **Annexure XIII**, proposed HANA Setup as per **Annexure XIV**, proposed SD-WAN setup as per **Annexure XII** and proposed MSS/ SOC Components as per **Table T.4 in Clause 5 of Section I**.
- 5) Backup size for current setup (**Annexure XIII**) provided. Bidder must size and quote for GCC, HANA, etc.
- 6) Bidders must size suitably for the missing quantities.
- 7) The columns for Unit Price from Tables B to I will be used by GIC Re as rate card for commissioning/ addition or decommissioning/ removal of components for future needs. These prices will be fixed for the entire Contract Period and GIC Re shall proportionally adjust payments whenever one or more components are added or deleted from the Setup.
- 8) The quoted price shall be in Indian Rupees ₹ (INR). Payment shall be made as per **Section II Clause 21**.
- 9) Bidders shall quote only the base price exclusive of applicable taxes like Goods & Services Tax (GST). GST as applicable will be paid additionally on actuals. GIC Re will be entitled to deduct TDS as applicable while making payments according to the Indian taxation rules. There shall be no escalation in the prices once the prices are fixed and agreed to by GIC Re and the Selected Bidder.
- 10) No payment of incidental expenses during execution of the ensuing contract will be demanded by Selected Bidder.
- 11) Kindly note that words like 'Nil', 'to be discussed', 'as applicable', etc. will not be considered and the bid shall be treated as unresponsive. Such bids are liable to be cancelled.
- 12) The **L1 Bidder** will be selected based on **Grand Total = A+B+C+D+E+F+G+H+I**. This Grand Total shall be referred to as **Contract Price/ Commercial Bid Value** and must be represented in figures as well as in words.

A One Time Charges (OTC)			
#	Cost Component	Description	Cost (₹)
1	GCC	Implementation/ Deployment of GCC Infrastructure at DC	
		Implementation/ Deployment of GCC Infrastructure at DR	
2	Oracle Servers	Implementation/ Deployment of Oracle Private Cloud Infrastructure at DC	
		Implementation/ Deployment of Oracle Private Cloud Infrastructure at DR	
3	SAP HANA Cloud	Implementation/ Deployment of SAP HANA Infrastructure at DC	
		Implementation/ Deployment of SAP HANA Infrastructure at DR	
4	SD-WAN	Implementation/ Deployment of SD-WAN with MPLS & ILL	
5	Backup, NOC, etc.	Implementation/ Deployment of NOC, Backup, etc., at DC & DR	
6	MSS & SOC	Implementation/ Deployment of SOC & MSS Solution at DC & DR	
7	Migration	Migration of VM, Servers, data, existing backups, etc.	
TOTAL (A)			

B	1	Storage and Backup at DC					
#	Element	Sub Type	Description	Qty (TB/GB) (X)	Unit Price (₹ per year) (Y)	Cost (₹ per year) (X*Y)	Cost for 5 Years (₹)
1	Storage	All Flash	Storage for VMs on GCC	80 TB			
2	Storage	All Flash	Storage for Oracle Private/ Physical Servers (2)	4 TB			
3	Storage	All Flash	Storage for SAP HANA Cloud (21)	18 TB			
4	Backup	Resilient	Backup (primary) (current size without HANA)	30 TB			
5	Storage	Resilient	Storage for secondary/ offsite Backup	30 TB			
6	Storage	Normal	Logs and archives				
Sub Total (B.1)							
B	2	Storage and Backup at DR					
#	Element	Sub Type	Description	Qty (TB/GB) (X)	Unit Price (₹ per year) (Y)	Cost (₹ per year) (X*Y)	Cost for 5 Years (₹)
1	Storage	All Flash	Storage for VMs on GCC	10 TB			
2	Storage	All Flash	Storage for Oracle Private/ Physical Servers (1)	2 TB			
3	Storage	All Flash	Storage for SAP HANA Cloud (5)	5 TB			
4	Storage	Normal	Logs and archives				
Sub Total (B.2)							
TOTAL (B.1 + B.2 = B)							

C	1	CPU & RAM at DC					
#	Element	Sub Type	Description	Qty (TB/GB) (X)	Unit Price (₹ per year) (Y)	Cost (₹ per year) (X*Y)	Cost for 5 Years (₹)
1	CPU	GCC	Number of vCPUs for VMs	512			
2	CPU	Physical	Number of vCPUs/ CPUs for Oracle Servers (2)	16			
3	CPU	HANA	Number of vCPUs for SAP HANA Cloud (21)	648			
4	RAM	GCC	RAM Size for all VMs	3 TB			
5	RAM	Physical	RAM Size for Oracle Servers (2)	128 GB			
6	RAM	HANA	RAM Size for SAP HANA Cloud (21)	12 TB			
Sub Total (C.1)							
C	2	CPU and RAM at DR					
#	Element	Sub Type	Description	Qty (TB/GB/ Value) (X)	Unit Price (₹ per year) (Y)	Cost (₹ per year) (X*Y)	Cost for 5 Years (₹)
1	CPU	GCC	Number of vCPUs for VMs	90			

2	CPU	Physical	Number of CPU for Oracle Servers (1)	8			
3	CPU	HANA	Number of vCPUs for SAP HANA Cloud (5)	176			
4	RAM	GCC	RAM Size for all VMs	388 GB			
5	RAM	Physical	RAM Size for Oracle Servers (1)	64 GB			
6	RAM	HANA	RAM Size for SAP HANA Cloud (5)	3 TB			
Sub Total (C.2)							
TOTAL (C.1 + C.2 = C)							

D	1	OS, DB, Software and Licenses at DC					
#	Element	Sub Type	Description	Qty (X)	Unit Price (₹ per year) (Y)	Cost (₹ per year) (X*Y)	Cost for 5 Years (₹)
1	OS	RHEL	RHEL for GCC, Oracle Servers	20			
2	OS	RHEL	RHEL for SAP HANA	21			
3	OS	Windows	Windows Server OS	57			
4	DB	MSSQL	MSSQL Standard for VMs	8			
5	DB	Oracle	Oracle for 2 Physical Servers (Core Based)	2			
6	Replication	DRM	DC-DR Replication Tool for VMs, Servers, SAP HANA				
7	Monitoring	Tool	Monitoring Tool for Cloud, NOC, SOC, etc. with SMS				
8	Others	Others	Any other Software and/ or licenses for the setup				
Sub Total (D.1)							
D	2	OS, DB, Software and Licenses at DR					
#	Element	Sub Type	Description	Qty (X)	Unit Price (₹ per year) (Y)	Cost (₹ per year) (X*Y)	Cost for 5 Years (₹)
1	OS	RHEL	RHEL OS for GCC, Oracle Servers	7			
2	OS	RHEL	RHEL for SAP HANA	5			
3	OS	Windows	Windows Server OS	6			
4	DB	MSSQL	MSSQL Standard for VMs	1			
5	DB	Oracle	Oracle for 1 Physical Server (Core Based)	1			
6	Monitoring	Tool	Monitoring Tool for Cloud, NOC, SOC, etc. with SMS				
7	Others	Others	Any other Software and/ or licenses for the setup				
Sub Total (D.2)							
TOTAL (D.1 + D.2 = D)							

E	1	Management Elements at DC					
#	Element	Sub Type	Description	Qty (X)	Unit Price (₹ per year) (Y)	Cost (₹ per year) (X*Y)	Cost for 5 Years (₹)
1	OS	RHEL	RHEL OS Management for GCC, Oracle Servers	20			
2	OS	RHEL	RHEL for SAPHANA	21			
3	OS	Windows	Windows Server OS Management	57			
4	DB	MSSQL	MSSQL Management for VMs	8			
5	DB	Oracle	Oracle Management for SAP & non-SAP servers	18			
6	DB	HANA	SAP HANA DB Management	21			
7	App	AD/ DNS	Management of AD, DNS & JBOSS EAP for entire GIC Re	6			
8	NOC	SDWAN	Management of SDWAN and all Network Links				
9	SOC	MSS	Management of all Security Services				
10	Backup	Service	Management of Backup as a Service				
11	Storage	Service	Management of Storage for entire solution				
12	Others	Others	Management of Middleware, load balancer and other tools/ software				
Sub Total (E.1)							
E	2	Management Elements at DR					
#	Element	Sub Type	Description	Qty (X)	Unit Price (₹ per year) (Y)	Cost (₹ per year) (X*Y)	Cost for 5 Years (₹)
1	OS	RHEL	RHEL OS Management for GCC, Oracle Servers	7			
2	OS	RHEL	RHEL for SAPHANA	5			
3	OS	Windows	Windows Server OS Management	6			
4	DB	MSSQL	MSSQL Management for VMs	1			
5	DB	Oracle	Oracle Management for SAP & non-SAP servers	5			
6	DB	HANA	SAP HANA DB Management	5			
7	App	AD/ DNS	Management of AD, DNS & JBOSS for entire GIC Re	2			
8	Storage	Service	Management of Storage for entire solution				
9	DR Drill	Service	DR Drill Twice per annum	2			
10	Others	Others	Management of Middleware, load balancer and other tools/ software				
Sub Total (E.2)							

TOTAL (E.1 + E.2 = E)

F SD-WAN with MPLS, ILL & P2P									
Hub/ Spoke Locations	Destination	Bandwidth (Mbps)	Link Type	Qty (X)	CPE Count	CPE Make/ Model (with UTM, FW, etc.)	Unit Price (₹ per Mbps per year) (Y)	Cost (₹ per year) (X*Y)	Cost for 5 Years (₹)
Mumbai HO	DC	200	MPLS	2	2				
Mumbai HO	Internet	300	ILL	2	2				
Mumbai Oriental	DC	50	MPLS	2	2				
Mumbai Oriental	Internet	75	ILL	2	2				
Delhi	DC	20	MPLS	2	2				
Delhi	Internet	50	ILL	2	2				
GIFT City	DC	20	MPLS	2	2				
GIFT City	Internet	50	ILL	2	2				
DC	DR	80	P2P	2	2				
DC	Internet	100	ILL	2	2				
DR	Internet	50	ILL	1	1				
TOTAL (F)									

G Managed Security Services Sizing and Price					
#	Solution/ Tools	Qty/ Size/ Throughput/ License (X)	Unit Price (₹ per year) (Y)	Cost (₹ per year) (X*Y)	Cost for 5 Years (₹)
1	SIEM	3500 EPS			
2	SOAR	1			
3	IPS & IDS (Host & Network)				
4	NGFW (with UTM)	2			
5	PIM/ PAM	30			
6	Cloud WAF	4			
7	DLP (Network + Endpoints + Servers)	700			
8	Data Classification	700			
9	Web Proxy	600			
10	EDR (for Endpoints)	600			
11	Server Security (AV for Servers)	100			
12	Cloud Sandboxing				
13	Cloud DDoS	>1 Gbps			
14	Software VPN	50			
15	Site-to-Site IPSEC VPN (for KL & London)	2			
TOTAL (G)					

H	SASE ZTNA Solution Enterprise Defender Standard (EDS)				
#	Solution/ Tools	Qty/ Size/ Throughput/ License (X)	Unit Price (₹ per year) (Y)	Cost (₹ per year) (X*Y)	Cost for 5 Years (₹)
1	SASE ZTNA Solution Enterprise Defender Standard (License + AMC + Professional Services)	100			
TOTAL (H)					

I	Miscellaneous				
#	Solution/ Tools	Qty/ Size/ Throughput/ License (X)	Unit Price (₹ per year) (Y)	Cost (₹ per year) (X*Y)	Cost for 5 Years (₹)
1	Any other component/ sub- component that is/ may be required				
TOTAL (I)					

GRAND TOTAL = Sum of cost for 5 years = A + B + C + D + E + F + G + H + I

Authorized Signatory:

Name & Designation of the Authorized Signatory:

Office Seal with date:

Place:

ANNEXURE V
SERVICE LEVEL AGREEMENT

(To be typed on stamp paper worth ₹500/-)

This Service Level Agreement (“Agreement”) is made and entered into on this _____ day of
2022

BY AND BETWEEN

General Insurance Corporation of India, incorporated, under the Companies Act, 1956 having its registered office at Suraksha, 170, J. Tata Road, Churchgate, Mumbai- 400020 (hereinafter referred to as "GIC Re"), which expression shall, unless it be repugnant to the meaning and context thereof, include its successors and permitted assigns of the one part.

AND

_____, a Company incorporated under the **Companies Act, 1956/2013** having its registered office at _____, (hereinafter referred to as "Selected Bidder"), which expression shall, unless it be repugnant to the meaning and context thereof, include its successors, and permitted assigns of the other part.

Both of which are individually referred to herein as ‘a Party’ and collectively as ‘the Parties’

RECITALS

WHEREAS GIC Re is desirous of appointing a Selected Bidder for **“RFP for Hosting and Management of GIC Re Hybrid Cloud Infrastructure”** conforming to all the specifications as per the Request for proposal No. **GICRE/ITMG/RFP/05/2021-22** dated **22nd March 2022** (hereinafter referred to as “RFP” which expression shall include all attachments and annexures thereto as well as all amendments, modifications, alterations, addendums, and corrigendum thereto).

AND WHEREAS GIC Re has called for bids from eligible Bidders pursuant to the RFP.

AND WHEREAS the Selected Bidder represents that it has the necessary resources and experience for providing **“Hosting and Management of GIC Re Hybrid Cloud Infrastructure”** and has submitted its Bid for providing the required services in accordance with the terms and conditions set forth hereinand, in the RFP, and any other reasonable requirements of GIC Re communicated from time to time.

AND WHEREAS the Selected Bidder has submitted its technical and commercial bid during thee-tenderingprocess which has been considered as appropriate by GIC Re based on the documents submitted by the Selected Bidder.

AND WHEREAS GIC Re has accepted the bid of the Selected Bidder based on the documents submitted by it under the tendering process and has issued Purchase Order No. _____ Dated _____.

Now in consideration of the promises and covenants contained in this Agreement, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged it is hereby agreed to, by and between the Parties as under:

1. DEFINITIONS

In this Agreement, the following terms shall be interpreted as follows:

- a) “Confidential Information” will have the same definition as given in the Reciprocal Non-Disclosure Agreement (NDA) entered between GIC Re and the Selected Bidder.
- b) “Agreement” means the Agreement entered between GIC Re and the “Selected Bidder” as recorded in this Contract form signed by GIC Re and the “Selected Bidder” including all Attachments and Annexes thereto, the RFP, the agreed terms as set out in the technical and commercial Bids, all documents incorporated by reference therein and amendments, alterations and modifications done to any of the above from time to time.
- c) “Document” means any embodiment of any text or image however recorded and includes any data, text, images, sound, voice, codes and databases or microfilm or computer-generated microfilm.
- d) “Effective Date” means the date of issuance of Purchase Order by GIC Re to the Selected Bidder.
- e) “Contract Period” means Implementation & Migration period/ phase plus period of Five (5) years from the date of Go-Live declared by GIC Re.
- f) “Intellectual Property Rights” means any patent or patent applications, copyright, trademark, trade name, logo, sign symbol, business name, internet domain names, email address names, design, trade secret, permit, service marks, brands, propriety information, moral rights, knowledge, technology, licenses, databases, computer programs, software, know how, rights in confidential information, rights in invention or other form of intellectual property right, title, benefits or interest, whether registered or unregistered and including any form of application for any of the foregoing which may already exist or may be created anywhere in the world, whether arising before or after the execution of this Agreement and the right to ownership and registration of these rights;
- g) “Kick Off Meeting” means a meeting convened by GIC Re to discuss and finalize the work execution plan and procedures with the Selected Bidder.
- h) “Selected Bidder’s team” means the employees of the Selected Bidder, its authorized agents and representatives or other personnel employed or engaged either directly or indirectly by the Selected Bidder for the purposes of implementation of this Agreement.
- i) “Negligence” means: any act or failure to act (whether sole, joint, or concurrent) by a person or entity which was intended to cause, or which was in reckless disregard of or wanton indifference to, avoidable and harmful consequences which such person or entity knew or should have known or with reasonable diligence could have known to result from such act or failure to act. Notwithstanding the foregoing, negligence shall not include any action taken in good faith for the safeguard of life or property,
- j) “Willful Misconduct” means: “intentional disregard of good and prudent standards of performance or proper conduct under this Agreement with knowledge that it is likely to result in any injury to any person or persons or loss or damage of property.
- k) “Parties” means GIC Re and the Selected Bidder and “Party” means either of the Parties.
- l) “Service” means facilities/services to be provided as per the requirements specified in the RFP and this Agreement and any other incidental services, such as Supply, maintenance, provision of technical assistance and other such obligations of the Selected Bidder covered under this Agreement.
- m) “Service Specification” means and includes detailed descriptions, statements to technical data, performance characteristics, and standards as applicable and as specified in this Agreement or the RFP as well as those specifications relating to Industry standards and codes applicable to the performance of the work, work performance quality and the specifications affecting the works or any additional specification required to be produced by the Selected Bidder to meet the design criteria or completion of the Services.
- n) “The Contract Price” means the price payable to the Selected Bidder under the Agreement for the full and proper performance of its contractual obligations on its part.
- o) “Bids” means the technical and commercial bids submitted by the Selected Bidder in response

to the RFP.

- p) “AMC” means Comprehensive Annual Maintenance Contract between Service Provider and GIC Re.

2. **INTERPRETATION**

In this Agreement unless a contrary intention is evident

- a) the Clause headings are for convenient reference only and may not be used for interpretation.
- b) unless otherwise specified a reference to a clause number is a reference to all its sub-clauses.
- c) unless otherwise specified a reference to a clause or sub-clause is a reference to the clause or sub-clause of this Agreement including any amendments or modifications to the same from time to time.
- d) a word in the singular includes the plural and a word in the plural includes the singular.
- e) a word importing a gender includes any other gender.
- f) a reference to a person includes a partnership and a body corporate.
- g) a reference to legislation includes legislation repealing, replacing, or amending that legislation.
- h) where a word or phrase is given a particular meaning, it includes the appropriate grammatical forms of that word or phrase which have corresponding meanings.
- i) in the event of an inconsistency or conflict between the terms of this Agreement, the RFP and the Bid, the terms of the RFP shall prevail over and supersede the Bids to the extent of the terms mentioned in the RFP but not on the terms modified under this Agreement. Any changes to the terms of the RFP and/or any additions thereto made in this Agreement shall prevail over and supersede the RFP. In the absence of any inconsistencies, the RFP shall bind the Parties in addition to terms and conditions of this Agreement.
- j) The rule of construction that the contract shall be interpreted against the Party responsible for the drafting or preparation of the contract, shall not apply.
- k) The expiration or termination of this Agreement shall not affect such of the provisions of this Agreement as expressly provide that they will operate after any such expiration or termination or which of necessity must continue to have effect after such expiration or termination, notwithstanding that the clauses themselves do not expressly provide for this.

3. **CONDITIONS PRECEDENT**

This Agreement is subject to the fulfillment of the following conditions precedent by the Selected Bidder.

- a) The Selected Bidder shall at his own expense deposit with GIC Re within 14 days from the receipt of notification of award of the contract from GIC Re, an unconditional, irrevocable, and continuing Performance Bank Guarantee (PBG) from a scheduled commercial bank acceptable to GIC Re, payable on demand, for the due performance and fulfillment of this Agreement. The PBG shall be denominated in the currency of India, INR and shall be in the form of a Bank Guarantee Bond. The PBG shall be valid for a period of **60 days** beyond the date of completion of all contractual obligations including warranty obligations, renewable as may be stipulated by GIC Re.

The PBG amount shall be INR _____/- (3% of the Contract Price/ Commercial Bid Value) and PBG shall be in the format attached as **Annexure VI** to the RFP. All charges whatsoever such as premium, commission, etc., with respect to the PBG shall be borne by the Selected Bidder.

No interest shall be payable on the PBG.

In the event of the Selected Bidder being unable to service this Agreement for whatever reason or any PBG owing to such invocation, the successful Bidder shall forthwith replenish/restore the PBG to its original value.

Notwithstanding and without prejudice to any rights whatsoever of GIC Re under this Agreement, the proceeds of the PBG shall be payable to it as compensation for any loss resulting from the Selected Bidder's failure to complete its obligations under this Agreement.

- b) The Selected Bidder shall obtain all statutory, regulatory, and other approvals required for the performance of the Services under this Agreement.
- c) The Selected Bidder shall execute an Integrity Pact with GIC Re which essentially envisages an agreement committing Officials/Representatives of the Parties to this Agreement (covered in terms of the threshold limit set by GIC Re), not to exercise any corrupt influence on any aspect of this Agreement.
- d) The Selected Bidder shall furnish a Deed of Indemnity in the format attached as **Annexure VIII** with the RFP.
- e) The Selected Bidder shall furnish the Code of Integrity undertaking in the format attached as **Annexure X** with the RFP.
- f) The Selected Bidder shall sign the Non-Disclosure Agreement (NDA) in the format attached as **Annexure VII** with the RFP.
- g) GIC Re reserves the right to waive any or all the conditions specified in this clause in writing and no such waiver shall affect or impair any right, power, or remedy that GIC Re may otherwise have.

4. VERIFICATION OF DOCUMENTS

Documents and/or reports submitted by the Selected Bidder shall be verified as per Standard Operating Procedure (hereinafter referred to as 'SOP') as well as SOP for GIC Re ITMG Procurement Guidelines. Notwithstanding anything contained anywhere in this Agreement, non-compliance as per SOP norms will result in termination of the Agreement or imposition of appropriate liquidated damages for any penalties imposed on / damages suffered by GIC Re, either pecuniary or otherwise. The said SOPs can be downloaded from the website of GIC Re.

5. REPRESENTATIONS & WARRANTIES

The Selected Bidder hereby represents and warrants as of the date hereof, which representations and warranties shall survive the term, expiration and termination hereof, the following:

- a) That the Selected Bidder is a validly organized entity and has the requisite experience of, the technical know-how, the professional skills the financial wherewithal for providing **RFP for Hosting and Management of GIC Re Hybrid Cloud Infrastructure** and has the ability, the power and the authority that would be required to successfully provide the Services sought by GIC Re for the purposes of this Agreement.
- b) That the Selected Bidder is not involved in any litigation or legal proceedings, pending, existing, and potential or threatened, that may have an impact of affecting or compromising the performance or delivery of Services under this Agreement.
- c) That the representations and warranties made by the Selected Bidder in the bid or in this Agreement are and shall continue to remain true and the Selected Bidder will fulfill all the requirements as are necessary for executing the obligations and responsibilities as laid down in this Agreement and the RFP and unless GIC Re specifies to the contrary, the Selected Bidder shall be bound by all the terms of the RFP and this Agreement throughout the term of this Agreement.
- d) That the Selected Bidder has the professional skills, personnel, resources, and statutory, regulatory, and other authorizations that are necessary for providing all such services as are necessary to fulfill the services stipulated in the RFP, the bids, and this Agreement.
- e) That there shall not be any privilege, claim or assertion made by a third party with respect to right or interest in, ownership, mortgage or disposal of any asset, property, movable or immovable as mentioned in any Intellectual Property Rights, licenses and permits.
- f) That the Selected Bidder shall use only such assets of GIC Re as GIC Re may permit for the sole purpose of execution of its obligations under the terms of this Agreement. The same shall be used in a reasonable manner. The Selected Bidder shall, however, have no claim to any right, title, lien, or other interest in any such property, and any possession of property for any

duration whatsoever shall not create any right in equity or otherwise, merely by fact of such use or possession during or after the term hereof.

- g) That the Selected Bidder shall procure all the necessary permissions, approvals, and licenses for use of various software and any copyrighted process/product free from all claims, titles, interests, and liens thereon and shall keep GIC Re indemnified in relation thereto.
- h) That the Selected Bidder will ensure that execution of the Services and the Scope of work herein are and shall be in accordance and in compliance with all applicable laws, including laws applicable to it as the provider of information technology products and services hereunder. That the execution of the Services under this contract is and shall be in accordance and in compliance with all applicable laws.
- i) That neither the execution and delivery by the Selected Bidder of this Agreement nor the Selected Bidder's compliance with or performance of the terms and provisions of this Agreement
 - i. will contravene any provision of any Applicable Law or any order, writ, injunction or decree of any court or Governmental /Municipal/Local Authority binding on it; or
 - ii. will conflict or be inconsistent with or result in any breach of any of the terms, covenants, conditions, or provisions of, or constitute a default under any Contract, or instrument to which the Selected Bidder is a party or by which it or any of its property or assets is bound or to which it may be subject; or
 - iii. will violate any provision of the Memorandum and Articles of Association of the Selected Bidder.
- j) That the Selected Bidder undertakes and/or certifies, that all registrations, recordings, filings and notarizations of this Agreement and all payments of any tax or duty, including stamp duty, registration charges or similar amounts which are required to be affected or made by the Selected Bidder which are necessary to ensure the legality, validity, enforceability, or admissibility in evidence of this Agreement shall have been made.
- k) That the Selected Bidder owns, has license to use or otherwise has the right to use, free of any pending or threatened liens or other security or other interests all its Intellectual Property Rights, which are required or desirable for performance of Services under this Agreement and regarding the same the Selected Bidder does not, so far as the Selected Bidder is aware, in carrying on its business and operations, infringe any Intellectual Property Rights of any person. As far as the Selected Bidder is aware, none of the Intellectual Property Rights, owned or enjoyed by the Selected Bidder or which the Selected Bidder is licensed to use, which are material in the context of Selected Bidder's business and operations for the performance of this Agreement are being infringed nor, so far as the Selected Bidder is aware, is there any infringement or threatened infringement of those Intellectual Property Rights licensed or provided to the Selected Bidder by any person. All Intellectual Property Rights (owned by the Selected Bidder or which the Selected Bidder is licensed to use) required by the Selected Bidder for the performance of this Agreement are valid and subsisting. All actions (including registration, payment of all registration and renewal fees) required to maintain the same in full force and effect have been taken thereon.
- l) The Selected Bidder shall keep GIC Re indemnified in relation to all warranties in this clause. Further, it is hereby clarified that no licenses or rights (including licenses or rights under patents) are granted either directly, by implication or otherwise by GIC Re. GIC Re shall retain ownership of its respective pre - existing intellectual property rights including any customizations, enhancements, or modifications thereto.
- m) That time is the essence of this Agreement and hence the Selected Bidder shall always maintain sufficient manpower, resources, and facilities, to provide the Services in a businesslike manner on a timely basis.
- n) That the Selected Bidder's security measures, confidentiality measures, policies and procedures are up to date and fully equipped to protect and maintain the confidentiality of the Confidential Information in terms of NDA.
- o) That in providing the Services or deliverables or materials, neither the Selected Bidder nor the

Selected Bidder's Team, shall utilize information which may be considered confidential information of, or proprietary to, any prior employer or any other person or entity.

- p) That Services will be performed in a professional manner consistent with industry standards.
- q) That all conditions precedent under this Agreement have been satisfied.

6. **SCOPE OF WORK**

The Scope of work of this Agreement has been defined in the RFP, the Corrigendum/ Addendums/ Amendments issued with respect to such RFP, the Bids, and this Agreement from time to time.

7. **IMPLEMENTATION PERIODS**

The cloud solution should have a warranty which shall be applicable after migration and implementation in the new DC & DR. Warranty will cover troubleshooting, removing bugs/ errors, etc. During the Contract Period if any upgrades/ updates/ new version releases of OS, DB, Hypervisor, etc. are released, it is to be installed free of cost. The Selected Bidder shall ensure smooth functioning of the software by providing offsite/ online/ telephonic support 24*7*365 during the Contract Period. The Selected Bidder shall also ensure the requisite training to the identified staff of GIC Re for maintenance of **the system/ solution**.

- a) **IMPLEMENTATION PHASE:** The implementation phase will be the period from the effective date of this contract to the acceptance and go live of the new Cloud Environment.
- b) **ACCEPTANCE:** The Selected Bidder will create, with user concurrence, a set of user acceptance tests (UAT) which will be run on the new production environment to the satisfaction of GIC Re, followed by Go-Live of new environment, post which GIC Re will provide acceptance of successful migration and implementation of new cloud environment.

8. **TERM OF THE CONTRACT**

This Agreement shall be in effect for a period of **5 years plus implementation & migration phase (referred to as 'Contract Period')** from the Effective Date hereof and will remain valid for the said period unless it is otherwise terminated earlier as per the provisions of this Agreement/ RFP. Upon completion of the term of Contract Period, this Agreement shall automatically expire, subject to due discharge of all obligations mentioned in Clause "consequences of termination" by the Selected Bidder to the satisfaction of GIC Re.

9. **TIME IS THE ESSENCE OF THIS CONTRACT**

It is hereby specifically agreed to between the Parties that time is the essence of this Contract.

10. **REPORTING PROGRESS**

- a) The Services, and/ or their Personnel to be provided by the Selected Bidder under this Agreement and the manner and speed of execution and maintenance of the Services are to be conducted to the satisfaction of GIC Re in accordance with this Agreement. Should the rate of progress of the work, compliance to the requirements of the standards of service, or any part of the services at anytime fall behind the stipulated time for completion or is found to be too slow to ensure completion of the works on time or insufficient for satisfactory operation of the project, GIC Re shall so notify the Selected Bidder through email.
- b) The Selected Bidder shall reply to the written notice giving details of the measures it proposes to take to expedite the progress to complete the Services by the prescribed time or to meet the standards of service required. The Selected Bidder shall not be entitled to any additional payment for taking such steps. If at any time it should appear to GIC Re that the actual progress of work does not conform to the approved programme/ plan the Selected Bidder shall produce, at the request of GIC Re, a revised programme/ plan showing the modification to the approved programme/ plan necessary to ensure completion of the work within the time for completion or steps initiated to ensure compliance to the stipulated requirements.

- c) In case during the implementation of this Agreement, the progress falls behind schedule or does not meet the desired requirements, the Selected Bidder shall deploy extra manpower, resources, infrastructure, etc., to make up the progress or to meet the requirements. Programme/ plan for deployment of extra manpower/ resources/ infrastructure must be submitted to GIC Re for its review and approval. All time and cost effect in this respect shall be borne by the Selected Bidder.
- d) The Selected Bidder shall monitor progress of all the activities specified in this Agreement and submit free of cost “Monthly Progress Report” about various aspect of the work to GIC Re. Extracts of the Monthly Progress Report to be termed, as “Executive Summary” shall be submitted, along with Monthly Progress Report.

11. STATUTORY AND OTHER REQUIREMENTS

- a) During the tenure of this Agreement nothing shall be done by the Selected Bidder in contravention of any laws, Acts, rules and/ or regulations or any amendments thereof and it shall keep GIC Re indemnified in this regard for any violation or non-compliance of the same.
- b) The Selected Bidder and its Team shall not alter/ change/ replace any hardware/ software/ Applications/ Licenses proprietary to GIC Re and/ or under warranty or AMS of third party without prior written consent of GIC Re.
- c) The Selected Bidder and its Team shall not, without the prior consent of GIC Re, install any hardware or software not purchased/ owned by GIC Re.

12. AGREEMENT ADMINISTRATION

The parties shall appoint an individual as their authorized representative (hereinafter referred to as ‘Representative’) through a written notice to the other party as the primary contact of each party with respect to this Agreement, which person may be re-designated by a party by notice to the other. Each Representative shall have the authority to:

- a) Exercise all the powers and functions of his/ her Party under this Agreement and ensure the proper administration and performance of the terms hereof, other than the power to amend this Agreement; and
- b) Bind his or her Party in relation to any matter arising out of or in connection with this Agreement.
- c) For execution or performance of the obligations under this Agreement, GIC Re’s Representative would act as an interface with the representative of the Selected Bidder. The Selected Bidder shall comply with any instructions that are given by GIC Re’s Representative during this Agreement in relation to the performance of its obligations under the terms of this Agreement.
- d) A Committee comprising of Representatives from GIC Re and the Selected Bidder shall meet on a regular basis to discuss any issues/ bottlenecks being encountered. The Selected Bidder shall draw the minutes of these meetings, take all necessary actions, and circulate the same to GIC Re.

13. RIGHT OF MONITORING, INSPECTION AND PERIODIC AUDIT

- a) GIC Re reserves the right to inspect, monitor and assess the progress/ performance of all the **Services envisaged under this Agreement** at any time during the validity of this Agreement. GIC Re may demand and upon such demand being made, it shall be provided with any document, data, material, or any other information which it may require, to enable it to do the same.
- b) GIC Re shall also have the right to conduct, either itself or through another person as it may deem fit, an audit to monitor the performance by the Selected Bidder of its obligations/ functions in accordance with the standards committed to or required by GIC Re and the Selected Bidder undertakes to cooperate with and provide to GIC Re/ another person appointed by GIC Re all documents and other details as may be required by them for this purpose after

giving Selected Bidder at least one week's notice in advance. Any deviations or contravention identified because of such audit/ assessment would need to be rectified by the Selected Bidder failing which GIC Re may, without prejudice to any other rights, issue a Notice of Default.

14. GIC RE'S OBLIGATIONS

- a) GIC Re's representative shall interface with the Selected Bidder, to provide the required information, clarifications, and to coordinate to resolve any issues as may arise during the execution of this Agreement.
- b) GIC Re shall provide adequate co-operation in providing details, assisting with coordinating, and obtaining of approvals from various governmental agencies, in cases where the intervention of GIC Re is proper and necessary.
- c) GIC Re shall ensure that timely approval is provided to the Selected Bidder, where any approval is required to be provided by GIC Re.

15. INFORMATION SECURITY

- a) The Selected Bidder shall not carry and/ or transmit any material, information, layouts, diagrams, storage media or any other goods/ material in physical or electronic form, which are proprietary to/ or owned by GIC Re out of GIC Re/ DC/ DR premises without prior written permission from GIC Re.
- b) The Selected Bidder shall adhere to the Information Security Policy of GIC Re as amended from time to time (Information Security Policy will be provided to the Selected Bidder at the time of migration). In case of any ambiguity or conflict between the terms of this Agreement and the Information Security Policy, the terms of the Information Security Policy shall prevail. In case the Selected Bidder is found to be in violation of the said policy, GIC Re reserves the right to terminate this Agreement in addition to any other remedies for breach, injunctive relief, and indemnity as per this Agreement and the applicable laws
- c) The Selected Bidder acknowledges that GIC Re's business data and other proprietary information or materials, whether developed by GIC Re or being used by it pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to GIC Re; and the Selected Bidder agrees to take utmost care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by Selected Bidder to protect its own proprietary information. Selected Bidder recognizes that the goodwill of GIC Re depends, among other things, upon Selected Bidder keeping such Proprietary Information confidential and that unauthorized disclosure of the same by Selected Bidder could damage reputation of GIC Re. Selected Bidder also recognizes that by reason of Selected Bidder's duties here under, it may come into possession of such proprietary information, even though it does not take any direct part in or furnish the services performed for the creation of said proprietary information and undertakes to limit access thereto to employees with a need to such access to perform the services required by this Agreement. Selected Bidder shall use such information only for performing the said services.
- d) The Selected Bidder shall, upon termination of this Agreement for any reason or upon demand by GIC Re whichever is earlier, return any and all information provided to Selected Bidder including any copies or reproductions, both hard copy and electronic copy.

16. INSURANCE

- a) The Selected Bidder shall, at his own expense, arrange appropriate comprehensive insurance to cover all risks assumed by the Selected Bidder under this Agreement as well as in respect of its personnel deputed under this Agreement. GIC Re will have no liability on this account.
- b) The Selected Bidder shall take out, at his own expense, comprehensive insurance policies against all risks of loss or damage caused to the equipment/ tools/ data owned by GIC Re or acquired for GIC Re.

- c) The Selected Bidder shall, at his own expense, arrange appropriate comprehensive insurance that will respond to the full extent of contractual liabilities and to all claims under the Deed of Indemnity.

17. INDEMNITY

The Selected Bidder shall execute and furnish to GIC Re a Deed of Indemnity annexed with RFP as **Annexure VIII** indemnifying GIC Re and holding it harmless to the extent of 100% in respect of the situations stated therein. All claims regarding indemnity and the Deed of Indemnity shall survive the termination or expiry of this Agreement.

18. CONFIDENTIALITY

Either Party shall not use Confidential Information, the name, or the logo of the other Party except for the purposes of this Agreement; The Selected Bidder shall sign the NDA as annexed to the RFP as **Annexure VII**. The obligations of the Parties in this respect shall be as per the Non-Disclosure Agreement (NDA) which shall survive the termination or expiry of this Agreement.

19. TERM AND EXTENSION

- a) The term of this Agreement is as prescribed in **Clause 8** (Term of the Contract).
- b) Further GIC Re reserves the right to grant any extension to the term above mentioned and shall notify in writing to the Selected Bidder, at least 30 days before the expiration of the Term hereof, whether it will grant the Selected Bidder an extension of the term. The decision to grant or refuse the extension shall be at the discretion of GIC Re. In case no written communication as aforesaid is received by Selected Bidder from GIC Re it shall mean GIC Re does not intend to give extension to this Agreement.
- c) In the event of extension of Service, GIC Re will continue payment for this extended period as per the terms and condition already agreed in this Agreement.
- d) The Selected Bidder shall continue to perform all its obligations hereunder, until such reasonable time beyond the Term of this Agreement within which, GIC Re shall either appoint an alternative person or create its own infrastructure to operate such Services as are provided under this Agreement and GIC Re will notify the Selected Bidder one month in advance about such extension of services and will continue payment for this extended period as per the terms and condition already agreed in this Agreement.

20. PRICE

Prices quoted/ Contract Price shall be firm and shall not be subject to any upward revision on any account whatsoever throughout the period of this Agreement except where specifically provided for elsewhere in this Agreement.

21. CHANGE ORDERS/ CONTRACT VARIATION

- a) The Selected Bidder agrees that the requirements given in the RFP and Agreement are broad requirements and are in no way exhaustive and guaranteed by GIC Re.
- b) It shall be the responsibility of the Selected Bidder to meet all the requirements of technical criteria and Scope of Work contained in the RFP and this Agreement and any upward revisions and/ or additions of quantities/ specifications/ sizes given in specifications etc., of the Bid required to be made shall not constitute a Change Order and shall be carried out without any change order, time, and cost effect to GIC Re.
- c) GIC Re at any time by written Change Order may change the scope of work of this RFP and Agreement, including the specifications, statement of work, number, and design criteria of any of the components thereof, delivery dates/ timing of submission of reports, personnel inputs, timing of an activity or a particular output.
- d) If any such change has cost or time implications for the Selected Bidder, GIC Re shall adjust price and delivery schedules equitably through a further written Change Order, on the written

request of the Selected Bidder. The Selected Bidder further understands and agrees that if any such change entails any reduction in the scope of work, then the cost and/ or time benefits shall be passed on to GIC Re through a mutual Change Order in writing.

- e) The Selected Bidder shall not make any change in the scope of work of this RFP and Agreement without the prior written approval of GIC Re.
- f) The Selected Bidder further understands and agrees that any alteration, variation or addition in the scope of work necessitated by amendments and/ or additions to any laws, rules or regulations before the time of award of the contract or during the currency of the contract shall not be considered a subject of a Change Order, provided that the nature of the mandate introduced by the law, rule or regulation is of such a nature that its non-inclusion, exclusion or alteration would render the subject matter of the procurement infructuous or expose GIC Re to the risk of non-compliance with applicable laws, rules or regulations.
- g) Any changes required by GIC Re over and above the minimum requirements given in the Scope of Work in the RFP, before giving its approval to detailed design, for complying with technical criteria and changes required to ensure systems compatibility and reliability for safe (As per codes, standards and recommended practices referred in the RFP, Bid) and trouble-free operation shall not be construed to be change in the Scope of Work under this Agreement.
- h) If there is a difference of opinion between the Selected Bidder and GIC Re Representative whether a particular work or part of the work constitutes a Change Order or not, the matter shall be handled in accordance with the procedures set forth in the next clause (Procedures for Change Order).
- i) Within 14 working days of receiving the comments from GIC Re on the specification, purchase requisitions and other documents submitted by the Selected Bidder for approval, the Selected Bidder shall respond in writing, which item(s) of the comments is/ are potential changes(s) in the Scope of Work covered in this Agreement and shall advise a date by which Change Order (if applicable) will be submitted to GIC Re.
- j) All such contract variations carried out via Change Orders shall be recorded in the form of an amendment to this Agreement.
- k) Any upward revisions and/ or additions to the Scope of Work of this RFP, consequent to errors, omissions, ambiguities, discrepancies in the specification etc. of the RFP which the Selected Bidder had not brought to GIC Re's notice at the time of the Bids shall not constitute a Change Order and such upward revisions and/ or additions shall be carried out by the Selected Bidder without any time and cost implications to GIC Re.

22. PROCEDURES FOR CHANGE ORDER

- a) During the implementation/ migration/ management or at any stage during the implementation of this Agreement, if the Selected Bidder observes that any new requirement which (other than that required for meeting the technical criteria) is not specific or intended by this Agreement has been stipulated by GIC Re while approving the specifications, purchase requisitions, other documents etc. it shall verbally discuss the matter with the Representative of GIC Re which shall be captured in writing in note filings or minutes of meeting.
- b) In case such requirement arises from the side of the Selected Bidder, their Representative would also verbally discuss the matter with GIC Re Representative giving reasons thereof which shall be captured in writing in note filings or minutes of meeting.
- c) In either of the two cases, the Representatives of the Parties shall discuss on the new requirement for better understanding and shall mutually decide whether such requirement constitutes a Change Order or not.
- d) If it is mutually agreed that such requirement constitutes a Change Order, then a joint memorandum will be prepared and signed by the Selected Bidder and GIC Re to confirm a Change Order and basic ideas of necessary agreed arrangement.
- e) Upon completion of the study referred to above under clause 22.d, the results of this study along with all relevant details including the estimated time and cost effect thereof with supporting documents would be submitted to GIC Re, within one week, to enable GIC Re to give a final

decision whether the Selected Bidder should proceed with the Change Order or not in the best interest of the works. The estimated cost and time impact indicated by Selected Bidder shall be considered as a ceiling limit and shall be provisionally considered for taking a decision to implement Change Order. The time impact applicable to this Agreement shall be mutually agreed, subsequently, based on the detailed calculations supported by all relevant back up documents. In case the Selected Bidder fails to submit all necessary substantiation/ calculations and back up documents, the decision of GIC Re regarding time and cost impact shall be final and binding on the Selected Bidder.

- f) If GIC Re accepts the implementation of the Change Order under Clause 22.e above in writing, which would be considered as Change Order, the Selected Bidder shall commence to proceed with the relevant work stipulated in the Change Order pending final agreement between the Parties about adjustment of the Contract Price and implementation schedule.
- g) In case, mutual agreement as to whether new requirement constitutes the Change Order or not, is not reached, then Selected Bidder in the interest of the works, shall take up the implementation of the work, if advised in writing to do so by GIC Re Representative pending settlement between the two parties to the effect whether such requirement constitutes a Change Order or not as per the terms and conditions of this Agreement. The time and cost effects in such a case shall be mutually verified and recorded. Should it establish that the said work constitutes a Change Order; the same shall be compensated as per the clause 21.h given below.
- h) The Selected Bidder shall submit necessary back up documents for the Change Order showing the break-up of the various elements constituting the Change Order for GIC Re's review. If no agreement is reached between GIC Re and Selected Bidder within 60 days after GIC Re's instructions in writing to carry out the change concerning the increase or decrease in this Contract Price and all other matters described above, either Party may refer the dispute to arbitration.

23. SUSPENSION OF WORK

The Selected Bidder shall, if ordered in writing by GIC Re, temporarily suspend the works or any part thereof for such a period and such time as ordered. The Selected Bidder shall not be entitled to claim compensation for any loss or damage sustained by them by reason of temporary suspension of the Services as aforesaid. An extension of time for completion, corresponding with the delay caused by any such suspension of the works as aforesaid shall be granted to the Selected Bidder, if request for same is made, provided that the suspension was not consequent to any default or failure on the part of the Selected Bidder. In case the suspension of works, is not consequent to any default or failure on the part of the Selected Bidder and lasts for a period of more than 3 months, the Selected Bidder shall have the option to request GIC Re to grant equitable adjustment in the Contract Price.

24. LIQUIDATED DAMAGES

In the event of low/ poor performance or delay by the Selected Bidder as per the requirements of this Agreement and RFP, the Selected Bidder is solely responsible for the Liquidated Damages (LD) which shall be calculated as under. The Monthly Recurring Charges (MRC) used below refers to MRC applicable for the month in which the Service or Incident Request was created.

For Service Request (SR) Management: The Selected Bidder shall make an estimate of the time required for carrying out the requested service/ task and this will be mutually agreed upon by the selected Bidder and GIC Re. Thereafter, the penalty/ LD for missed deadlines for SRs will result in maximum **penalty amount of 20% MRC per month**. The Selected Bidder shall provide a timeline chart for standard SRs (e.g., creation/ deletion of VMs, compute and storage modification, etc.). For all other SRs, timeline will be mutually decided, as described above. The tool provided by Selected Bidder must capture such time frames for SRs and subsequent LD calculations.

For Incident Request (IR) Management: The liquidated damages for every miss of an SLS (Service Level Summary) deadline for Incidents or event request (ticket) will be as per below table (LD Calculation Matrix for IR). So, if an event is raised with severity as 'Very High Level', then missing the 'resolution time' deadline of 1 hour will result in Liquidated damages.

The LD Calculation Matrix below specifies performance parameters as baseline performance, lower performance, and breach. All Service Level calculations will be done on monthly basis. The agreement also specifies the penalties for lower performance and breach conditions.

Payment to the Service Provider is linked to the compliance with the LD Calculation Matrix. The matrix specifies three levels of performance, namely:

- The Service Provider will get 100% of the Contract Price if the baseline performance metrics are complied.
- The Service Provider will get payment after deducting penalty at the rates specified below in case of the lower performance.
- If the performance of the Service Provider in respect of any parameter falls below the prescribed lower performance limit and is not corrected within 48 hours shall be considered as a breach of Agreement.

Calculating the Hosting Service Unavailability Credit:

- Selected Bidder shall maintain the Hosting Services in Proper Operational Condition. The Hosting Service should be backed by the following Service Availability Guarantee (hereafter "Hosting Service Availability Guarantee").
- Hosting Services will be considered unavailable if the fault/ incident reported to the Selected Bidder by GIC Re or identified by Selected Bidder himself is of Severity Level "Critical", "High", "Medium" or "Low" ("Hosting Service Unavailability"). Selected Bidder will calculate, monthly, the time of Hosting Service Unavailability experienced by GIC Re. A month shall be deemed to begin at 12:00AM Greenwich Mean Time ("GMT") on the first day of a calendar month and end 12:00AM GMT on the first day of the next calendar month ("Month"). At the end of a Month, Selected Bidder shall calculate the total amount of time the Hosting Services were unavailable measured from the time when a fault/ incident of any Severity Level was reported to the Selected Bidder or is identified by Selected Bidder, whichever first occurs, until the time the fault/ incident is repaired/ resolved, and the Hosting Services restored (the "Hosting Service Unavailability Time"). Such Hosting Service Unavailability Time shall be used to determine any Service Unavailability credit that GIC Re shall be entitled to ("Hosting Service Unavailability Credit"). The Hosting Service Unavailability Credit will be a percentage of the Monthly Recurring Charge ("MRC") for the Hosting Service as set forth in following tables. The Hosting Service Unavailability Credit will be calculated in totality for the Hosting Service.
- GIC Re shall also calculate penalty (for incidents) at the rates stated below and the net amount so calculated during the months in a quarter shall be added together and the total amount shall be deducted from the quarterly bill to be submitted by the Selected Bidder.
- The Service Provider shall provide GIC Re with an online report of the service unavailability & downtime.

LD/ Hosting Service Unavailability Credit Calculation Matrix for Incidents (IRs):

(a) For Severity Level "Critical/ Very High":

Sr. No.	Duration of Service Unavailability (hours)	Penalty Percentage
1.	0 – 1	No Credit/ Penalty
2.	1 – 2	10% of MRC
3.	2 – 4	15% of MRC
4.	4 – 6	25% of MRC
5.	6 – 8	35% of MRC
6.	For each subsequent 1-hour period thereafter up to 24 hours from the time of logging of call	4% of MRC in addition to the above
7	Beyond 24 hours will be considered Breach of Agreement	100% of MRC

(b) For Severity Level “High”:

Sr. No.	Duration of Service Unavailability (hours)	Penalty Percentage
1.	0 – 1.5	No Credit/ Penalty
2.	1.5 – 3	5% of MRC
3.	3 – 6	10% of MRC
4.	6 – 9	15% of MRC
5.	9 – 12	25% of MRC
6.	For each subsequent 3-hour period thereafter up to 36 hours from the time of logging of call	3% of MRC in addition to the above
7	Beyond 36 hours will be considered Breach of Agreement	100% of MRC

(c) For Severity Level “Medium”:

Sr. No.	Duration of Service Unavailability (hours)	Penalty Percentage
1.	0 – 4	No Credit/ Penalty
2.	4 – 9	5% of MRC
3.	9 – 15	10% of MRC
4.	For each subsequent 9-hour period thereafter up to 48 hours from the time of logging of call	5% of MRC in addition to the above
5	After 48 hours	Severity level to be set at serial no. 5 of High (Table b)

(d) For Severity Level “Low”:

Sr. No.	Duration of Service Unavailability (hours)	Penalty Percentage
1.	0 - 8	No Credit/ Penalty
2.	8 - 16	5% of MRC
3.	16 - 24	10% of MRC
4.	For each subsequent 12-hour period thereafter up to 48 hours from the time of logging of call	5% of MRC in addition to the above
5	After 48 hours	Severity level to be set at serial no. 5 of High (Table c)

GIC Re has sole discretion to waive LD if there are valid reasons. The LD will be calculated monthly and then added up for a quarter and deducted from Quarterly Recurring Charges to the Selected Bidder. The Service Provider shall adhere to all requirements laid out in the RFP and this Agreement.

Penalty & LD on One-Time Charges (OTC):

In the event of delayed Implementation & Migration of entire Setup, i.e., after the expiry of the Migration and Go-Live period of 16 weeks, the Selected Bidder shall be liable to pay Liquidated Damages at a percentage of the value of the OTC stated in the Commercial Bid subject to a maximum of 10% (ten percent) as detailed below:

- @ 1% for delay up to one week.
- @ 2.5% for delay up to two weeks.
- @ 5% for delay up to three weeks.
- @ 10% for delay for four weeks and above.

For this clause, part of the week is considered as a full week.

Any such Liquidated Damages when levied may be offset as against any pending payment/future payment by GIC Re to the Service Provider. Alternatively, the Liquidated Damages shall be deducted from the PBG submitted. The Service Provider shall replenish the PBG with the amount equal to the Liquidated Damages levied in not later than 10 working days from the date of levy of Liquidated Damages.

Each Levy of Liquidated Damages shall be exclusive of the other.

If the maximum Liquidated Damages per year exceeds 25% of PBG, submitted by the Selected Bidder, GIC Re reserves the right to terminate the Agreement by giving 15 days' notice and/or pursue other remedies available under the Agreement.

25. RECOVERY OF LIQUIDATED DAMAGES

The Liquidated Damages will be recovered from Selected Bidder, on demand by GIC Re. Any such Liquidated Damages when levied may be offset as against any pending payment/ future payment by GIC Re to the Selected Bidder. GIC Re also reserves the right to recover the Liquidated Damages amount by invoking the Performance Bank Guarantee. The Selected Bidder shall replenish the PBG with the amount equal to the Penalty levied in not later than 10 working days from the date of levy of Liquidated damages.

GIC Re has the right to recover Liquidated Damages amount from any dues that may be payable to the Successful Bidder under any previous contract with GIC Re under the right of set off.

Any such recovery of Liquidated Damages shall not in any way relieve the Service Provider from any of its obligations to complete the work or from any other obligations and liabilities under this Agreement.

All Liquidated Damages levied shall be exclusive of each other.

26. NON-ACCEPTANCE/ NON-EXECUTION OF ORDER

In case the Successful Bidder refuses to accept/ execute the order, GIC Re will procure the same from the respective OEM as per terms & conditions and rate accepted by OEM. The Successful Bidder shall bear the difference in cost of the items/ products (GIC Re is having all the rights to recover the difference/ liquidated damages amount from PBG as well as any amount payable to the Bidder). If required, GIC Re may also act against the Successful Bidder and blacklist them without any correspondence in this regard.

27. PAYMENT TERMS

- a) The Contract Price shall be equal to the amount specified in the Commercial Bid (**Annexure IV**). Payments will be released only on satisfactory acceptance of the deliverables for each task as per the following schedule:
 - The Selected Bidder must complete the implementation, data migration and Go-Live for DC and DR sites within **16 weeks** of receiving the Purchase Order.
 - One-Time Charges as per the Commercial Bid (**Annexure IV**) would be paid on completion of activities as per Scope of work and sign-off from GIC Re.
 - Recurring charges would be paid at the end of each quarter from date of Go-Live.
- b) All Payments shall be made in Indian Rupees Only and will be subject to provisions of the **Clause 24 Liquidated Damages** or any other recoverable due from Selected Bidder to GIC Re.
- c) GIC Re shall be entitled to make recoveries from the Selected Bidder's bill/ invoice, the Performance Bank Guarantee, or from any other amount due to the Selected Bidder, of the equivalent value of any payment made to it due to inadvertence, error, collusion, misconstruction, misstatement, or mistake.
- d) Selected Bidder shall be deemed to have considered all the costs required for successful implementation of the Scope of Work as per RFP and this Agreement while submitting the Commercial bid. GIC Re will not be liable to pay any extra cost, charges or out of pocket expenses.
- e) Payment for the implementation of the Scope of Work as per the RFP and this Agreement will be released after signoff for successful completion of the Scope of Work.
- f) The Selected Bidder shall not, in any case whatsoever, link its billing to GIC Re's asset and/ or revenue base.

28. EVENTS OF DEFAULT BY THE SELECTED BIDDER

The failure on the part of the Selected Bidder to perform any of his obligations or comply with any of the terms of this Agreement shall constitute an Event of Default on the part of the Selected Bidder. The Events of Default as mentioned above may include inter-alia the following: -

- a) The Selected Bidder fails to perform any thing as per any instruction or directive issued by GIC Re which GIC Re deems proper and necessary to execute the Scope of Work under this Agreement.
- b) The Selected Bidder fails to adhere to any of the terms of this Agreement, or if the Selected Bidder falls short of matching such standards/ targets as GIC Re may have designated with respect to any task necessary for the execution of the Scope of work under this Agreement. The above-mentioned failure on the part of the Selected Bidder may be in terms of failure to adhere to timelines, specifications, requirements, or any other criteria as defined by GIC Re.
- c) The Selected Bidder fails to remedy a failure to perform its obligations in accordance with the specifications issued by GIC Re despite being served with a Notice of Default which lays down the specific deviance on the part of the Selected Bidder to comply with any stipulations or standards as laid down by GIC Re.
- d) The Selected Bidder/ Selected Bidder's Team fails to conform with any of the Service/ Facility Specifications/ standards as set out in the scope of work of this Agreement or has failed to adhere to any amended direction, modification or clarification as issued by GIC Re during the term of this Agreement and which GIC Re deems proper and necessary for the execution of the scope of work under this Agreement.
- e) The Selected Bidder fails to demonstrate or sustain any representation or warranty made by it in this Agreement, with respect to any of the terms of its Bid, the RFP, and this Agreement.
- f) There is a proceeding for bankruptcy, insolvency, winding up or there is an appointment of receiver, liquidator, assignee, or similar official against or in relation to the Selected Bidder.
- g) The Selected Bidder fails to comply with or is in breach or contravention of any applicable laws.
- h) Failure on the part of the Selected Bidder to respect any of its commitments regarding any part of its obligations under its Bid, the RFP or under this Agreement.

29. CONSEQUENCES IN EVENT OF DEFAULT

- a) Where there has been an Event of Default, GIC Re shall issue a Notice of Default to the Selected Bidder, setting out specific defaults/ deviances/ omissions and providing a notice of 30 days to enable the Selected Bidder to remedy the default committed.
- b) Where despite the issuance of a Notice of Default to the Selected Bidder by GIC Re the Selected Bidder fails to remedy the default to the satisfaction of GIC Re, GIC Re may, where it deems fit, issue to the Selected Bidder another Notice of Default or proceed to adopt such remedies as may be available to GIC Re.
- c) Where an Event of Default subsists or remains uncured GIC Re shall be entitled to:
 - Impose any such obligations and conditions and issue any clarifications as may be necessary to inter alia ensure smooth continuation of Services and the Selected Bidder shall be obliged to comply with which may include unilateral re-determination by GIC Re of the Contract Price payable to the Selected Bidder hereunder. The Selected Bidder shall in addition take all available steps to minimize loss resulting from such Event of Default.
 - GIC Re may, by a written Notice of Payment Suspension to the Selected Bidder, suspend all payments to the Selected Bidder under this Agreement, provided that such Notice of Payment Suspension:
 - i. shall specify the nature of the failure; and
 - ii. shall request the Selected Bidder to remedy such failure within a period of 15 days from the date of receipt of such Notice of Payment Suspension by the Selected Bidder
 - Where GIC Re deems necessary, it shall have the right to require replacement of any

member of the Selected Bidder's Team/ sub-contractors/ Selected Bidders (other than the "Selected Bidder" under this Agreement) with another suitable member. The Selected Bidder shall in such case forthwith find a suitable replacement for such outgoing member/ sub-contractors/ Selected Bidders (other than the "Selected Bidder" under this Agreement) with another member/ sub-contractors/ Selected Bidders (other than the "Selected Bidder" under this Agreement) to the satisfaction of GIC Re. Failure on the part of the Selected Bidder to find a suitable replacement and/ or terminate all agreements/ Agreements with such member, shall amount to a breach of the terms hereof and GIC Re in addition to all other rights, have the right to claim damages and recover from the Selected Bidder all losses/ or other damages that may have resulted from such failure by invoking the PBG or otherwise.

30. TERMINATION

GIC Re may terminate this Agreement in whole or in part by giving the Selected Bidder 30 days prior and written notice indicating its intention to terminate this Agreement under following sub-clauses:

- a) Where GIC Re is of the opinion that there has been an Event of Default on the part of the Selected Bidder and the default has not been rectified in terms of the Notice of Default, which would make it proper and necessary to terminate this Agreement.
- b) Where it comes to GIC Re's attention that the Selected Bidder (or the Selected Bidder's Team) is in a position of actual conflict of interest with the interests of GIC Re in relation to any of terms of the Selected Bidder's Bid, the RFP, or this Agreement.
- c) Where the Selected Bidder's ability to survive as an independent corporate entity is threatened or is lost owing to any reason whatsoever, including inter-alia the filing of any bankruptcy proceedings against the Selected Bidder, any failure by the Selected Bidder to pay any of its dues to its creditors, the institution of any winding up proceedings against the Selected Bidder or the happening of any such events that are averse to the commercial viability of the Selected Bidder. GIC Re reserves the right to take any steps as are necessary to ensure the effective transition of the project to new Selected Bidder and to ensure business continuity and the Selected Bidder shall co-operate for the same.
- d) Termination for Insolvency: GIC Re may at any time terminate this Agreement with immediate effect by giving written notice to the Selected Bidder, without compensation to the Selected Bidder, if the Selected Bidder becomes bankrupt or otherwise insolvent, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to GIC Re.
- e) Termination for Convenience: The notice of termination shall specify that termination is for GIC Re convenience, the extent to which performance of work under this Agreement is terminated, and the date upon which such termination becomes effective.
- f) GIC Re may terminate this Agreement if the Selected Bidder fails to comply with any decision reached consequent upon arbitration proceedings pursuant to dispute resolution clause hereunder.
- g) If at any point of time and for any period, the Liquidated damages exceeds 100% of PBG submitted by the Selected Bidder.
- h) If the aggregate of Liquidated Damages levied under the Liquidated Damages clause exceeds the amount mentioned therein, GIC Re reserves the right to terminate this Agreement by giving 30 days' notice and pursue other remedies available under this Agreement in addition to setting off the Liquidated Damages or recovering the same from PBG.
- i) The Selected Bidder may, subject to approval by GIC Re, terminate this Agreement before the expiry of its term by giving GIC Re a prior and written notice at least 90 days in advance indicating its intention to terminate the Agreement.

31. CONSEQUENCES OF TERMINATION/EXPIRY

- a) In the event of termination of this Agreement, the Selected Bidder's services shall stand cancelled effective from the date of termination of this Agreement.
- b) In the event of termination of this Agreement, GIC Re reserves its rights to call for new bids or award the contract to the next best value Bidder of this tendering process.
- c) In the event of termination/ expiry of this Agreement due to any cause whatsoever, [whether consequent to the expiry of the stipulated Term of this Agreement or otherwise] GIC Re shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Services which the Selected Bidder shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/ expiry, and further allow and provide all such assistance to GIC Re and/ or the new Selected Bidder, as may be required, to take over the obligations of the Selected Bidder in relation to the execution/ continued execution of the Scope of Work of this Agreement.
- d) Where the termination of this Agreement is prior to its stipulated Term (due to any reason), GIC Re through unilateral re-determination of the Contract Price payable to the Selected Bidder shall pay the Selected Bidder for that part of the Services which have been authorized by GIC Re and satisfactorily performed by the Selected Bidder up to the date of termination.
- e) Without prejudice to any other rights, GIC Re may retain such amounts from the payment due and payable by GIC Re to the Selected Bidder as may be required to offset any losses caused to GIC Re because of any act/ omissions of the Selected Bidder. In case of any loss or damage due to default on the part of the Selected Bidder in performing any of its obligations regarding executing the scope of work under this Agreement, the Selected Bidder shall compensate GIC Re for any such loss, damages, or other costs, incurred by GIC Re.
- f) Additionally, the Selected Bidder and the Selected Bidder's Team shall perform all their obligations and responsibilities under this Agreement in an identical manner as were being performed before the termination of this Agreement with the Selected Bidder as described above to execute an effective transition and to maintain business continuity. All third parties shall continue to perform all/ any functions as stipulated by GIC Re and as may be proper and necessary to execute the Scope of work under this Agreement in terms of the Selected Bidder's Bid, the RFP, and this Agreement.
- g) Nothing herein shall restrict the rights of GIC Re to invoke the Performance Bank Guarantee, enforce the Deed of Indemnity and pursue such other rights and/ or remedies that may be available to GIC Re under this Agreement equity or law.
- h) The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of this Agreement that are expressly or by implication intended to come into or continue in force on or after such termination.

32. DISPUTE RESOLUTION & ARBITRATION

If a dispute, difference or claim (including non-contractual dispute, difference or claim) between the Parties arises during or after the tenure of this Agreement, out of or in connection with this Agreement (including that relating to the existence, interpretation, construction, meaning, scope, operation, application, effect, validity or the breach of the provisions of this Agreement), the Parties shall attempt in good faith to resolve such dispute, difference or claim promptly, without the need for litigation and so as to allow as far as possible for commercial relationships to remain unaffected in the following manner: -

- (i) through negotiations between respective senior executives of the Parties who have authority to settle the dispute, difference, or claim.
- (ii) if the dispute, difference, or claim is not resolved through negotiations within three (3) months of the same arising, through mediation with the assistance of a mediator agreed between the Parties.

- (iii) if the dispute, difference, or claim is not resolved through mediation within six (6) months of the initiation of the same or if either Party did not or will not participate in the mediation procedure, either Party may refer the dispute, difference or claim to Arbitration as provided for herein.
- a) **Where the Selected Bidder is a Public-Sector Undertaking of the Government of India:**
- Subject to the Parties' committed efforts to settle the dispute, difference or claim amicably as per this clause or through mutual consultation through the good offices of empowered agencies of the Government of India, the dispute, difference or claim other than those related to taxation matters, shall be referred to and settled by arbitration in accordance with the Administrative Mechanism for Resolution of CPSEs Disputes (AMRCD) as mentioned in DPE OM No. 4(1)/2013-DPE(GM)/FTS-1835 dated 22-05-2018 and the decision made in pursuance thereof shall be binding on the Parties.
- b) **Where the Selected Bidder is not a Public-Sector Undertaking of the Government of India:**
- Subject to the Parties' committed efforts to settle the dispute, difference or claim amicably as per this clause, the dispute, difference, or claim shall be referred to and settled by Arbitration. The Arbitration proceedings shall be conducted in accordance with the Arbitration and Conciliation Act, 1996 or any enactment, modification, or re-enactment in force at the relevant time.
 - Qualification of the Arbitrators: The Arbitrators constituting the Arbitral Tribunal shall be persons with not less than ten years of experience in matters of Information Technology and use of Cloud Computing in the Insurance/ Reinsurance industry or as lawyers/ other professional advisers serving this segment, including persons retired from this industry.
 - Declaration by the prospective Arbitrators: Where a person is approached for appointment as Arbitrator under this clause, he/ she shall, before accepting the appointment, make a declaration or disclosure in writing to the Parties as laid out in schedule VI of the Arbitration and Conciliation Act, 1996 in view of section 12 r/w schedule V and Schedule VII of the same.
 - Number of Arbitrators: The Arbitral Tribunal shall consist of three (3) Arbitrators. Both the Parties shall appoint one Arbitrator each (the initiator shall appoint its arbitrator and call upon the other Party to appoint its arbitrator within 14 days of the request), the third Arbitrator (who shall serve as Chairman) shall be appointed by the two party-appointed Arbitrators as soon as practicable (no later than 28 days after the appointment of the second of the two Party-appointed Arbitrators). The Arbitral Tribunal shall be constituted only after the appointment of the third Arbitrator. Where a Party fails to appoint an arbitrator within 14 days of being called upon to do so or where the two Party-appointed arbitrators fail to appoint a third within 28 days of the appointment of the second of the two Party-appointed Arbitrators, then upon application, the Indian Regulator will appoint an arbitrator to fill the vacancy. At any time prior to the appointment by the Indian Regulator the Party or arbitrators in default may make such appointment.
 - Seat of arbitration, language and applicable law: The seat of arbitration shall be Mumbai, India. The language of arbitration shall be English and the laws applicable to the arbitration shall be the laws of India.
 - Arbitral Award: The Arbitral Tribunal's award shall be in writing. The Parties shall submit to the arbitral award which shall be final and binding on the Parties and the same shall be enforceable in any competent court of law.
- c) **Right of Action:** It is a condition precedent to any right of action or suit upon this Agreement except for the interim measures under Section 9 of the Arbitration and Conciliation Act, 1996 that an arbitral award shall be first obtained.
- d) **Jurisdiction:** If these arbitration provisions shall be held to be invalid, then all such disputes or differences or claims shall be referred to the exclusive jurisdiction of the competent courts at Mumbai, India.
- e) **Continuance of this Agreement:** Notwithstanding the fact that settlement of dispute(s) (if

any) under arbitration may be pending, the parties hereto shall continue to be governed by and perform the work in accordance with the provisions of this Agreement to ensure continuity of operations.

- f) This Clause shall survive the termination/ expiration/ special cancellation/ invalidity of this Agreement.

33. LIMITATION OF THE SELECTED BIDDER'S LIABILITY TOWARDS GIC RE

The Selected Bidder, with respect to damage caused by the Selected Bidder to GIC Re's property, shall not be liable to GIC Re for any indirect or consequential loss or damage; and shall not be liable to GIC Re for any direct loss or damage that exceeds the total of:

- a) payments payable under this Agreement to the Selected Bidder, i.e., 100% of the Contract Price, and
- b) the proceeds the Selected Bidder may be entitled to receive from the insurance maintained by the Selected Bidder to cover such a liability,

This limitation of liability shall not affect the Selected Bidder's liability, if any, for damage to Third Parties caused by the Selected Bidder or any person acting on behalf of the Selected Bidder in carrying out the Services.

Nothing in these terms shall exclude or limit the liability of the Selected Bidder in the case of:

- a) death or personal injury resulting from the Selected Bidder's or Selected Bidder's Team's negligence.
- b) Negligence and Willful Misconduct.
- c) fraud.
- d) breach of Confidentiality provisions and the NDA.
- e) indemnification provisions in this Agreement.
- f) or other liability to the extent that the same may not be excluded or limited as a matter of law.

34. CONFLICT OF INTEREST

The Selected Bidder shall disclose to GIC Re in writing, all actual and potential conflicts of interest that exist, arise, or may arise (either for the Selected Bidder or the Selected Bidder's Team) while performing the Services as soon as practical after it becomes aware of that conflict.

35. SEVERANCE

In the event any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, then the remaining provisions of this Agreement will nevertheless remain in full force and effect. The Parties agree to negotiate in good faith a substitute, valid and enforceable provision which most nearly effects the Parties' intent in entering into this Agreement.

36. GOVERNING LANGUAGE

The Agreement shall be written in English language. All correspondence and other documents pertaining to this Agreement that are exchanged by the Parties shall be written in English language only.

37. PUBLICITY

The Selected Bidder agrees not to advertise, publish, or disclose the existence or terms of this Agreement or that it has contracted to furnish the services described in this Agreement, without the prior written consent of GIC Re. In particular, the Selected Bidder shall not make or permit to be made a public announcement or media release about any aspect of this Agreement including its existence unless GIC Re first gives the Selected Bidder its written consent.

38. FORCE MAJEURE

- a) The failure or occurrence of a delay in performance of any of the obligations of either Party shall constitute a Force Majeure event only where such failure or delay could not have reasonably been foreseen, or where despite the presence of adequate and stipulated safeguards the failure to perform obligations has occurred. This would include natural and unavoidable catastrophes that interrupt the expected course of events which may include, but are not restricted to, instances of wars or revolutions, fires, floods, epidemics, quarantine restrictions, freight embargoes and any event or circumstance of a nature analogous to any of the foregoing which would have an impact on GIC Re. In such an event, the affected party shall inform the other Party in writing within 15 days of the occurrence of such event. GIC Re will make the payments due for Services rendered till the occurrence of Force Majeure. However, any failure or lapse on the part of the Selected Bidder in performing any obligation as is necessary and proper, to negate the damage due to projected force majeure events or to mitigate the damage that may be caused due to the abovementioned events or the failure to provide adequate disaster management/ recovery or any failure in setting up a contingency mechanism would not constitute force majeure, as set out above.
- b) Force Majeure shall not include any events caused due to acts/ omissions of any Party or result from a breach/ contravention of any of the terms of the RFP/ Bids, and this Agreement. It shall also not include any default on the part of a Party due to its negligence or failure to implement the stipulated/ proposed precautions, as were required to be taken under this Agreement.
- c) In case of a Force Majeure, all Parties will endeavor to agree on an alternate mode of performance to ensure the continuity of service and implementation of the obligations of a Party under this Agreement and to minimize any adverse consequences of Force Majeure.

39. RELATIONSHIP BETWEEN GIC RE AND THE SELECTED BIDDER

- a) The relationship between the Parties shall be that of independent contractor and contractee. Nothing in this Agreement constitutes any fiduciary relationship between GIC Re and Selected Bidder/ Selected Bidder's Team or any relationship of employer employee, principal and agent, or partnership or joint ventures, between GIC Re and the Selected Bidder.
- b) No Party has any right or authority either express or implied to bind the other Party in any manner whatsoever except as agreed under the terms of this Agreement or to assume or create any obligation or responsibility on behalf of the other.
- c) GIC Re has no obligations to the Selected Bidder or the Selected Bidder's Team except as agreed under the terms of this Agreement.
- d) The Selected Bidder shall comply with all laws, rules, and regulations applicable to the Services being procured hereunder and all applicable laws, rules, and regulations to which it may be subject from time to time.
- e) However, if due to any deeming fiction or if the law otherwise provides for a situation where GIC Re may be held vicariously or otherwise liable for acts of Selected Bidder, the Selected Bidder shall protect, indemnify and hold harmless GIC Re in respect of any losses, costs, damages whether direct or indirect arising out of the failure, omission or non-observance of any laws, rules or regulations which it was expected to comply with hereunder or any act of the Selected Bidder which as a reasonable entity, it should not have committed.

40. NO ASSIGNMENT

The Selected Bidder shall not transfer any interest, right, benefit or obligation under this Agreement without the prior written consent of GIC Re and any purported attempt to do so shall be deemed void.

41. SUB-CONTRACTING

In case sub-contracting is required, the Selected Bidder shall seek prior written permission and submit the list of subcontractors to GIC Re for its approval in writing in sufficient time so as not

to impede the progress of work.

If such approval is granted, the Selected Bidder shall ensure that the sub-contractor(s) comply with all the requirements of this RFP and Agreement.

Such approval by GIC Re of a sub-contractor(s) shall not relieve the Selected Bidder from any of its obligations, duties, or responsibilities under this Agreement and the Selected Bidder shall be liable to GIC Re for all the Services under this Agreement, including Services performed by any such Sub-Contractor. To the fullest extent possible under applicable law, the Selected Bidder shall be liable to GIC Re for the acts, omissions, Negligence, Willful Misconduct, fraud, bad faith, or breach of any sub-contractor(s) in connection with this Agreement.

Any such sub-contractor(s) shall remain liable to GIC Re for the due performance of this Agreement and GIC Re may bring any claim in any way in respect of or in connection with this Agreement against any such sub-contractor(s).

42. ENTIRE CONTRACT/ AGREEMENT

The terms and conditions laid down in the RFP and the Bids of the Selected Bidder shall be read in consonance with and form an integral part of this Agreement and shall together constitute the entire Contract/ Agreement. This Agreement supersedes any prior Contracts/ agreements, understanding or representation of the Parties on the subject matter.

43. GOVERNING LAW

The validity, construction and performance of this Agreement shall be governed by and construed in accordance with the laws of India.

44. JURISDICTION OF COURTS

Subject to the Dispute Resolution clause, the courts of India at Mumbai have exclusive jurisdiction to determine any proceeding in relation to this Agreement.

45. COMPLIANCE WITH LAWS

The Selected Bidder shall comply with the laws in force in India while performing this Agreement.

46. NOTICES

A “notice” means:

- i. a notice; or
- ii. other communication required to be in writing under this Agreement.

All notices, requests or consents, permissions, approvals, or other communications provided for or permitted to be given under this Agreement shall be in writing and shall be deemed effectively given when personally delivered or mailed by pre-paid certified/ registered mail, return receipt requested, addressed as follows and shall be deemed received two days after mailing or on the date of delivery if personally delivered to:

To GIC Re, at:
ITMG,
General Insurance Corporation of India,
Suraksha, 170, J Tata Road, Churchgate,
Mumbai – 400020.
Phone: 022-22867124/ 158

To Selected Bidder at:
<Name:>
<Address:>

<Phone:>

<Email:>

Notice via Email: Notice is a notice as defined above or scanned copy of a notice, where sent by email to official email id of Authorized Representative as per clause “Agreement Administration” or ITMG Team, on the date that the email is received. However, if the time of deemed receipt of any notice is not before 5.45 p.m. IST on a Business Day at the address of the recipient it is deemed to have been received at the commencement of business on the next Business Day.

There shall be no retrospective effect to any notices served.

Any Party may change the address to which notices are to be directed to it by notice to the other party in the manner specified above. A notice served on a Representative as per clause “Agreement Administration” is taken to be notice to that Representative’s Party

47. WAIVER

- a) Any waiver of any provision of this Agreement is ineffective unless it is in writing and signed by the Party waiving its rights.
- b) A waiver by either Party in respect of a breach of a provision of this Agreement by the other Party is not a waiver in respect of any other breach of that or any other provision.
- c) The failure of either Party to enforce at any time any of the provisions of this Agreement shall not be interpreted as a waiver of such provision.

48. MODIFICATION

Any modification of this Agreement shall be in writing and signed by an authorized representative of each Party and annexed to the Agreement as addendum.

49. CO-OPERATION

Each party to this Agreement agrees to execute and deliver all documents and to perform all further acts and to make all further steps that may be reasonably necessary to carry out the provisions of this Agreement and transactions contemplated thereby.

50. SURVIVAL

Notwithstanding any expiration or termination of this Agreement, the provisions of this Agreement that are either by express language meant to survive or impliedly meant to survive termination, shall survive such expiration or termination.

51. ANTI-FRAUD AND CORRUPTION

It is the GIC Re’s policy that GIC Re as well as the Selected Bidder observe the highest standard of ethics and propriety during the procurement process, execution of the contract, the contract duration and thereafter (hereinafter referred to as the ‘Contract Cycle’).

Definitions:

In pursuance of this policy, GIC Re defines, for the purpose of this provision, the terms set forth below as follows:

- a) “Corrupt Practice” means the offering, promising, giving, receiving, or soliciting, directly or indirectly, anything of value, either tangible or intangible, which a person is not entitled to, to influence or which has the potential to influence the action of an official during the Contract Cycle.
- b) “Fraudulent Practice” means the following:
 - a misrepresentation or omission of facts or submission of fake or forged documents to

influence any component of the Contract Cycle.

- an intentional act of commission or omission designed to deceive, resulting in GICRe suffering a loss and/ or the perpetrator achieving a gain.
- c) “Collusive Practices” means a scheme or arrangement whether formal or informal, between two or more Bidders, with or without the knowledge of the GIC Re, designed to establish prices at an artificial, noncompetitive levels or which affects submission or non - submission of bids; Similar clauses seen in documents released by NBCC, SBI, Govt. Ministries and UN organizations.
- d) “Coercive Practices” means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in a procurement process or affect the contract cycle.

Misdemeanor for this purpose shall include Corrupt, Fraudulent, Collusive and Coercive practices which shall carry meanings as per the definitions above.

Measures to be taken by GIC Re:

- a) GIC Re will be within its rights to terminate this Agreement with the Selected Bidder for any Misdemeanor during the Contract Cycle, ban/ blacklist/ debar the Selected Bidder from this and further procurements and the like.
- b) GIC Re will be within its rights to take any other action against the Selected Bidder deemed appropriate as per the terms of the RFP and this Agreement as well as the law of the land.

Measures to be taken by the Selected Bidder:

- a) The Selected Bidder shall during the entire Contract cycle, comply with the provisions of the Anti-Fraud Policy of GIC Re and not commit any Misdemeanor.
- b) The Selected Bidder shall procure the compliance with the above obligations (as mentioned in a.) from its associated persons, officers, employees, agents, subcontractors, or independent contractors as may be used for the fulfilment of its obligations under the RFP and this Agreement during the entire Contract cycle.
- c) The Selected Bidder undertakes that the Selected Bidder shall be responsible to GIC Re for the Misdemeanors and non-compliance of the Anti-Fraud Policy committed by the above-named persons during the entire Contract cycle.
- d) If the Selected Bidder gains knowledge of any conduct by any of its associated persons, officers, employees, agents, subcontractors, or independent contractors which constitutes a Misdemeanor or non-compliance of the Anti-Fraud Policy, or if it has reasonable suspicion of the existence of such conduct, it shall immediately inform GIC Re of such knowledge and if requested by GIC Re, provide information it may reasonably require regarding such conduct.

IN WITNESS WHEREOF, the parties have caused this Agreement to be duly executed as of the day and year first written above.

For and on behalf of General Insurance Corporation of India by:

Name:

Title:

Date:

In presence of (Witnesses)

(i)

(ii)

For and on behalf of “Service provider ’s Name” by:

Name:

Title:

Date:

In presence of (Witnesses)

(i)

(ii)

ANNEXURE VI
PERFORMANCE BANK GUARANTEE

(Stamp paper/ Franking to be done by bank for value of ₹500/-)

Bank Guarantee No.....

Date.....

To,
General Insurance Corporation of India,
170, "Suraksha",
J. Tata Road,
Churchgate,
Mumbai 400020.

In consideration of the **General Insurance Corporation of India**, a company registered under the Companies Act 1956, and having its registered office at 170, "Suraksha", 170, J. Tata Road, Mumbai 400020 (hereinafter called 'Corporation'), which expression shall, unless it be repugnant to the meaning and context thereof, include its successors, administrators, executors and permitted assigns having entered into an agreement dated _____ for the **"RFP for Hosting and Management of GIC Re Hybrid Cloud Infrastructure"** (hereinafter called "the Agreement") with _____ having its registered office at _____ (hereinafter called the said "Selected Bidder" which expression shall, unless it be repugnant to the meaning and context thereof, include its successors, administrators, executors and permitted assigns) and the Selected Bidder having agreed to provide a guarantee for its performance in the form of an unconditional, irrevocable and continuing Performance Bank Guarantee as per the terms and conditions of the Request for Proposal No. **GICRE/ITMG/RFP/05/2021-22** dated **22nd March 2022**.

(Hereinafter referred to as "the RFP") and the Agreement, for the due fulfillment by the Selected Bidder of the terms and conditions contained in the RFP, the Selected Bidder's Technical bid and the Agreement,

1. We, _____ (Name of the bank and full registered office address) (hereinafter called the "Bank"), at the request of _____ (Name of Selected Bidder/s) do hereby guarantee and undertake to issue this Performance Bank Guarantee (hereinafter called "this Guarantee") and to pay to the Corporation on its first written demand all monies payable by the Selected Bidder to the extent of an amount not exceeding ₹ (Rupees only) at any time without any cavil, demur, reservation, contest, argument, recourse or protest and /or without any reference to the Selected Bidder and without the Corporation needing to prove or to show grounds or reasons for demand for the sum specified therein.
2. We, _____ (Name of the bank and full address), do hereby undertake to pay the amounts due and payable under this Guarantee without any demur, merely on a demand from the Corporation stating that the amounts claimed is payable. Any such demand made on the Bank shall be conclusive as regards the amount due and payable by the Bank under this Guarantee. However, our liability under this Guarantee shall be restricted to an amount not exceeding ₹ ____/ (Rupees only).
3. We, _____ (Name of the bank and full address), undertake to pay to the Corporation any money so demanded not exceeding ₹ ____/ (Rupees only) and any such demand made on us by the Corporation shall be conclusive and binding notwithstanding any difference between the Corporation and the Selected Bidder or dispute raised by the Selected Bidder whether or not in any suit or proceeding pending before any court, tribunal, arbitrator or any authority, our liability under this Guarantee being absolute and unequivocal.
The Payment so made by us under this Guarantee shall be a valid discharge of our liability for payment hereunder and the Selected Bidder shall have no claim against us for making such

payment.

4. We, _____ (Name of the bank and full address), further agree that this Guarantee herein contained shall remain in full force and effect during the entire tenure of the said Agreement and till 60 days after all the contractual obligations (including warranty obligations) of the Selected Bidder under the said Agreement, the Selected Bidder's technical bid and Corporation's RFP dated **22nd March 2022** are completed and that it shall continue to be enforceable till all the dues of the Corporation be under or by virtue of the Corporation's RFP or the said Agreement have been fully paid and its claim authorities satisfied or discharged by the said Selected Bidder.

Unless a claim or demand under this Guarantee is made or presented to the Bank within 12 months from the expiry date of this Guarantee, all the rights of the Corporation under this Guarantee shall cease, and the Bank shall be released and discharged from all liability hereunder.

5. We, _____ (Name of the bank and full address), further agree with the Corporation that the Corporation shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said Agreement or Scope of Work as specified in the Selected Bidder's technical bid or the Corporation's RFP, or to extend the time of performance of the said Selected Bidder from time to time to postpone for any time or from time to time the exercise of powers vested in the Corporation or any rights that the Corporation may have against the said Selected Bidder or to forbear or enforce any of the terms and conditions relating to the said Agreement or any other course or remedy or security available to the Corporation. We shall not be relieved from our liability under this Guarantee by any exercise by the Corporation of its liberty with reference to the matters aforesaid or any of them or by any reason of any other act or forbearance of other acts or omission or commission on the part of the Corporation or any other indulgence shown by the Corporation or by any such matter or thing whatsoever which under the law would but for this provision, have effect of so relieving us. We further agree to waive notice of any such change, addition, or modification or other acts mentioned above.
6. Any claim which we, _____ (Name of the bank and full address), have against the Selected Bidder shall be subject and subordinate to the prior payment and performance in full of all the obligations of it hereunder. The Bank will not, without prior written consent of the Corporation, exercise any legal right or remedy of any kind in respect of any such payment or performance so long as the obligations hereunder remain owing and outstanding regardless of the insolvency, liquidation, or bankruptcy of the Selected Bidder or otherwise howsoever. We, the Bank, will not counter claim or set off against our liabilities to the Corporation hereunder any sum outstanding to the credit of the Corporation with us.
7. This Guarantee will not be discharged due to the change in the name, constitution or address of the Bank, the Corporation or the Selected Bidder. We further agree that no change or addition to or other modification of the terms of the Agreement or Scope of Work for (the subject matter of procurement) which may be made between GIC Re and the Selected Bidder, shall in any way release us from any liability under this Guarantee and we hereby waive notice of any such changes, addition, or modification.
8. We, _____ (Name of the bank and full address), undertake not to revoke this Guarantee during its currency except with the prior consent of the Corporation in writing.
9. Notwithstanding anything to the contrary contained herein:
1. Our liability under this Bank Guarantee shall not exceed ₹ _____
/- (Rupees only),
 2. This Bank Guarantee shall come into force immediately and shall be valid up to and including [dd/mm/yyyy] _____ (being the date of expiry date of Guarantee),
 3. The Corporation's right as well the Bank's liability under this Guarantee shall stand extinguished unless a written claim or demand is made under this Guarantee on or before completion of one year (12 months) from the date of expiry of this Guarantee i.e., on or before [dd/mm/yyyy].
4. Our obligation to pay under this Guarantee is as principal debtor and not as surety and it shall

not be necessary for the Corporation “to proceed against” the said Selected Bidder “before proceeding against” the Bank and the Guarantee shall be enforceable against the Bank notwithstanding any other security or Guarantee which the Corporation may have obtained or may obtain from the Selected Bidder at the time when proceedings are taken against the Bank in any manner whatsoever.

10. We have the power to issue this Guarantee in your favor and Shri _____ is executing this Guarantee on our behalf, has the necessary power to do so on behalf of the Bank.
11. This Guarantee shall be irrevocable and the obligations of us herein shall not be conditional of any prior notice by us.

Date:day of, 2022

For _____ (Name of the bank)

(Signature of the authorized officer of the Bank)

Name and designation of the officer

Seal, name & address of the Bank

Witnesses:

1.

Signature

Name

Designation

Official Address

2.

Signature

Name

Designation

Official Address

ANNEXURE VII RECIPROCAL NON-DISCLOSURE AGREEMENT

(Notary to be done on a stamp paper of value ₹500/-)

This Reciprocal Non-Disclosure Agreement (hereinafter referred to as “NDA”) is entered into on this _____ day of _____ 2022, by and between:

_____, a Company incorporated under the Companies Act, 1956/ 2013, having its registered office at _____, hereinafter referred to as “Selected Bidder” which expression shall, unless it be repugnant to the meaning and context thereof, include its successors, and permitted assigns of the one part;

and

General Insurance Corporation of India, a company duly incorporated and existing under the laws of India, having its registered office at “Suraksha”, 170, J. Tata Road, Churchgate, Mumbai – 400020, India, hereinafter referred to as “GIC Re” which expression shall, unless it be repugnant to the meaning and context thereof, include its successors and permitted assigns of the other part

Hereafter, referred to individually as a **“Party”** and collectively as the **“Parties”**. For purposes of this NDA, the party receiving Confidential Information (as defined herein below), shall be referred to as the **“Receiving Party”** and the party providing the Confidential Information shall be referred to as the **“Disclosing Party”**.

WHEREAS the Selected Bidder is *inter alia* engaged in the business of Hosting and Management of GIC Re Hybrid Cloud Infrastructure from _____.

AND WHEREAS, GIC Re is engaged in the business *inter alia*, of Reinsurance and Risk Management related activities.

AND WHEREAS Selected Bidder and GIC Re are in the process of consultations and discussions for exploring business opportunities as per the Scope of Work under GIC Re’s Request for Proposal (RFP) No. **GICRE/ITMG/RFP/05/2021-22** dated **22nd March 2022** and to eventually enter into a detailed Agreement for the same. (“Purpose”)

AND WHEREAS to facilitate the Purpose, certain Confidential Information (as defined below) will be required to be shared between the Parties.

AND WHEREAS, the Parties wish to protect the Confidential Information (as defined herein below) from any unauthorized use or disclosure in accordance with the terms and conditions of this NDA.

NOW, THEREFORE, in consideration of the promises and covenants contained it is agreed as follows:

A. Definition of “Confidential Information”

- a) **“Confidential Information”** means any information disclosed to, received by, otherwise accessed by, or coming to the knowledge of the Receiving Party to this NDA, either orally or in writing, whether disclosed directly or indirectly that:
 - is by its character or nature or by the circumstances in which it is disclosed/received/ assessed

and/or it came to knowledge, such that a reasonable person under like circumstances would treat it as confidential; or

- is designated by the Disclosing Party as confidential or identified in terms connoting its confidentiality; or
- is proprietary to the Disclosing Party and not generally known to the public, whether in tangible or intangible form, whenever or however disclosed; or
- the Disclosing Party considers confidential.

and includes but is not limited to, the following types of information and other information of a similar nature (whether or not reduced to writing): discoveries; inventions; concepts; software in various stages of development; designs; drawings; flowcharts; specifications; techniques; models; data; database; source code; object code; documentation; methods; processes; policies; procedures; information related to processes; technologies or theory; know-how; marketing techniques and materials; marketing and development plans; business plans; strategic plans; development tools; reports; business records; project records; projections; performance results related to past, present or future business activities of Disclosing Party, its affiliates, subsidiaries and affiliated companies; business manuals; customer/Selected Bidder names and other information related to customers/Selected Bidders, price lists, pricing policies; financial information; and any scientific or technical or commercial information, information and trade secrets;

- b) Confidential Information also includes information disclosed to the Receiving Party by third parties on behalf of the Disclosing Party.
- c) Confidential Information shall include any copy, abstract, extract, sample, note or module of any Confidential Information and any part or any extract or summary or derivation thereof.

B. Obligation of receiving party:

Receiving Party promises and agrees to hold the confidential information received from the Disclosing Party in confidence.

Receiving Party shall not use Confidential Information, the name, or the logo of the other party except for the purpose of this Agreement.

Disclosure of confidential information by Employees or hired institutions or authorized agents of the Receiving party will be deemed as the act by the Receiving Party, thereby, subjecting them to same liability under this NDA.

C. Information not categorized as “Confidential Information”

The obligation imposed, under this NDA, on Receiving Party shall not apply to information which:

- a) Receiving Party can demonstrate by prior existing records, was within Receiving Party's legitimate possession prior to the time of disclosure by the Disclosing Party and without restriction as to use or disclosure.
- b) was within the public domain/ public knowledge prior to disclosure by the Disclosing Party or comes into the public domain/ public knowledge through no wrongful act, fault, negligence, or breach of this NDA on the part of the Receiving Party.
- c) is independently developed by the Receiving Party without use of, reference to or reliance upon Confidential Information of the Disclosing Party.
- d) is or becomes lawfully available to Receiving Party on a non-confidential basis from an independent third-party source (after diligent inquiry) who is free to divulge such information without restriction as to use or disclosure.

Provided, the Receiving Party understands and agrees that:

- i. Any information known only to a few people to whom it might be of commercial interest and not generally known to the public is not public domain/ public knowledge.
- ii. A combination of two or more parts of the Confidential Information is not public knowledge merely because each part is separately available to the public.

D. Restriction on Disclosure

Except as otherwise expressly permitted under this NDA, the Receiving party shall hold and keep in strictest confidence all Confidential Information and shall not directly or indirectly, in any way:

- a) disclose, reveal report, publish, duplicate, copy, transmit or otherwise use or disseminate in any manner whatsoever any Confidential Information of the Disclosing Party.
- b) use the Confidential Information of the Disclosing Party (i) for Receiving Party's own benefit or that of any third party, (ii) to the Disclosing Party's detriment, or (iii) for any purpose other than for achieving the Purpose.
- c) commercially exploit any Confidential Information of the Disclosing Party.
- d) acquire any right in, or assert any lien against, the Confidential Information of the Disclosing Party; or
- e) refuse for any reason to promptly return all Confidential Information of the Disclosing Party if instructed to do so.

E. Permitted Disclosures

Receiving Party is permitted to:

- a) disclose relevant aspects of the Disclosing Party's Confidential Information to the Receiving Party's directors, officers, employees, consultants, attorneys, and auditors solely to the extent necessary for achieving the Purpose; provided, that
 - (1) before disclosing any Confidential Information of the Disclosing Party, all persons or entities receiving Confidential Information shall be bound by obligations of confidentiality towards the Disclosing Party no less restrictive than those of this NDA. Such persons shall be strictly prohibited from making any use, publishing, or otherwise disclosing to others, or permitting others to use for their benefit or to the detriment of the Disclosing Party, any of the Confidential Information.
 - (2) The Receiving Party shall use the same care to avoid disclosure or unauthorized use of Confidential Information as it uses to protect its own confidential information, but in no event less than reasonable care including but not limited to execution of a confidentiality agreement with the persons or entities receiving Confidential Information. Receiving Party shall establish and maintain reasonable security measures to provide for the safe custody of the Confidential Information and to prevent unauthorized access to the Confidential Information.
 - (3) All such Confidential Information shall be labeled as confidential.
- b) Disclose relevant aspects of the Disclosing Party's Confidential Information if and to the extent legally compelled or required order of a court of competent jurisdiction to disclose any Confidential Information of the Disclosing Party in connection with any legal or regulatory proceedings. In such case, the Receiving Party will immediately notify the Disclosing Party to allow the Disclosing Party a reasonable opportunity to seek appropriate protective measures or other remedies prior to disclosure or waive compliance with the terms of this NDA. The Receiving Party shall cooperate with any attempt by the Disclosing Party to seek judicial protection for such Confidential Information
- c) Disclose relevant aspects of the Disclosing Party's Confidential Information with the prior written consent of the Disclosing Party.

F. Effects of Unauthorized Disclosure

- a) The Receiving Party will be liable for the breach of, acts and omissions of, and any loss, theft or unauthorized/inadvertent disclosure or use of Confidential Information by, any person or entity that received Confidential Information from or through the Receiving Party.
- b) Receiving Party acknowledges and agrees that the misappropriation or misuse of Confidential Information of the Disclosing Party will result in irreparable and continuing damage to the Disclosing Party for which there may be no adequate remedy at law. In the event of such a breach by the Receiving Party leads to Disclosing Party suffering or incurring losses, damages, claims or expenses, the Disclosing Party shall be entitled to liquidated damages and

legal as well as equitable relief, as appropriate, including but not limited to an injunction, in addition to any monetary relief in the form of indemnification.

- c) The Receiving Party will promptly report to the Disclosing Party any disclosures of Confidential Information otherwise than as permitted by this NDA and any breaches in security that may or has the potential to affect the Disclosing Party or its Confidential Information of which it is aware and will specify the corrective action to be taken.

G. Return of documents

Upon written demand by the Disclosing Party, the Receiving Party shall promptly and in any event within 14 days of receipt of such request, at its own cost:

- a) procure the return or return to the Disclosing Party all Confidential Information supplied which the Receiving Party has in his possession or under his control which includes but is not limited to all tangible material embodying the Confidential Information provided, every copy of Confidential Information and copies that have been converted to computerized media in the form of image, data or word processing files whether manually or by image capture or in any other form of storage; and
- b) destroy or have destroyed all copies received or made of the Confidential Information to the extent Confidential Information is held in non-tangible form (e.g., electronic copies); and
- c) promptly thereafter provide a certificate signed by an Authorized Representative of the Receiving Party certifying compliance with the obligations point (a) and (b) above.

H. Title and Proprietary Rights

Notwithstanding the disclosure of any Confidential Information by the Disclosing Party to the Receiving Party, the Disclosing Party shall retain exclusive title and all intellectual property and proprietary rights in the Confidential Information. The Receiving Party acknowledge that all Confidential Information is owned solely by the Disclosing Party and/or its licensors. No other right, title, license, or interest is granted by a Disclosing Party to a Receiving Party aside from the right specifically granted by this NDA. No license under any trademark, patent or copyright or application for same which are now or thereafter may be obtained by Disclosing Party is either granted or implied by the conveying of Confidential Information. The Receiving Party shall not conceal, alter, reverse-engineer, decompile, disassemble, obliterate, mutilate, deface, or otherwise interfere with any software, trademark, trademark notice, copyright notice, confidentiality notice or any notice of any other proprietary right of the Disclosing Party on any copy of the Confidential Information, and shall reproduce any such mark or notice on all copies of such Confidential Information. Likewise, the Receiving Party shall not add or emboss its own or any other mark, symbol, or logo etc. on such Confidential Information.

I. No Warranty

The parties warrant that they have the full legal rights required to provide the Confidential Information provided hereunder. All other warranties, express or implied, including but not limited to the implied warranty of merchantability or fitness for a particular purpose are expressly disclaimed. Except for the express warranty provided herein. All Confidential Information is provided “as is” and without warranty of any other nature. In no event shall the Disclosing Party be liable for the inaccuracy or incompleteness of the Confidential Information. None of the Confidential Information disclosed constitutes any representation, warranty, assurance, guarantee or inducement by Disclosing Party to the Receiving Party with respect to the fitness of such Confidential Information for any particular purpose.

J. No Commitment

The disclosure of Confidential Information does not and is not intended to represent a commitment by the Disclosing Party to enter any business relationship with the Receiving Party or with any other entity under this NDA. If the Parties desire to pursue business opportunities,

they shall execute a separate written Agreement to govern such Business relationship.

K. Term

This NDA shall commence from the date set forth above and expire with the termination or expiration of the agreement unless earlier terminated in writing by both Parties. This NDA may be terminated by either Party at any time upon thirty (30) days written notice to the other Party. The provisions of this NDA shall however apply to any Confidential Information which may have been disclosed in connection with the discussions and negotiations regarding the Purpose, prior to the date first mentioned above.

Notwithstanding the foregoing, the Receiving Party's duty to hold in confidence the Confidential Information that was disclosed during the Term and the obligations under this NDA shall always remain in effect and shall survive any termination/expiry of this NDA or the Agreement.

L. Arbitration

The Arbitration proceeding shall be as per the procedure laid down in the SLA (**Annexure V**).

M. Governing Law and Jurisdiction

- a) The validity, construction and performance of this NDA shall be governed by and construed in accordance with the laws of India.
- b) Subject to the provisions of Arbitration clause, the Parties agree to submit to the jurisdiction of a court of competent jurisdiction at Mumbai, India and to comply with all requirements necessary to give such court the jurisdiction.

N. Miscellaneous

- a) No failure or delay by the Disclosing Party in exercising or enforcing any right, remedy or power hereunder shall operate as a waiver thereof, nor shall any single or partial exercise or enforcement of any right, remedy or power preclude any further exercise or enforcement thereof or the exercise or enforcement of any other right, remedy or power.
- b) This NDA shall not be assignable or transferable (entirely or in part) by either Party (whether by operation of law, sale of securities or assets, merger or otherwise) to any third party without the written consent of the other Party.
- c) This NDA supersedes all prior discussions, agreements, covenants, arrangements, communications, representations, or warranties, whether oral or in writing by any of the parties or by any officer, employee, or representative of any party with respect to the subject matter hereof and constitutes the entire agreement between the Parties with respect to the subject hereof.
- d) No waiver or modification of any of the terms of this NDA will be valid or binding upon either Party unless made in writing and signed by a duly authorized representative of each Party.
- e) If any of the provisions of this NDA shall be held by a Court or other tribunal of competent jurisdiction to be unenforceable; the remaining portions hereof shall remain in full force and effect.
- f) Upon 45 days written notice, the Disclosing Party may audit the use of the disclosed Confidential Information. The Receiving Party agrees to co-operate with the Disclosing Party's audit and to provide reasonable assistance and access to information.
- g) The Receiving Party shall not export, directly or indirectly, any technical data acquired from the Disclosing Party pursuant to this NDA or any product utilizing any such data to any country for which the Indian government or any agency thereof at the time of export requires an export license or other government approval without first obtaining such license or approval.
- h) Any notices or communications required or permitted to be given hereunder may be delivered by hand, deposited with a nationally recognized overnight carrier, electronic mail,

or mailed by certified mail, return receipt requested, postage prepaid, in each case to the address of the other party indicated below. All such communications and notices shall be deemed to have been given and received

- ii. in the case of personal delivery or electronic mail, on the date of such delivery,
- iii. in case of delivery by a nationally recognized overnight carrier and in mailing, within a reasonable period of such mailing.

IN WITNESS WHEREOF this NDA has been executed by the duly authorized representative of each Party on the day and year first above written.

By: _____

Name: _____

Title: _____

GENERAL INSURANCE CORPORATION OF INDIA

By: _____

Title: _____

Date: _____

ANNEXURE VIII
DEED OF INDEMNITY

(To be on non-judicial stamp paper worth minimum ₹500/-)

This Deed of Indemnity is made and executed at Mumbai on this _____ day of _____ 2022 by _____, a Company incorporated under the Companies Act 1956/ 2013, having its registered office at, _____ (hereinafter referred to as "the Selected Bidder"), which expression shall, unless it be repugnant to the meaning and context thereof, include its successors and permitted assigns of the First part

In favor of

General Insurance Corporation of India, having its registered office at Suraksha, 170, J. Tata Road, Church gate, Mumbai- 400020 (hereinafter referred to as "GIC Re"), which expression shall, unless it be repugnant to the meaning and context thereof, include its successors and permitted assigns of the other part.

WHEREAS the Selected Bidder has agreed with GIC Re to successfully provide services as per the Scope of Work mentioned in the RFP Ref _____ dated _____ (hereinafter referred to as "RFP") which expression shall include all attachments and annexures thereto as well as all amendments, modifications, alterations, and the Bids submitted by the Selected Bidder and the Terms and Conditions agreed as per the agreement dated _____ (hereinafter referred to as "the Agreement"). and the Non - Disclosure Agreement dated _____ (hereinafter referred to as "NDA").

AND WHEREAS pursuant to the RFP/ Agreement, the Selected Bidder is required to execute a Deed of Indemnity in favor of GIC Re to indemnify it.

The Selected Bidder hereby executes and furnishes to GIC Re this Deed of Indemnity (hereinafter referred to as "this Indemnity"), which is an unlimited, unconditional, irrevocable, and continuing indemnity, indemnifying GIC Re to the extent of 100% in respect of the situations stated hereinafter:

NOW THIS DEED WITNESSETH AS UNDER:

1. The Selected Bidder shall indemnify, defend, and hold GIC Re harmless from and against any monetary liability (including but not limited to loss, charge, claim, fines, penalties, damages, expense, fees etc. of any nature) or non-monetary action (including but not limited to civil, criminal, administrative, arbitral or any other proceeding) arising out of or in any way connected with the Selected Bidder's performance of this RFP/ Agreement/ NDA.
2. In addition to the general indemnification provided in clause 1 above, The Selected Bidder hereby undertakes to indemnify GIC Re as per the terms and conditions of the RFP/ Agreement including that:
 - a) The Selected Bidder warrants that it shall procure all the necessary permissions, approvals, and licenses for use of various software and any copyrighted process/product free from all claims, titles, interests, and liens thereon and shall keep GIC Re indemnified in relation thereto.
 - b) The Selected Bidder warrants that it owns, has license to use or otherwise has the right to use, free of any pending or threatened liens or other security or other interests all its intellectual property rights, which are required or desirable for performance of its Services under the RFP/ Agreement and regarding the same the Selected Bidder does not, as far as the Selected Bidder is aware, in carrying on its business and operations, infringe any Intellectual Property Rights of any person. So far as the Selected Bidder is aware, none of the Intellectual Property Rights, owned or enjoyed by the Selected Bidder or which the Selected Bidder is licensed to use, which are material in the context of Selected Bidder's business and operations for the performance of the RFP/ Agreement are being infringed nor, so far as the Selected Bidder is aware, is there any infringement or threatened infringement of those Intellectual Property

Rights licensed or provided to the Selected Bidder by any person. The Selected Bidder warrants that all Intellectual Property Rights (owned by the Selected Bidder or which the Selected Bidder is licensed to use) required by the Selected Bidder for the performance of the Agreement are valid and subsisting. All actions (including registration, payment of all registration and renewal fees) required to maintain the same in full force and effect have been taken thereon. The Selected Bidder shall keep GIC Re indemnified in relation to any breach of the warranties in this clause.

- c) The Selected Bidder warrants that during the tenure of the Agreement, nothing shall be done by the Selected Bidder in contravention of any law, Acts, or rules and regulations, or any amendments thereof and shall keep GIC Re, indemnified in case of breach of this warranty.
- d) The Selected Bidder shall adhere to the Information Security Policy of GIC Re as amended from time to time. In case the Selected Bidder is found to be in violation of the said policy, GIC Re reserves the right to terminate this Agreement in addition to any other remedies for breach, injunctive relief, and indemnity as per this Agreement and the applicable laws.

3. In addition to the indemnification provided in clause 1 and 2 above, the Selected Bidder hereby undertakes to indemnify GIC Re as per the terms and conditions of this Indemnity which are as follows:

- a) The Selected Bidder shall indemnify and hold harmless GIC Re against any costs, loss, damages, expense, claims whether on account of bodily injury, death, or damage to property (including any intellectual property claims) arising in favor of any person, corporation or other entity (including GIC Re and any third party) or liabilities of any kind howsoever suffered, arising or incurred inter alia during and after the Agreement period arising out of:
 - a. any Negligence or wrongful act or omission or Willful Misconduct by the Selected Bidder, the Selected Bidder's Team or any third party engaged by the Selected Bidder in connection with or incidental to the Agreement; or
 - b. any breach of any of the terms of, the RFP, Selected Bidder's Bids and the Agreement by the Selected Bidder, the Selected Bidder's Team or any third party engaged by the Selected Bidder.
 - c. performance or non-performance under the Agreement.
- b) In addition to the above the Selected Bidder shall always indemnify and hold harmless GIC Re against all claims by employees, worker, contractors, sub-contractors, suppliers, agent(s), employed, /engaged or otherwise working for the Selected Bidder, in respect claims of wages, salaries, remuneration, compensation or the like.

4. In addition to the indemnification provided in clause 1, 2 and 3 above, the Selected Bidder hereby undertakes to indemnify GIC Re as per the terms and conditions of the Non-Disclosure Agreement signed between GIC Re and the Selected Bidder which are as follows:

The Selected Bidder acknowledges and agrees that the misappropriation or misuse of Confidential Information of GIC Re will result in irreparable and continuing damage to GIC Re for which there may be no adequate remedy at law. In the event of such a breach by the Selected Bidder leads to GIC Re suffering or incurring losses, damages, claims, or expenses, GIC Re shall be entitled to legal as well as equitable relief, as appropriate, including but not limited to an injunction, in addition to any monetary relief in the form of indemnification.

5. Notwithstanding the above, Selected Bidder shall have no obligations with respect to any indemnity claim to the extent that the indemnity claim arises or results from:
- a) Selected Bidder's compliance with GIC Re's specific technical designs or instructions.
 - b) Inclusion in a service of any content or other materials provided by GIC Re.
 - c) Modification of a service after delivery by Selected Bidder to GIC Re if such modification was not made by or on behalf of the Selected Bidder, provided the modification is not in accordance with any applicable specifications or documentation provided by or on behalf of the Selected Bidder.

- d) Operation or use of some or all the service in combination with products, information, specification, instructions, data, materials not provided by or on behalf of the Selected Bidder,
 - e) Use of the services for any purposes for which the same has not been designed or developed or other than in accordance with any applicable specifications or documentation provided by or on behalf of the Selected Bidder.
 - f) GIC Re's failure to use any modification of the services furnished under the Agreement and communicated in writing in accordance with the requirements of clause 'Notices' of the Agreement including, but not limited to, corrections, fixes, or enhancements made available by the Selected Bidder.
6. The Selected Bidder hereby undertakes that it shall forthwith on demand and without demur pay to GIC Re such sum or sums that become payable under any of the clauses indemnifying GIC Re due to the default/defaults of the Selected Bidder or any third party associated with the Selected Bidder.
 7. Notwithstanding anything to the contrary in this Indemnity or in the Agreement, GIC Re's decision as to whether the Selected Bidder or any third party associated with the Selected Bidder has made any default/defaults or the amounts to which GIC Re is entitled by reason thereof will be binding on the Selected Bidder for the purpose of this Indemnity and the Selected Bidder shall not be entitled to ask GIC Re to establish its claims under this Indemnity but will pay the same, on demand, without any objection, provided always, the mutual rights under the Agreement shall not in any way be prejudiced by reason of such demand by GIC Re and payment by Selected Bidder under this Indemnity and the claims under the Agreement which shall be settled in accordance with the Agreement without prejudice to GIC Re's rights to demand immediately under this Indemnity and the Selected Bidder's liability to pay the same.
 8. To the extent the Selected Bidder maintains, at its expense, an insurance policy or policies providing liability insurance with respect to the acts or omissions covered by the Agreement/Indemnity, GIC Re shall be covered by such policy or policies, in accordance with its or their terms, to the maximum extent of the coverage available there under. The Selected Bidder shall perform all such actions to ensure coverage for GIC Re under such policy during the tenure of this Indemnity.
 9. This Indemnity shall be valid for the entire duration of the Agreement and any renewal or extension thereof and further for a period of 6 months thereafter and renewable thereafter whenever a claim as per this Indemnity arises. The Indemnity provisions shall survive any termination or expiration of the Agreement.
 10. GIC Re will have the fullest liberty from time to time to enforce or forbear from enforcing any of the terms & conditions of the Agreement and the Selected Bidder shall not be released from its liability under this Indemnity by the exercise of GIC Re's liberty with reference to the matters aforesaid or by reason of any time being given to the Selected Bidder or any forbearance, act or omission on GIC Re's part or any indulgence by GIC Re to the Selected Bidder or by any variations or modifications of the Agreement or any other act, matter or thing whatsoever on GIC Re's part.
 11. This Indemnity and the powers and provisions herein contained are in addition to and not by way of limitation or substitution for any other guarantee, indemnities hereto before, given to GIC Re by the Selected Bidder and this Indemnity does not revoke or limit such indemnities or guarantees.
 12. For this Indemnity, the words defined in the RFP/ Agreement but not defined herein shall have the same meaning as defined in the RFP/ Agreement.

IN WITNESS WHEREOF, the Selected Bidder has caused this Indemnity to be duly executed as of the day, month and year first written above.

Signed and delivered by within named: _____ (Selected Bidder)

By:

Name:

Title:

Date:

In the presence of:

- 1.
- 2.

ANNEXURE IX UNDERTAKING BY BIDDER

(TO BE SUBMITTED ON THE COMPANY LETTER HEAD)

To
General Insurance Corporation of India
Mumbai, India

Bid for “Hosting and Management of GIC Re Hybrid Cloud Infrastructure”

1. I/ We agree to abide by the terms and conditions of the RFP including all corrigendum/addendum issue, if any.
2. I/ We certify that we have never been involved in any illegal activity or financial frauds.
3. I/ We certify that the facts mentioned in our response to the RFP are true, complete, and correct to the best of my/our knowledge and belief. It is also certified that we are not blacklisted by any Government Department/ any State Governments or any undertaking of the Government of India/State Governments nor any criminal case is registered/pending against us or our owner/partner anywhere in India. I/We have no objection if enquiries are made about my work/clients listed by me/us.
4. I/We certify that I/We have read and understood the terms and conditions of the RFP and will abide by them till the completion of the Contract Period.
5. I/We certify that all the requirements highlighted as part of Scope of Work, Technical Bid, Agreement, etc., are covered in totality in the proposal submitted by me/us.
6. I/We note that you are not bound to accept any or all bids you may receive.

Place:

Date:

Signature of the authorized representative:

Name & Designation of the authorized representative:

Office Seal:

ANNEXURE X CODE OF INTEGRITY

(On letter head of the Bidder)

DECLARATION

I _____ working as _____ in _____ (name of the Bidder and Bidder's address in full be mentioned), hereby solemnly affirm and declare that I have been authorized by the Bidder to sign the bids. I, hereby declare and certify, on behalf of the Bidder, that we have accepted all the terms & conditions mentioned in the RFP No: **GICRE/ITMG/RFP/05/2021-22** and we shall abide by all the terms & conditions of Agreement/RFP/Purchase order.

I further declare that in relation to my/our Bid submitted to GIC Re, in response to RFP No: **GICRE/ITMG/RFP/05/2021-22**, I/whereby..... undertake that I/we shall abide with the Code of Integrity as detailed in the RFP and always make disclosure as to any Conflict of Interest and understand that any breach of the Code of Integrity will render me/us liable to be removed from the list of registered suppliers and would also subject me/us to other punitive action such as cancellation of contracts, forfeiture of EMD, banning, debarring, and blacklisting or action in Competition Commission of India, and so on.

Signature of Authorized Signatory
(With Seal & Stamped)

Place:

Date:

Name:

Designation:

Address:

ANNEXURE XI APPLICATION LANDSCAPE

#	App	Access Type	OS	DB	Management				License Ownership		
					App	OS	DB		App	OS	DB
1	SAP ECC	Thick Client	RHEL	Oracle & HANA	GIC Re	SB	SB		GIC Re	SB	GIC Re
2	SAP BW	Thick Client	RHEL	Oracle & HANA	GIC Re	SB	SB		GIC Re	SB	GIC Re
3	SAP PF/ Pension	Thick Client	RHEL	Oracle	GIC Re	SB	SB		GIC Re	SB	GIC Re
4	SAP BO	Web App	RHEL	Oracle	GIC Re	SB	SB		GIC Re	SB	GIC Re
5	SAP Enable Now	Web App	Windows 2012	MSSQL	GIC Re	SB	SB		GIC Re	SB	SB
6	SAP ESS	Web App	RHEL	Oracle	GIC Re	SB	SB		GIC Re	SB	GIC Re
7	SAP PO	Web App	RHEL	Oracle & HANA	GIC Re	SB	SB		GIC Re	SB	GIC Re
8	SAP Solman	GUI/ Web App	RHEL	Oracle	GIC Re	SB	SB		GIC Re	SB	GIC Re
9	BAS Convergence	Web App	Windows 2016	MySQL	GIC Re	SB	SB		GIC Re	SB	SB
10	Life Re Rating	Web App	Windows 2016	MySQL	GIC Re	SB	SB		GIC Re	SB	SB
11	MSGPM	RDP	Windows 2012	NA	GIC Re	SB	SB		GIC Re	SB	SB
12	DMS	Web App	RHEL	Oracle	GIC Re	SB	SB		GIC Re	SB	SB
13	RMS App	RDP only	Windows 2019	MSSQL	GIC Re	SB	SB		GIC Re	SB	SB
14	Renova	Thick Client/ RDP	Windows 2008	MSSQL	GIC Re	SB	SB		GIC Re	SB	SB
15	GIC FTP	RDP/ FTP	Windows 2019	NA	GIC Re/ SB	SB	SB		SB	SB	SB
16	AD/ DNS	RDP	Windows 2016	NA	SB	SB	SB		SB	SB	SB
17	Facial Recognition	Thick Client	Windows 2016	MSSQL	GIC Re	SB	SB		GIC Re	SB	SB
18	GICDRemark	Thick Client	Windows 2016	MSSQL	GIC Re	SB	SB		GIC Re	SB	SB
19	JBOSS EAP	Thick Client	RHEL	NA	SB	SB	NA		SB	SB	SB

* Numbers provided above might vary to some extent. Please take into consideration delta variations for this. *

* SB: Selected Bidder*

* SB to consider future application additions as well. *

ANNEXURE XII NETWORK BANDWIDTH & ENDPPOINTDETAILS

MPLS, ILL & P2P Bandwidth Details:

Hub/ Spoke Locations	Destination	Bandwidth (Mbps) (A)	Link Type	Qty (with redundancy) (B)	CPE Count	Total Effective Bandwidth (Through SD-WAN) (A*B) (Mbps)
Mumbai HO	DC	200	MPLS	2	2	400
Mumbai HO	Internet	300	ILL	2	2	600
Mumbai Oriental	DC	50	MPLS	2	2	100
Mumbai Oriental	Internet	75	ILL	2	2	150
Delhi	DC	20	MPLS	2	2	40
Delhi	Internet	50	ILL	2	2	100
GIFT City	DC	20	MPLS	2	2	40
GIFT City	Internet	50	ILL	2	2	100
DC	DR	80	P2P	2	2	160
DC	Internet	100	ILL	2	2	200
DR	Internet	50	ILL	1	1	50

Location wise Endpoint Details:

Location	User/ Endpoint Count
GIC HO Mumbai	485
GIC Oriental House Mumbai	100
GIC GIFT City	5
GIC Delhi	10
Total	600

ANNEXURE XIII
CURRENT DC & DR SIZING (VIRTUAL AND ORACLE PHYSICAL SERVERS)

VMWARE Cloud							
VM	Application	vCPUs	Memory (GB)	Storage (GB)	OS	DB	DR (Yes/No)
ECC PROD	SAP	48	128	1388	Red Hat Enterprise Linux 7 (64-bit)	Oracle (with SAP)	Yes
ECC DEV	SAP	2	24	950	Red Hat Enterprise Linux 7 (64-bit)	Oracle (with SAP)	No
ECC QAS	SAP	16	60	1982	Red Hat Enterprise Linux 7 (64-bit)	Oracle (with SAP)	No
ECC SANDBOX	SAP	48	128	2219	Red Hat Enterprise Linux 7 (64-bit)	Oracle (with SAP)	No
BO DEV	SAP	2	24	250	Red Hat Enterprise Linux 7 (64-bit)	Oracle (with SAP)	No
BO PROD	SAP	4	32	200	Red Hat Enterprise Linux 7 (64-bit)	Oracle (with SAP)	No
BW DEV	SAP	10	24	2770	Red Hat Enterprise Linux 7 (64-bit)	Oracle (with SAP)	No
BW PROD	SAP	9	64	4162	Red Hat Enterprise Linux 7 (64-bit)	Oracle (with SAP)	Yes
BW SANDBOX	SAP	9	64	4753	Red Hat Enterprise Linux 7 (64-bit)	Oracle (with SAP)	No
PF/ PENSION PRD	SAP	6	48	1226	Red Hat Enterprise Linux 7 (64-bit)	Oracle (with SAP)	No
ESS PROD	SAP	4	48	300	Red Hat Enterprise Linux 7 (64-bit)	Oracle (with SAP)	Yes
ESS DEV	SAP	6	24	250	Red Hat Enterprise Linux 7 (64-bit)	Oracle (with SAP)	No
PO DEV	SAP	2	32	200	Red Hat Enterprise Linux release 8.0 (Ootpa)	Oracle (with SAP)	No
PO PRD	SAP	2	32	100	Red Hat Enterprise Linux release 8.0 (Ootpa)	Oracle (with SAP)	Yes
SOLMAN DEV	SAP	4	24	450	Red Hat Enterprise Linux 7 (64-bit)	Oracle (with SAP)	No
SOLMAN PROD	SAP	4	32	2941	Red Hat Enterprise Linux 7 (64-bit)	Oracle (with SAP)	No
SAP Enable Now	SAP	8	48	200	Microsoft Windows Server 2016 or later (64-bit)	MSSQL 2016 Standard	No
SAP-ROUTER	SAP	4	8	200	Microsoft Windows Server 2012 (64-bit)	NA	No
DMS PROD	DMS	6	12	800	Red Hat Enterprise Linux 7 (64-bit)	NA	Yes
DMSUAT	DMS	6	12	710	Red Hat Enterprise Linux 7 (64-bit)	NA	No

GIC RE Global AD	AD	4	8	400	Microsoft Windows Server 2016 or later (64-bit)	NA	Yes
GICDREMARK	REMARK	8	12	1750	Microsoft Windows Server 2016 or later (64-bit)	MSSQL 2016 Standard	No
GIC-EAA Connector 1	ZTNA	4	8	100	Microsoft Windows Server 2016 or later (64-bit)	NA	Yes
GIC-EAA Connector 2	ZTNA	4	8	100	Microsoft Windows Server 2016 or later (64-bit)	NA	Yes
GICOSDFR	Facial Recognition	4	12	200	Microsoft Windows Server 2016 or later (64-bit)	MSSQL 2016 Standard	Yes
GICMSPROJECT	MS Project	2	4	200	Microsoft Windows Server 2016 or later (64-bit)	NA	No
GICI-WIN-FTP	FTP	2	8	3500	Microsoft Windows Server 2019 (64-bit)	NA	No
GICREBIOMTS	StarLink	4	4	200	Microsoft Windows Server 2016 or later (64-bit)	MSSQL 2014 Standard	No
BASCONVERGE NCE	WebApp	2	4	100	Microsoft Windows Server 2016 or later (64-bit)	MYSQL	Yes
LIFERERATING	WebApp	2	4	200	Microsoft Windows Server 2016 or later (64-bit)	MYSQL	Yes
LIFRENEW	Renova	1	4	100	Microsoft Windows Server 2008 R2 (64-bit)	MSSQL 2008 Standard	No
RMSANALYSIS1	RMS	8	64	1024	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSANALYSIS2	RMS	8	64	1024	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSANALYSIS3	RMS	8	64	1024	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSANALYSIS4	RMS	8	64	1024	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSANALYSIS5	RMS	8	64	1024	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSANALYSIS6	RMS	8	64	1024	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSANALYSIS7	RMS	8	64	1024	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSANALYSIS8	RMS	8	64	1024	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSANALYSIS9	RMS	8	64	1024	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSANALYSIS10	RMS	8	64	1024	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSANALYSIS11	RMS	8	64	1024	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSANALYSIS12	RMS	8	64	1024	Microsoft Windows Server 2019 (64-bit)	NA	No

RMSDB-NEW	RMS	16	128	8192	Microsoft Windows Server 2019 (64-bit)	MSSQL 2019 Standard	No
RMSHN-NEW	RMS	8	64	1024	Microsoft Windows Server 2019 (64-bit)	MSSQL 2019 Standard	No
RMSVM1	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM2	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM3	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM4	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM5	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM6	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM7	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM8	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM9	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM10	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM11	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM12	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM13	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM14	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM15	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM16	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM17	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM18	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM19	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM20	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM21	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM22	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM23	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
RMSVM24	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No

RMSVM25	RMS	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
SAP-JUMP-SRV	Jump Server	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
SAP-JUMP-SRV01	Jump Server	4	8	200	Microsoft Windows Server 2019 (64-bit)	NA	No
HRMS App Server	HRMS	8	16	300	Microsoft Windows Server 2019 (64-bit)	NA	No
HRMS DB Server	HRMS	16	32	450	Microsoft Windows Server 2019 (64-bit)	MSSQL 2019 Standard	No
MSG LRM Server	MSG	8	8	400	Microsoft Windows Server 2012 (64-bit)	NA	No
Oracle Physical Servers							
Server	Application	vCPUs	Memory (GB)	Storage (GB)	OS	DB	DR (Yes/No)
docdb	DMS Prod DB	8	64	1750	Red Hat Enterprise Linux Server release 6.3 (Santiago)	Oracle Database 11g Enterprise Edition (11.2.0.1.0)	Yes
Dmsdb-prod	DMS UAT DB	8	64	1024	Red Hat Enterprise Linux Server release 7.7 (Maipo)	Oracle Database 12c Enterprise Edition (12.1.0.2.0)	No

****DR for GCC and Oracle DB Server to be sized based on the DR column in this table****

****DR for HANA Cloud to be sized as per proposed HANA Sizing Table in Annexure XIV****

ANNEXURE XIV PROPOSED SAP HANA DB CLOUD SIZING

SAP HANA Cloud/ Grid DC						
SAP Frontend Instance/ VM	Environment	OS	vCPU	vRAM (GB)	SSD-Root/ Storage (GB)	Qty (with HA)
ECCPROD	Production	RHEL 8.x for SAP HANA	64	1024	1200	2
ECCDEV	Development	RHEL 8.x for SAP HANA	16	512	1200	1
ECCQAS	UAT	RHEL 8.x for SAP HANA	32	1024	1200	1
ECCPREPROD	Sandbox	RHEL 8.x for SAP HANA	64	1024	1200	1
PF/ PENSION PROD	Production	RHEL 8.x for SAP HANA	16	1024	1200	2
PF/ PENSION QAS	DEV/ UAT	RHEL 8.x for SAP HANA	16	1024	1200	1
ESSPROD	Production	RHEL 8.x for SAP HANA	48	256	300	2
ESSDEV	DEV/ UAT	RHEL 8.x for SAP HANA	24	256	300	1
BWPROD	Production	RHEL 8.x for SAP HANA	64	512	1200	2
BOPROD	Production	RHEL 8.x for SAP HANA	16	512	1200	2
BWDEV	DEV/ UAT	RHEL 8.x for SAP HANA	16	256	350	1
BODEV	DEV/ UAT	RHEL 8.x for SAP HANA	8	256	350	1
BWPREPROD	Sandbox	RHEL 8.x for SAP HANA	16	256	350	1
POPROD	Production	RHEL 8.x for SAP HANA	16	256	350	2
PODEV	DEV/ UAT	RHEL 8.x for SAP HANA	8	128	200	1
TOTAL						21
SAP HANA Cloud/ Grid DR						
SAP Frontend Instance/ VM	Environment	OS	vCPU	vRAM (GB)	SSD-Root/ Storage (GB)	Qty
ECCPROD	Production	RHEL 8.x for SAP HANA	64	1024	1200	1
ESSPROD	Production	RHEL 8.x for SAP HANA	48	256	300	1
BWPROD	Production	RHEL 8.x for SAP HANA	32	512	1200	1
PF/ PENSION PROD	Production	RHEL 8.x for SAP HANA	16	1024	1200	1
POPROD	Production	RHEL 8.x for SAP HANA	16	256	350	1
TOTAL						5

****The SAP Frontend Instances/ VMs will be running on GCC and must connect seamlessly at near-zero latency with the SAP HANA DB Cloud/ Grid. ****

ANNEXURE XV TECHNICAL BID COMPLIANCE

The bidders shall fill and submit the following tables, based on their proposed solution. These tables will be used for technical marking as per scheme of marks explained in **Annexure III**.

A	Cloud Setup	
#	Minimum Requirement Specifications	Compliance (Yes / No)
1	Specify underlying hardware (Make & Model)	
2	The solution shall allow delivery of enterprise-class compute and storage services using latest x86 server infrastructures. It should be capable of supporting multiple hypervisors.	
3	The underlying hardware should have Latest Intel CPU and other components.	
4	Storage should be sized as per <u>Annexures XIII & XIV</u> . If there is any overhead, then selected bidder shall size accordingly to meet the minimum requirement in the RFP.	
5	The Selected Bidder shall provide desired capacity and performance using ALL FLASH (SSD) drives, as internal storage of proposed solution.	
6	Memory requirement: as per <u>Annexures XIII & XIV</u> .	
7	CPU requirement: as per <u>Annexures XIII & XIV</u> .	
8	Setup must have Redundant Hot Plug High Efficiency Power Supply with N+1 configuration.	
9	The solution shall provide the capability to define & change storage policies on a per-VM basis.	
10	The solution shall provide scale-up (by adding SSD) and scale-out architecture with no disruption to the workloads already running on the platform.	
11	The solution shall ensure zero data loss in case of disk, host, or network failure.	
12	The solution shall support checksum of data to ensure data integrity to enable automatic detection and resolution of silent disk errors.	
13	The solution should be able to work on latest x86 server hardware available from all the leading vendors in the industry and should not be restricted to a particular vendor/ make/ model.	
14	The Solution shall provide Remote management features, management software capable of providing role-based security, alerts of critical component failure along with power monitoring. It shall also provide for controlling Power, Fan management, Compute node initialization, Resource discovery and inventory management, Resource alerts and monitoring management, Compute node power management and diagnostics for elements including I/O options and compute nodes, etc.	
15	The solution should support VM based replication. All licenses to enable the same must be part of overall solution.	
16	The solution must support back up of all Virtual machines, so that the same can be recovered in case of data loss, all licenses to enable the same must be part of overall solution.	
17	The solution shall support all the leading hypervisors.	
18	The solution must offer multidimensional auto-scaling of cloud services where resource like RAM and CPU can scale vertically, and systems/ servers can scale horizontally.	
19	The solution must be able to create, delete, shutdown, reboot VMs from Cloud Management portal.	

20	The solution must be able to size VMs and select require operating system when provisioning any VMs.	
21	The solution must be able to predict billing of resources before provisioning any cloud resources integrated with billing system.	
22	The solution must be able to set threshold of resources of all types of scalabilities.	
23	The solution must be able to provision any kind of resources either static or elastic resources.	
24	The solution must be capable of allowing VMs to self-service compute, network and storage infrastructures automatically based on workload demand.	
25	The solution must ensure that the VM format is compatible with other cloud systems.	
26	The Solution must provide Unified Infrastructure Management with complete inventory management of VMs, servers & physical resources.	
27	The solution must ensure the ability to map private IP address of VMs to public IP address as and when required through WAF.	
28	The solution must provide near zero downtime host patching with maintenance mode to move running workloads to other hosts on the platform with a consistent audit trail of the patching process.	
29	The solution must be able to monitor the network traffic of VMs.	
30	The solution must offer provision to analyze amount of data transferred among each VMs.	
31	The solution must offer provision to monitor uptime of each VM.	
32	The solution must offer provision to monitor the load of all VMs/ servers and set threshold for alerts.	
33	The Selected Bidder must ensure availability of historical data/ logs for resource utilization for a minimum period of 6 months.	
34	The Selected Bidder must ensure that there are sufficient graphical reports of resource utilization and available capacity.	

B	General Cloud Requirements	
#	Minimum Requirement Specifications	Compliance (Yes / No)
1	The Selected Bidder shall provide and manage a Hybrid Infrastructure of MEITY GCC, Oracle Physical Server/ Cloud & SAP HANA Cloud for hosting the applications & DBs of GIC Re at the proposed DC & DR.	
2	The DC & DR sites shall be at least an Uptime/ TIA 942 certified Tier III DC providing 99.99% service availability SLAs.	
3	The proposed DC & DR sites shall be well equipped with physical, logical, network & infrastructure security solutions, access protection systems (including physical access control), and shall maintain the access logs.	
4	The proposed DC & DR sites shall be well equipped with intrusion detection & protection systems, firewalls, system management solutions & tools, backup & restore solutions, monitoring tools, network load balancer for applicable servers and network layer security to isolate GIC Re's Web, App & DB environment.	
5	The proposed DC & DR sites shall have the ability to scale up or down the servers/ VMs/ compute resources on-demand/ as desired without significant downtime.	
6	The proposed infrastructure shall include the physical/ virtual machines, OS, application Servers, DB servers, AV solutions, system management & backup agents.	

7	The solution must be intelligent enough to predict incoming load and assign resources to VMs/ Servers dynamically without rebooting system.	
8	The solution must always allocate minimum 50% buffer resources against running load to handle sudden spikes.	
9	The solution must provide high availability (HA) across VMs so that even if any host goes down, all guest VMs should be migrated to the next available host.	
10	The solution must support horizontal load balancing along with vertical. Load balancer should be used to load balance traffic. Load balancer should be able to trigger new VMs to handle additional load. If load goes down, newly triggered VMs should be recycled.	
11	The Selected Bidder shall provide a dashboard of all VMs and Servers to monitor allocated and used resources. There should be provision to generate historical reports of resources utilization (minimum 6 months).	
12	Cloud dashboard must allow to generate reports for trend analysis of system usage.	
13	The solution must have provision to create golden image of VMs so that it can be used to make more machines of same configuration.	
14	The solution must have provision to take snapshots of VMs so that working images of testing/ quality servers can be created.	
15	The Selected Bidder shall migrate and manage the current SASE ZTNA EDS solution to enable roaming users to access GIC Re's applications & DBs hosted in DC & DR in a secure manner.	
16	The Selected Bidder shall provide a site-to-site (IPsec) VPN connectivity for foreign branches of GIC Re to access GIC Re's applications & DBs hosted in DC & DR in a secure manner.	

C	DR Management (DRM) Tool	
#	Minimum Requirement Specifications	Compliance (Yes / No)
1	The Selected Bidder shall provide name and other details of the Solution.	
2	The proposed solution must provide a single dashboard for heterogeneous environments including physical & virtual environments (Oracle DB & GCC & SAP HANA).	
3	The proposed solution must provide Application/ DB wise impact analysis from application perspective.	
4	The proposed solution must provide real time visibility of all DR solution parameters like RPO, RTO, Maximum Tolerable Period of Disruption (MTPod), application health, replication status and alerts on any deviation.	
5	The proposed solution must provide reports on important parameters like disk space, password changes, file addition/ deletion, firewall/ network policies and application monitoring services, etc., to ensure DR readiness.	
6	The proposed solution must be capable of recovering multiple systems parallelly and support inbuilt load balancing techniques for optimized recovery.	
7	The proposed solution must be capable of Recovering Servers, VMs, Storage, Network, Application, DB, Webserver and Middleware layers on the click of a button.	
8	The proposed solution must not rely on scripting for recovery automation.	
9	The proposed solution must allow automating process document and storing it over the cloud/ across DC.	

10	The proposed solution must facilitate workflows for bringing up the applications, and all the components it depends on, at DR.	
11	The proposed solution must provide APIs for Hypervisor integration and automate various actions pertaining to VMs.	
12	The proposed solution must provide alerts through SMS, email, etc. in case of threshold breach or threat of SLA violation.	
13	The proposed solution must provide out of the box exception handling manager which may allow taking automated remedial action in response to certain alerts/ alarms.	
14	The proposed solution must provide reports on RPO deviation, RTO deviation, Data lag, Application DR Readiness status and replication status.	
15	The proposed solution must provide DR drill and audit reports with RPO & RTO, compliant with requirements of GIC Re.	
16	The proposed solution must be capable of generating reports in pdf, csv, XML, other readable formats.	

D	Hypervisor	
#	Minimum Requirement Specifications	Compliance (Yes / No)
1	The Selected Bidder shall provide name and other details of the Solution.	
2	The Virtualization software (solution) should be based on hypervisor technology which sits directly on top of Hardware (Bare Metal).	
3	The Solution must be able to run various operating systems like windows client, windows server, Linux (at least RHEL, SUSE, Ubuntu, Debian, FreeBSD, Oracle Enterprise Linux, and CentOS).	
4	The Solution must be able to run all our requisite applications (current and future; Annexure XI) across the VMs.	
5	The Solution must have the capability for creating Virtual Machines to provision new servers.	
6	The Solution must continuously monitor utilization across Virtual Machines and should intelligently and dynamically allocate resources among the Virtual Machines.	
7	The Virtualized Infrastructure must be able to consume Storage across various protocols like DAS, NAS, and SAN.	
8	The Solution must allow for taking snapshots of the Virtual Machines to be able to revert to an older state.	
9	The Solution must cater for the fact that if one server fails all the resources running on that server shall migrate to another set of servers.	
10	The Solution must provide patch management capabilities such that it must be able to update patches on its own hypervisor and update operating systems.	
11	The Solution must provide the monitoring, prioritizing, and reserving capabilities for storage, processor, network, memory to ensure that the most important Virtual Machines get adequate resources even in the times of congestion.	
12	The Solution must support Live Migration of a Virtual Machine from one node/ host to another.	
13	The Solution must deliver all listed Hypervisor capabilities using x86 server infrastructure.	
14	The Solution must provide security on the hypervisor, as well as VMs. It should provide the ability to apply security to virtual machines and security policies that can follow the machines.	

15	The Solution must provide policy-based configuration management to ensure compliance across all aspects of the DC infrastructure, including virtual and physical resources.	
16	The Solution must have the ability to live migrate VM files from one storage array to another without any VM downtime and support such migration from one storage protocol to another (e.g., FC, ISCSI, NFS, DAS, vSAN).	
17	The Solution must provide an integrated back-up solution as per defined backup policy.	
18	The Solution must include DR functionality management that must be integrated with the rest of the virtualization management, with functionality to automate testing and executing of DR plans (to reduce RTOs) without disrupting production environment.	
19	The Solution must also provide solution to address replication between heterogeneous storage arrays across sites.	
20	The Solution must have the ability to extend recovery plans with custom scripts, like it should be able to reconfigure VM's IP addresses to match network configuration at DR site.	
21	The Solution must provide network information of cloud virtual resources.	
22	The Solution must have built-in user-level controls and administrator logs for transparency and audit control.	
23	The Solution must support use of appropriate load balancers for network request distribution across multiple VMs.	
24	The Solution must provide facility to make template and clones from VMs.	
25	The Solution must support live migration of VMs to other physical servers/ hosts in case of any failure.	
26	The Solution must continuously monitor utilization across Virtual Machines/ Servers and shall intelligently allocate available resources among the Virtual Machines whenever required.	
27	The Solution must be able to create virtual instances of required configuration without limiting to any standard templates.	

E	Compute	
#	Minimum Requirement Specifications	Compliance (Yes / No)
1	The Solution must be able to create Virtual Machines with required number of vCPUs, ensuring that the ratio of vCPU-to-core should not exceed 4:1.	
2	The Solution must allow Virtual Machines consume RAM dynamically in such a way that if some of the VMs in Physical machine are not utilizing the RAM, this RAM can be utilized by some other VM in the same physical machine which has a requirement. This should be applicable for vCPUs as well.	
3	The Solution must allow scalability of compute as and when required from respective cloud infrastructure (GCC, HANA, etc.) of the DC & DR.	
4	The Solution must be able to dynamically allocate and balance computing capacity across collections of hardware resources of one physical box aggregated into one unified resource pool.	
5	The Solution must support detecting, in real time, resource requirements of a system in virtual environment and automatic scaling of resource parameters like RAM and CPU to compensate resource requirement in a system.	
6	The VMs should be scalable in terms of RAM and CPU automatically without reboot.	
7	The Solution must make provision of resource utilization graph i.e., RAM, CPU, storage, load, etc., of each VM/ Server. There should be provision to set alerts based on defined thresholds. There should be provision to configure different email addresses where alerts can be sent.	

8	All the VMs must be auto scalable in terms of compute & RAM.	
----------	--	--

F	Storage	
#	Minimum Requirement Specifications	Compliance (Yes / No)
1	The Solution must provide ALL FLASH/ SSD storage for current (Annexures XIII & XIV) and future requirements.	
2	It must also integrate with other storage types and infrastructures from leading Vendors to leverage high performance shared storage to centralize Virtual Machine file storage for greater manageability, flexibility, and availability.	
3	The Proposed Storage Solution must have the ability to thin provision and thin reclaim disks to avoid allocating all storage space upfront.	
4	The Solution must support migration of live Virtual Machine files from one storage array to another storage array.	
5	The Solution must allow scalability of storage as and when required from respective cloud infrastructure (GCC, HANA, Oracle Physical Servers, etc.) of the DC & DR.	
6	The Solution must make provision of resource utilization graph i.e., disk of each VM/ Server. There should be graphs of each disk partition and emails should be sent if any threshold of disk partition utilization is reached.	

G	NextGen SIEM + SOAR	
1	SIEM Operation	Compliance (Yes / No)
i	The Selected Bidder shall provide name and other details of the Solution.	
ii	The Solution must be able to handle events at least equal to the events handled by existing SIEM Solution.	
iii	The Solution must be scalable by adding additional receivers and log sources and still be managed through a single, unified security control panel	
iv	The Solution must provide reports that are customizable to meet the regulatory, legal, audit, standards, and management requirements.	
v	The Selected Bidder shall provide Next Generation SIEM solution offering that's in the Gartner's Leader/ Visionary segments in the magic quadrant for at least 3 consecutive years.	
vi	The Selected Bidder shall provide Security Automation and Orchestration engine (Complete Incident Response, Playbooks, Case Management and Automated Response) from the same platform vendor/ OEM as NextGen SIEM.	
vii	User and Entity Behavior Analytics must be available in the solution.	
viii	The Solution must support Network Threat Behavior Analytics (both Flow based analytics and Deep packet inspection (PCAP) capabilities).	
ix	The Solution must support Security Analytics (with big data analytics/ Security data-lake platform built-in) - powering the machine analytics and search analytics for threat hunting in the platform.	
x	The Solution must support Multitenancy (no additional cost or no additional instances to be rolled out) with RBAC features.	

xi	The Proposed Solution must support deployment as appliance as well as software models supporting scalability for future and should be designed as Pay-as-you-go model.	
xii	The Solution must never drop logs that are ingested to the platform.	
xiii	<p>The Solution must offer all of the below built-in threat detection modules at no additional cost:</p> <ul style="list-style-type: none"> o User and Entity Behavioral Analytics Module. o Network Threat Analytics Module. o User Threat Analytics Module. o Endpoint Threat Analytics module. o Fraud Detection Module o Multi-dimensional Behavior Analytics Module o Privileged user Monitoring Module. o SANS Top 20 Modules. o Web Application defense module. o APT Module. o Honeypot Module. o Core Threat Detection Module. o Threat Intelligence Service Module. o Others. 	
xiv	<p>The Solution must offer all the below built-in Compliance Modules at no additional cost:</p> <ul style="list-style-type: none"> o ISO 27001 Compliance. o HIPAA Compliance. o PCI Compliance. o NESA Module o FISMA Compliance Module. o GPG Module. o GLBA Module. o SOX Module. o NEI Compliance Module. o NRC Compliance Module. o DoDI Compliance Module. o NERC Compliance Module. o NIST Compliance Module. o CMR Compliance Module. o COBIT-5 Framework Controls. 	
xv	The Solution must support very granular level of role-based access.	
xvi	The Solution must correlate security/ network events to enable the SOC to quickly prioritize its response to help ensure effective incident handling.	
xvii	The Solution must provide remediation guidance for identified security incidents and SOC must immediately act on them.	
xviii	The Solution must provide capability to discover similar patterns of access, communication etc. occurring from time to time, for example, slow and low attack.	
xix	The event correlation on SIEM must be in real time and any delay in the receiving of the events by SIEM is not acceptable.	
xx	Event dropping/ caching by SIEM solution is not acceptable and same must be reported and corrected immediately.	
xxi	The Solution must integrate logs from new devices into existing collectors without affecting the existing SIEM processes.	

xxii	The Solution must have capability of displaying of filtered events based on event priority, event start time, end time, attacker address, target address etc.	
xxiii	The Solution must support configurable data retention policy based on GIC Re's requirement.	
xxiv	The Solution must provide tiered storage strategy comprising of online data, online archival, offline archival and restoration of data. Please elaborate on log management methodology proposed.	
xxv	The Solution must have capability for log purging and retrieval of logs from offline storage.	
xxvi	The Solution must support collection of logs from all the endpoints, devices, VMs, Servers, Components, etc., in GIC Re's Hybrid Cloud Infrastructure.	
xxvii	The Solution must support log integration for IPv4 as well as for IPv6.	
xxviii	The Solution must provide 24*7*365 extensive monitoring of the entire infrastructure and prompt responses to attacks and security incidents.	
xxix	The Selected Bidder's SOC Team must notify about security incidents or provide information about security incidents potentially affecting GIC Re.	
xxx	The Selected Bidder's SOC Team must provide all reports, customized as per GIC Re's need, monthly. The Team must review these reports and take all necessary actions with prior approval from GIC Re.	
2	Collection Layer	Compliance (Yes / No)
i	The Solution must collect the System/ Machine Data, Network Data and User data in real-time as well as batch processing.	
ii	The Solution must correct event time for machine data from systems with incorrect timestamps. Also, describe how the platform handles the machine data are configured with different time zones.	
iii	The Solution must support the options for scheduling delivery, compressing, and/or encrypting remotely collected machine/ network (flows and packets)/ user data (behavioral data) logs.	

iv	<p>The data collector/ agent must be able to collect data through different methods, including but not limited to:</p> <ul style="list-style-type: none"> o UDP/TCP o SNMP o Cisco SDEE o NetFlow o JFlow o Sflow o AIX, iSeries (via 3rd party integration) o Windows Event Logs (RPC) - this includes custom Event Logs (by using RPC not WMI). o Windows Event Logs (local) – this includes custom Event logs o Single-line Flat Files o Multi-line Flat Files o Compressed Flat Files (single and multi-line) o NetApp CIFS o eStreamer o Metasploit o Nexpose o Nessus o eEye Retina o Tripwire o API 	
v	The Solution must secure the communication during the data collection mechanism.	
vi	The Solution must have the capability of data filtering at the collector level.	
3	User & Entity Behavioral Analytics (UEBA)	Compliance (Yes / No)
i	The U.E.B.A must be offered out of the box at no additional cost or license.	
ii	The U.E.B.A must be able to detect and respond to insider threats, compromised account, and privileged account abuse, etc.	
iii	The U.E.B.A must collect machine data from across GIC Re environment and fill in forensic gaps with endpoint and network monitoring.	
iv	The U.E.B.A must be able to correlate log information to single identities to know the actors behind the actions impacting GIC Re environment with Identity Inference, which attributes identities to anonymous log messages, streamlining forensic investigations.	
v	The U.E.B.A must create a heuristic baseline of user activity by analyzing behavior, so it must perform multidimensional baselining, enabling the modelling of a broad set of user behaviors. Baselines are used to detect anomalous behavior via machine learning and other statistical analysis techniques.	
vi	The U.E.B.A must use the heuristic baseline to detect unusual behaviors in real time, so it must continuously analyze current activity against baselines established for each identity and peer group. Detect behavioral deviations from user and peer group baselines.	
vii	The U.E.B.A must detect threats of data exfiltration, privileged identity misuse and fraud.	
viii	The U.E.B.A must provide case management, incident investigation, and extensive reporting, so it must Accelerate investigation and response with embedded security orchestration and automation functionality.	

ix	The U.E.B.A must use pre-staged Smart Response actions to rapidly collect forensic data and invoke targeted countermeasures. Report on the results of your security program, including detection and response times.	
4	Machine / User Data Analysis	Compliance (Yes / No)
i	The Solution must analyze the collected data in real time.	
ii	The Solution must support 4 layer of log data classifications by default out of the box: o Layer 1: Audit – Operation Security. o Layer 2: Classification. o Layer 3: Common Event. o Layer 4: MPE (Rule Name).	
iii	The Solution must describe data enrichment capabilities, including the number and type of available fields.	
iv	The Solution must represent large search results in a single view.	
v	The Solution must describe the steps required to narrow search results to a specific type of log source from a specific server within the environment.	
vi	The Solution must perform geolocation tracking for IP addresses.	
vii	The Solution must perform DNS resolution for IP addresses.	
viii	The Solution must contextualize the user information with a detailed information about the user attributes from the domain such as username, title, department, last time to log on, last time he/ she failed in the password, email address, etc.	
5	Real-Time Advanced Analytics	Compliance (Yes / No)
i	The Solution must be capable of creating real-time advanced analytics rules. It shall be a GUI-driven interface.	
ii	The Solution must support the below out-of-the-box analytics rules (but not limited to): o 3 Classification types o 39 Sub Classifications o 30,000+ Common Events (Sub Classification) o 600,000+ Message Processing Engine Rules o 1000+ Predefined Use Cases o 1250+ Predefined Reports	
iii	The Solution must perform advanced analytics against all data or a subset of the data.	
iv	The Solution must have a risk-based priority engine that can assign a risk value for all the logs, events, and alarms natively at no additional cost.	
v	The Solution must allow GIC Re to build a filter and reuse it with multiple use cases /rules.	
vi	The Solution must be able to minimize false positives.	

vii	<p>The Solution must support 15 different types of correlation/ Use cases (but not limited to):</p> <ul style="list-style-type: none"> o Behavioral: <ul style="list-style-type: none"> ü Whitelist based correlation. ü Blacklist based correlation. ü Machine analytics-based correlation. ü Statistical based correlation. ü Trend based correlation o Unique Value: <ul style="list-style-type: none"> ü Unique value observed based correlation-based correlation. ü Unique value non-observed compound-based correlation. ü Unique values non-observed scheduled based correlation o Log: <ul style="list-style-type: none"> ü Log Observed based correlation. ü Non-Observed Compound based correlation. ü Non-Observed Scheduled based correlation. ü Session sequence-based correlation. o Threshold: <ul style="list-style-type: none"> ü Threshold observed based correlation. ü Threshold non-observed compound-based correlation. ü Threshold non-observed scheduled based correlation. 	
6	Security Orchestration, Automation & Response	Compliance (Yes / No)
i	The Solution must automate response to threats.	
ii	The Solution must have the capabilities to calculate the Mean time to detect and Mean time to respond for all the incidents detected and responded using the platform as the key KPIs.	
iii	The Solution must have an end-to-end case management feature and must be able to integrate to Selected Bidder's service desk tool to initiate and close a service/ incident ticket in bidirectional mode.	
iv	The Solution must have pre-built playbooks for Incident response and have the capability to build new playbooks or customize the existing one.	
v	<p>The Solution must be able to perform the actions below (but not limited to):</p> <ul style="list-style-type: none"> o Disable user account o Remove user from domain group o Quarantine an infected machine o Add IP to Firewall block list o Prevent the user from running non-authorized process or application o Enforce service to start o Enforce service to stop o Enforce service to be disabled o Add item to a watch list o Remove item from watch list o Disable local user account o Enforce the user to be logged off from a machine o Extract the pcap file and open the leaked attachment o Execute remote command o Delete file o Take memory dump 	
vi	The Solution must allow GIC Re to add their own automated remediation.	

vii	The Solution's automated remediation must provide a built-in hierarchy approval workflow.	
viii	The Solution must be there in the platform out of the box at no additional cost.	
ix	The Solution must provide incident tracking through an integrated security incident response platform.	
x	The security incident response platform must be fully integrated with analysis functions not through a separate Web UI or solution.	
xi	The Solution must have built-in case management with collaboration and evidence locker capability and integrate also with external ticketing system.	
xii	The Solution must calculate the mean time to detect and mean time to respond automatically and show that on the dashboard for analysis.	
xiii	The Solution must have the compliance packages such as ISO, PCI, HIPAA, GPG, etc., as correlation rules, saved searches, saved reports out of the box with no additional cost.	
xiv	In addition to internal security incident response capabilities, describe how the solution provides integration with third-party ticketing systems that GIC Re may utilize.	
xv	The Solution's built-in case management must allow any case to be shared with other collaborators, who can also add forensic evidence and annotations to expedite threat detection and response. All activity must be tracked as part of the case history, providing real-time status and a tamper-proof audit trail.	

H	PIM/ PAM	
1	Architecture	Compliance (Yes / No)
i	The Selected Bidder shall provide name and other details of the Solution.	
ii	The Privileged Identify/ Access Management (PIM/ PAM) Solution must be a provided through a dedicated instance on VM in GIC Re environment.	
iii	The Solution must be agent-less.	
iv	The Solution must support High Availability/ Redundancy deployments for higher availability and DRBC Solution. The system must be highly available (24*7*365) and redundant from hardware failure, application failure, data failure, and/ or catastrophic failure. The system must have provisions to keep the Solution running at 100% with proper alerting, fail-over, bypass in equally secure manner with availability of credentials.	
v	The Solution must provide a secured process for encrypted storing and backups. The encryption algorithm must be FIPS 140-2 compliant or higher.	
vi	The architecture must support network load balancing and clustering technology.	
vii	If a database is used/required, the database must be managed from within the Solution, and no outside DBA access must be available. The Solution must be fully managed and hardened.	
viii	The platform must be highly secured, tamper-proof for the Solution and for the storage. The Solution must provide web-based interface for easy access and management.	
2	Performance and Scalability	Compliance (Yes / No)

i	The Solution must be able to be implemented in virtual environment. Solution must also be able to control, manage privileged accounts and identities on Hypervisors/ platform virtualization software. (Installation on virtual servers and control of users and resources in virtual servers etc.)	
ii	The product must be capable of handling unlimited user accounts and systems. There must be no latency or performance degradation in using an average of 500 concurrent users and systems.	
iii	In multi-tiered architecture the Solution must have the capability to deploy the password database, management console, web server and reporting database etc. on separate machines which can be connected to a central management console. (Web-based Central administration within unified suite, single user interface, central repository)	
iv	The Solution must provide scalability through a modular design for adding capacity and scalability metrics. It must have capability to integrate with HR applications / Identity and Access Management applications or Physical access applications that the Bank may procure.	
3	Discovery of Systems, Accounts and Services	Compliance (Yes / No)
i	The Solution must be capable of dynamically and automatically detecting new resources/ locations like desktops/ servers/ operating systems/ services/ scheduled tasks/ IIS service accounts/ network devices/ hypervisors in virtual systems etc., throughout the environment and provision them to the product and automatically discover privileged accounts and enforce the right password policy.	
ii	The Solution must support open API/ provide APIs to add "connectors" to manage devices that are not currently supported 'out-of-the-box'. It must also be capable of connecting to legacy applications.	
iii	<p>The Solution must be able to support/manage privileged accounts and create seamless single sign on in the following:</p> <ul style="list-style-type: none"> o Windows, Unix, RHEL, etc., o Different flavors of Linux, Oracle, MSSQL Server, etc. o SOC applications/ solutions like SIEM, DLP, Server Security, etc. o Network Devices/ components (routers, switches, firewall, IDS/IPS etc.) o Applications as per <u>Annexure XI</u>. o All current and future VMs/ Servers, endpoints, etc. o Web-based or client-server application, IIS, Apache, SharePoint, MS Exchange, IBM lotus, etc. o client support application like TOAD, SQL Plus, SSH and ODBC services/devices, o Middleware like Oracle WebLogic, IBM WebSphere, JBoss, Tomcat SSL/ VPN applications, etc. o Storage devices or any other Solution procured/ deployed by GIC Re during Contract Period. 	
iv	The Solution must be capable of providing multi-domain access.	
v	The Solution must be able to seamlessly connect to Active Directory and LDAP-Compliant directory services accounts, TACACS/ TACACS+ and RADIUS, etc.	
vi	For identity consolidation, Solution must provide AD bridging capabilities over heterogeneous non-windows platforms as this helps to manage Unix, Linux, RHEL and other non-windows platform accounts through Microsoft AD thereby enabling consolidation of authentication and account information.	

vii	The Solution must be able integrate with ODBC query results from configuration management databases (CMDBs) and other sources, bulk-import system lists from text files, and to make ad-hoc entries through the management console.	
viii	The product must be able to manage remote target systems through a firewall (e.g., servers in a DMZ, remote locations etc.) through secure built-in connectivity (without requirement of additional security; such as third-party VPN).	
4	Password/ Credential Management	Compliance (Yes / No)
i	The Solution must have a strong inbuilt password vault/ management system with single-sign-on feature. Password vault must be replicated over a secured channel and off-site data backup, data restoration capabilities must be offered. PIM/ PAM Solution as a whole and specially the password vault, must be installed on a highly secure/ hardened system with minimal services running, in a physically safe environment with least number of people having access to the administrative controls.	
ii	The password vault must be highly reliable, the switch over to HA/ DR must be instantaneous without manual intervention, and provisions must be available to recover credentials securely in case of catastrophic failures.	
iii	The Solution must also support printing of password in secure PIN mailer. PIN mailer printer and stationery to be provided by vendor.	
iv	The Solution must be able to create flexible password management policies. A policy can be applied to an object /a group of objects, or a group of policies can be applied to a group of objects/ objects.	
v	After dynamically discovering resources/ services/ processes, the Solution must be able to propagate password changes to relevant targets across the network to avoid the possibility of service disruptions and lockouts whenever changes are made.	
vi	The Solution must allow bulk operations to be performed on managed accounts (such as force password change immediately, reconcile password, verify password).	
vii	The Solution must support scheduled password changes and GIC Re must be informed after all such scheduled password changes.	
viii	The Solution must protect password change process against race conditions like a failed attempt to update password on target system (password in vault must not be updated) or inability/ delay in determining if the password has successfully been updated on target systems or application configuration files (old password mustn't be removed from the vault). Recovery of managed systems from a backup media must also be supported by Solution, e.g., a database recovery to a point 5 days back.	
ix	Any failed password change event or exceptions must be promptly reported after a certain number of retries, as per GIC Re Password Policy.	
x	The Solution must have the capability to reset individual passwords or groups of passwords on-demand, and to schedule automated checks to ensure that each password stored in the database correctly matches the current login for each target account.	
xi	The Solution must keep the passwords in very strong encrypted form. Support for Hardware Security Modules (HSMs) must be available. The Solution must also provide for strong encryption inside the system components/ processes, between its distributed modules, and between the web application and user machines, to protect passwords and other sensitive information.	

xii	The Solution must be able to change password on demand, based on a specific criteria or policy, automatically or manually, support password verification, reconciliation, and reporting, set password parameters like constitution, history, and change timings.	
xiii	The Solution must support transparent connection to the target device, without seeing the password or typing it in as part of the connection.	
xiv	The Solution must be able to manage credentials in all current and future operating systems, applications, Database Management Systems, etc., in GIC Re environment.	
xv	The Solution must be able to manage passwords stored in plain or encrypted, hardcoded in system files or user-defined files, database tables, network devices etc. including within application configuration files, code, or scripts.	
xvi	The Solution must have provisions to provide credentials for authenticating applications/scripts during run-time.	
5	Access Management	Compliance (Yes / No)
i	The Solution must be able to automatically and dynamically provision users in real time with trusted Windows domains, popular directories such as AD/ LDAP/ TACACS+/ RADIUS servers in accordance with the user entitlements and access privileges granted (based on least privileges principle).	
ii	The Solution must be able to support granular command filtering or context-sensitive entitlements on various platforms for super-user privileged management.	
iii	The Solution must also be able to detect and support concurrent login to managed systems as a privileged user.	
iv	The Solution must be capable of organizing/ grouping target server/ device accounts into logical groups and apply granular/ fine grained access control to access the individual accounts or the groups of accounts.	
v	The Solution must support full Segregation of Duties, e.g., roles are clearly and unambiguously defined with no overlapping. In addition to user access roles and entitlements, Solution must also support role based administrative access to provide Segregation of Duties for administrative management and control. The user permission must be only as per his original privilege after logging in to the OS.	
vi	The Solution must have the capability to restrict users to use RDP to other endpoints.	
vii	The Solution must be capable of having dual control systems (maker-checker) for approval and authorization of critical operations with 4-eye principles.	
viii	The Solution must be capable of integration with strong authentication including biometric authentication, OTP authentication support on alternate channel, hardware/software tokens etc. with single sign on facilities.	
ix	The Solution must be able to integrate with Port-wise Access Manager.	
x	The Solution must have login security by limiting user login by parameters like originating IP address, Host/ domain name, terminal ID, type of login program or time of the day or geographical location, etc., and limited concurrent login sessions by users.	
xi	The Solution must be capable of maintaining details of shared/ pooled accounts by mapping it to the individual users.	
xii	The Solution must be capable of having command level restrictions, i.e., of assigning specific commands to be run by specific users/ groups, from specific nodes etc. The Solution must be able to block commands from command line and in queries as configured for users/ groups/ target resources.	

6	Workflows	Compliance (Yes / No)
i	The Solution must be capable of integrating with a Change Management/ ticketing system to initiate access approval workflows for scheduled changes and be able to control required access (based on least privilege principle) and monitor and/ or terminate super user connections that exceed pre-set time limits (change window).	
ii	The Solution must have the ability to enforce approval workflow only to the human users which can be created to a very granular level.	
iii	The Solution must support a workflow approval process that is flexible to assign multiple approvers (i.e., require 2 or more approvals before access is allowed). Solution must also be able to provide delegation of management tasks like approval/ review etc. Solution must support easy customization of approval workflows according to business needs (without requiring code changes). Solution must also be able to support emergency/ break glass scenarios.	
7	Auditing/ Reporting	Compliance (Yes / No)
i	The Solution must provide a central live Dashboard covering features like management of devices, events and password policies, user activities, event logs etc.	
ii	The Solution must have all regular pre-configured report templates like entitlements reports, user activities, privileged accounts inventory, applications inventory, compliance reports etc.	
iii	The Solution must have capability to create custom reports based on users, events, activities, target systems, password uses and status etc.	
iv	The Solution must have the ability to distribute the reports to intended users through e-mail, to run all reports by frequency, on-demand and schedule them.	
v	The reports must support CSV, Excel, or PDF. This report extraction must not have any performance impact, and feature for report extraction must be available on demand & scheduled as per GIC Re's requirement. The Solution must support customizable reports.	
vi	The Solution must record access for password requests, approvals and check-out, delegation changes, reporting and other activities, access to its management console for configuration and reporting, and all password change job activity.	
vii	The Solution must be able to record sessions, take video recordings of screen shots, keystrokes/ commands, and output, replay sessions for forensic purposes, and provide optimized search capabilities on different parameters like users, events, time, target resources etc.	
viii	The Solution must have real-time session monitoring support and full audit-trail for user activities in the Solution itself.	
8	Alerting and Integration	Compliance (Yes / No)
i	The Solution must be so that events can trigger email/ SMS alerts, run specific programs, and communicate with trouble ticketing applications, SIEM Solutions, and other security frameworks, etc.	
ii	The Solution must be capable of alerting on actions such as password requests and check-outs, password changes, failed password change jobs, console and web application activities etc. and attempts of access violations (running elevated/ higher privilege commands, modifying password/ user files, adding users to privileged groups etc.)	

iii	The Solution must have the ability to integrate with vulnerability management Solutions for deep, authenticated scans, i.e., must be able to provide credentials to these scanning applications during run-time.	
iv	The Solution must be able to provide simple methods for integrations that are not provided out-of-the-box with minimum of effort.	
9	Compliance Reports	Compliance (Yes / No)
i	The Solution must provide pre-configured reports to monitor compliance with regulatory/ audit mandates. It must also provide screen-based templates/ capabilities to create/ generate custom reports without writing codes.	

I	Cloud WAF	
#	Minimum Requirement Specifications	Compliance (Yes / No)
1	The Selected Bidder shall provide name and other details of the Solution.	
2	The Solution must offer protection against all the OWASP Top 10 Attacks.	
3	The Solution must support SSL traffic inspection.	
4	The Solution must offer IP Reputation Based Protection (Bot/ Anonymous Proxy).	
5	The Solution must have Application/ VM specific security policies, which are ready to deploy.	
6	The Solution must check for HTTP Protocol Constraints (RFC Compliance) and must be tweakable.	
7	The Solution must be able to create and deploy Unique Security Policy for each Web Application.	
8	The Solution must provide Support for applications that uses HTTP but listen on Non-Standard Ports.	
9	The Solution must support Virtual patching.	
10	The Solution must be able to define an Input Validation Policy, to check user inputs.	
11	The Solution must be able to configure File Upload Restriction (based on type).	
12	The Solution must offer Brute Force Protection (Attempts/ Source IP) with ability to feed in Captcha Challenge.	
13	The Solution must be able to configure URL Access Limiting (URL wise).	
14	The Solution must support URL redirection.	
15	The Solution must be able to configure Page Access Rules (Forceful browsing to follow an order).	
16	The Solution must offer HTTP Method based protection.	
17	The Solution must get periodic security signature updates.	
18	24*7*365 Technical Assistance must be provided.	
19	The Solution must provide Bandwidth usage information.	
20	The Solution must mask PII/ Sensitive Data in Solution logs.	
21	The Solution must support Multitenancy or dedicated instances deployment.	
22	The Solution must give Detailed Security Event Reporting monthly.	
23	The Solution must display SSL Certificate Expiry information in the Portal.	

24	The Solution must offer Application-level DDoS Protection.	
25	The Solution must offer Load Balancing.	
26	The Solution must support BCP (DC-DR failover).	
27	The Solution must be protected from the Volumetric Network Level DDoS.	
28	The Solution's portal must provide enough information to review the events and take decision.	

J	DLP & Data Classification	
#	Minimum Requirement Specifications	Compliance (Yes / No)
1	The Selected Bidder shall provide name and other details of the Solution.	
2	The Selected Bidder must offer a comprehensive gateway level Data Loss/Leakage Solution for Data Protection	
3	The Solution must be capable to support the following use cases: o Network (web only) o Discover (Data in motion for web only) o Endpoints o Cloud (any current or future SaaS applications, without any additional licenses)	
4	The Solution must have the capability to integrate with the following: o Cloud Proxy o M365 o Active Directory o SIEM o Other SOC components	
5	The DLP Solution must be able to Discover and Monitor data within the enterprise.	
6	The Solution must cover all components/ devices of GIC Re Infrastructure including (but not limited to) - Endpoints (desktops, Laptops, Removable storage, Remote computers), File shares (SAN), Databases (HANA, MSSQL and Oracle), Operating systems (Windows, Mac, Linux, Unix), websites, Portable storage including USB, CD/DVD, Home storage, smartphones, and tablets. It must support All File Types (Bidders to provide a list of those supported).	
7	Solution must have the ability to scan data wherever it is transmitted or used, on the network.	
8	Solution must provide a centralized interface for policy editing and policy management, across the entire network.	
9	Solution must be compatible and must have tight integration with proposed data classification Solution.	
10	Solution must be able to monitor as well as block data sharing as per the data classification/ policies.	
11	Solution must be able to identify Malware threats (i.e., Malware communications or malware data theft, etc.).	
12	Solution must be able to provide visibility on critical Data sent during unusual hours.	
13	Solution must be capable to enforce client level resource throttling.	
14	Solution must monitor and enforce policies without adding latency or failure points to the network	
15	Solution must have the capability to enforce additional layer of monitoring for specific group of users.	

16	Solution must have facility of storage and backup of data, logs, and other records for audit as well as for forensics purposes for a period of 6 months.	
17	The Monitoring and Discovery capabilities must be separate preferably with storage capabilities.	
18	The Solution must be able to inspect HTTP as well as HTTPS - SSL traffic.	
19	The Solution must be able to identify, intercept and analyze SSL traffic to detect any data breach through SSL traffic.	
20	The Solution must be capable to identify and store data from all TCP Protocols.	
21	The Protocol Detection done by the Solution must be port agnostic.	
22	The Solution must Detect keywords/ patterns based on proximity to each other.	
23	The Solution must detect on full Boolean expressions for keywords and key phrases.	
24	The Solution must detect and validate a wide range of sensitive data by assigning appropriate weight to each sensitive data match.	
25	The Solution must be able to classify files as “Encrypted” based on file analysis.	
26	The Solution must register content in an automated way without manual intervention.	
27	The Solution must detect sensitive content from databases and transfer intelligence to Email and Web Monitoring Solutions.	
28	Solution must recursively inspect the contents of encapsulated and compressed (e.g., ZIP, TAR, RAR) archives and detect against fingerprinted content or patterns.	
29	The Solution must allow define a single set of policies once and deploy across all devices. Policy enforcement must be same for connected as well as disconnected endpoints.	
30	The Solution must be capable of identifying and detecting data based on: <ul style="list-style-type: none"> o Predefined regex for sensitive data o Identified documents/ image formats o Tagging of the classified documents o Keywords and patterns 	
31	The Solution must be capable of defining DLP Policies based on content, sender/ recipient, file characteristics, and communications protocol, etc.	
32	Solution must have out of the box Rule Sets available that can be enabled or disabled as required.	
33	System must be able to send alert via email and SMS.	
34	The Solution must allow creation of policies based on Metadata of files such as share/ repository/ data created, etc.	
35	Events generated by the Solution must be able to retain source IP address, destination IP address, protocol, port, sender/ recipient e-mail address, SMTP headers, etc.	
36	In case of Policy violation, the Solution must be able to retain all content/ attachments in the transaction, not just the content that violated policy.	
37	Solution must be able to display and highlight a summary content that violated the policy for any incident.	
38	Solution must provide an in-built case management tool.	
39	Solution must allow case content to be exported with full content and attachments for review by an external reviewer.	
40	Solution must be able to identify and store all event data with appropriate metadata (date/ time, user, protocol, etc.).	

41	Solution must be able to Store and index event data for faster search even after the incident has happened.	
42	Solution must be capable to search any traffic sent out based on: IP Address, URL, Ports & Protocols, document types, keywords, hashes, and time stamp.	
43	Reports built around GIC Re requirements must be easily created in the Solution.	
44	Solution must allow to export historical records from all traffic/ content analyzed by the DLP system into an external system for analysis.	
45	Solution must be capable to scan for identification of classified/ sensitive unstructured data/ files on predefined schedules provided by the admin. The schedule must be customizable basis on different users and groups.	
46	Solution must support NFS, Samba, HTTP, HTTPS, FTP, etc.	
47	The Solution must support monitoring/ blocking of bulk data containing classified/ sensitive structured data/ files.	
48	The Solution must support scanning of databases such as Oracle, Microsoft SQL Server, HANA, etc., for identification of classified/ sensitive structured data/ files.	
49	Solution must be able to have inventory of user/endpoint wise classified data and must have capabilities to perform differential scanning.	
50	The Solution must provide option to Preserve Last Access Time after scanning to maintain archive sanctity.	
51	Solution must be manageable from a single management console for all DLP components.	
52	Solution must offer standard reports on system traffic and performance and throughput metrics.	
53	Solution must provide custom report summarization and grouping across different variables and attributes.	
54	Solution must have a “dashboard” view designed for use by executives that can combine information in a single view.	
55	Solution must be capable of providing the management workflow through Email and Department Head wise.	
56	Solution must have capability to offer different policy behavior when the endpoint is not in the network (roaming users).	
57	For certain policies, Solution must offer the use case where a user can get exceptions through self-approval on providing justifications. Exception approval must also support workflow where department head can approve the exceptions.	
58	Selected Bidder must provide additional policy templates in future without any additional overhead cost.	
59	Solution must be capable of configuring policies based on URL categories.	
60	Solution must be able to monitor/ block the mails syncing with the mobile through Active Sync.	
61	Solution must have feature to detect confidential data sent within image files through features like optical character recognition.	
62	In case of any policy violation, Solution must be able to notify the user who is sending the data as per the policy, classification of data to rectify, alerting or seeking confirmation about the uploading, accessing, etc.	

63	The Solution must have the capability to define specific information technology/ information security policies over and above in-built DLP policies.	
64	Solution must have an approval workflow for the DLP lifecycle. The incident raised by DLP must be managed and highlighted to GIC Re and Selected Bidder's SOC team. The proposed Solution must be capable to provide incident details, with time stamp and subsequent auto escalation as per SLA defined in the process governance system.	
65	Solution must be able to integrate with the ticketing Solution.	
66	Solution must provide GUI based policy enforce & review feature and must also support time bound policy configuration.	
67	Solution must seek policy review confirmations and track the same.	
68	Solution must allow to perform keyword searches to quickly find specific information among various policies.	
69	Solution must capture and track policy exceptions and alert on the expiration of approved exceptions.	
70	The Solution must have tight integration with Proxy to the level of getting unencrypted SSL traffic for further monitoring	
71	The Solution must be transparent to intermediate network elements.	
72	The Solution must not require network reconfiguration, IP addressing or topology changes, or modification to client IP.	
73	The Solution must support installation of agent in user's PC/ workstations in stealth mode and remain unnoticeable.	
74	The Solution must be capable to monitor user's mobile devices. It must be able to integrate with Mobile Device Management Solution.	
75	Solution must have the capability to record the user activity based on policy violation triggers.	
76	Solution must be capable of configuring policies based on Geo location.	
77	Based on manual data classification through DLP the proposed Solution must be able to classify the data and generate alerts.	
78	Solution must provide/ support Manual classification of data at endpoints through HDLP agent.	
79	The Solution must allow GIC Re to define a single set of policies once and deploy across all devices/ components. The policy testing must be preferably on offline data. The Solution must have module to test the policies and must be deployed at outgoing gateways.	
80	Manual classification offered can be in-built or through 3rd party integration, manual classification policies must be built through central management console only.	
81	DLP Solution must monitor and prevent data using HTTP/ HTTPS over browsers like Chrome, Firefox, Edge, and Explorer, etc., at endpoints. Solution must also provide capability to monitor confidential data even if the data leak attempt is made through non-supported browser.	
82	DLP Solution must prevent confidential/ sensitive files from downloading, copying to CD/ DVD/ USB/ iPod®/ Bluetooth®, and other removable media and print screens. DLP Solution must also block any data copied from removal media to the organization laptop or desktop.	
83	Solution must support centralized deployment, administration, management, and reporting for DLP along with host DLP agent push from same centralized management console.	

84	Solution must have the ability to monitor the outgoing protocol traffic in sniff mode from external gateways without any integration with web and email gateways.	
85	File & Folder/ Disk encryption Solution must be integrated with DLP policies.	

K	EDR	
#	Minimum Requirement Specifications	Compliance (Yes / No)
1	The Selected Bidder shall provide name and other details of the Solution.	
2	<p>The Solution must, at minimum, perform the following checks on client/ endpoints:</p> <ul style="list-style-type: none"> o Hooking o SSDT hooks o Alternate SSDT hook (KTHREAD Service Table) o IDT Hooks (interrupt descriptor table) o System drivers IO hooks o System entry (SYSENTER and int2E) hooks o Local and global Windows hooks (SetWindowsHookEx) o User mode hooks (IAT, EAT, Inline) for processes and DLLs o Model Specific Registers hooks o Kernel Object hooks o Metasploit detection 	
2	The Solution must gather security information from the host/ clients/ endpoints including its network shares, patch level, and running Windows tasks.	
3	The Solution must not rely on Anti-virus signatures in order to return an analysis and indicate if an endpoint is compromised.	
4	The Solution must analyze Windows internal structures for alteration and consistency.	
5	The Solution must search for kernel and user mode hooks in SSDT, IDT, IAT/EAT, and IRP_MJ.	
6	The Solution must be able to analyze and report on the MD5 hashes and file size of all executable files found on the system	
7	The Solution must be able to provide a complete environmental correlation that shows the clients/ endpoints and the number of systems where the identified malicious file was found.	
8	The Solution must be able to track and monitor host/ client/ endpoint activity from time of last boot and correlate an infected file back to the original malware executable.	
9	The Solution must be able to whitelist files that may have suspicious behaviors but are in fact legitimate.	
10	The Solution must be able to check for known file hashes with the File Reputation Service, NIST, and custom hash databases, etc.	
11	The Solution must be able to integrate with other SOC components (SIEM, SOAR, etc.) to cross reference against known threats.	
12	The Solution must allow building custom hash set and using it to correlate against suspicious files.	
13	The Solution must be able to validate the digital signatures of all executables.	
14	The Solution must be able to analyze loaded DLL, determine whether they are packed and provide a view of the binary strings in memory.	
15	The Solution must allow baseline scans of hosts/ clients/ endpoints and use this information to build a database of all unique files found that can be used for comparison on future scans.	

16	The Solution must be able to analyze anomalies on the following endpoint clients: o Windows 7 (32 & 64 bits) o Windows 8 (32 & 64 bits) o Windows 10 (32 & 64 bits) o Windows 11 (32 & 64 bits)	
18	The Solution must allow remote upgrade of the agents running on the endpoint clients.	
19	The Solution must allow remote removal of the agents running on the endpoint clients.	
20	The Solution must encrypt the communication between the agents and the management server.	
21	The Solution must encrypt the communication between the management console and the management server.	
22	The Solution must be able to change the communication port between the management console and the management server.	
23	The Solution must be able to set scan priority on the host to prevent performance degradation on the client (low priority scan option).	
24	The Solution must be able to support throttling of client resource requirement.	
25	The Solution must allow configurable selection of analysis checks/ modules to be run on the client/ endpoint.	
26	The Solution must be able to remotely cleanup the infected clients through integration with 3rd party solutions.	
27	The Solution must be able to report on the client status: o Scan in progress o Offline o Idle	
28	The Solution must be able to provide a detailed report of individual client/ endpoints and must contain the following information, at minimum: o Hostname o Last Scan o Any pending scan request o IP Address o Username logged in o Agent installed date	
29	The Solution must be able to report on the preliminary status of analyzed host machines/ clients/ endpoints with below classification: o Compromised o Suspected Compromised o Clean o No Data	
30	The Solution must be able to export reports as HTML, PDF, and Excel, etc..	
31	The scan report must provide a preliminary assessment of the state of the client at the end of the scan, accompanied with supporting detail to support the result.	
32	The solution must support agent capping for CPU and memory utilization.	
33	Solution must provide utility to deploy agents.	
34	Solution must provide monthly reports and SOC Team shall review the same and take necessary actions.	

L	Server Security & Anti-Ransomware	
1	Server Security	Compliance (Yes / No)
i	The Selected Bidder shall provide name and other details of the Solution.	
ii	The Solution must provide security monitoring and protection across physical and virtual servers including anti-malware, fine grained intrusion detection and prevention, Application whitelisting, real-time file integrity monitoring, configuration monitoring & consolidated event logging.	
iii	The Solution must have out of the box Host IDS and IPS Policies. These prebuilt policies for Windows & RHEL environments must monitor and prevent suspicious server activity.	
iv	The Solution must have compensating controls to restrict application and operating system vulnerabilities to be exploited.	
v	The Solution must have file and system tamper detection and application whitelisting capabilities.	
vi	The Solution must have application control to lock down configuration settings for file systems and be able to block use of removable media.	
vii	The Solution must detect system files and registry entries on modification or deletion.	
viii	The Solution must provide alert to administrators for generated events. Actions must include alerting the administrator and logging the event.	
ix	The Solution must provide near real-time event monitor allowing GIC Re & Bidder's SOC Team to see events as they happen, view details (user, machine, events triggered, etc.) to allow a response to incursions or the compromise of data.	
x	The Solution must have granular policies to protect against zero-day threats and ransomwares and even the approved whitelisted applications must go through anti-malware scans.	
xi	The Solution must not be dependent on signatures only for protecting servers and VMs from malware and ransomware.	
xii	The Solution must simplify continuous monitoring and compliance reporting of GIC Re Hybrid Cloud Infrastructures for cyber security and compliance.	
xiii	The Solution must be a single tool to effectively identify policy violations and suspicious activities at an application or instance-level, in real-time, across the physical and virtual servers.	
xiv	The Solution must be able to create one base policy for set of servers and the same base policy can be replicated to other set of servers.	
xv	The Solution must not require updates to be rolled to client system to approve new applications to be executed.	
xvi	The Solution must not be dependent on any external verification of allowed/ banned application. It must be able to take its input based on local state of server system.	
xvii	The Solution must integrate with change management, data center automation, and configuration management database (CMDB) Solutions.	
2	Antivirus & AntiSpyWare For Servers	Compliance (Yes / No)
i	Solution must provide automated and centralized download and deployment of latest virus signature updates from the Internet to servers across the organization, across different Windows/ RHEL/ other platforms.	

ii	Solution must have the ability to detect and remove unwanted programs, toolbars, adware, spyware, dialers, etc. Post detection the actions that the antivirus performs must be the following (but not limited to): Alert/ Notify, Clean, Delete/ Remove, Move/ Quarantine, Prompt for Action.	
iii	The Solution must support file scan caching to avoid repetitive scanning of files which are unchanged since the previous scan.	
iv	The Solution must automatically scan whenever the I/O is happening from external devices and Network shares in real-time when accessed.	
v	The Solution must provide policies to lockdown the server like – change in registry, Internet Explorer file settings, Exe file execution etc. to block unknown zero-day attacks and reduce dependency on frequent signatures	
vi	The Solution must allow the On Demand Scanner to recognize the last scanned file and resume scanning from that file if an “On demand Scan” is interrupted.	
vii	The Solution must have the ability to control the amount of CPU resources dedicated to a scan process.	
viii	The Solution must be capable of blocking TCP/ IP ports on the VMs/ Servers and also creating exceptions for specified applications to use these blocked ports.	
ix	The Solution must be capable of integrating completely with EDR (at endpoints) and take actions.	
x	The Solution must Discover and Report the IP Address of the end -point system (infection source) that sent malicious code to the server and optionally, block further communications from the infection source end-point system for a configurable time or indefinitely.	
xi	The Solution must provide Self-protection from modifying or disabling Antivirus Client.	
xii	The Solution must scan system memory for installed rootkits, hidden processes, and other behavior that suggests malicious code is attempting to hide itself.	
xiii	The Solution must allow for automated rollback of virus definition from Central Console, if required.	
xiv	The Solution must have enhanced tamper protection that guards against unauthorized access and attacks, from viruses that attempt to disable security measures.	
3	Sandboxing & Anti-Ransomware	Compliance (Yes / No)
i	The Selected Bidder shall provide name and other details of the Solution.	
ii	The Solution must provide security monitoring and protection across physical and virtual servers and east-west and north-south Network Traffic.	
iii	The Solution must integrate with SIEM, SOAR, Server Antivirus & EDR to provide complete ransomware prevention of entire environment.	
iv	The Solution must perform sandboxing of files, packets, etc. to detect and prevent any threats.	
v	The Solution must have sandboxing capability to prevent against a new class of threats by utilizing comprehensive protection.	
4	Firewall & HIPS	Compliance (Yes / No)
i	The Solution must have host firewall capabilities to directly block unwanted traffic.	

ii	Solution must support Stateful packet inspection functionality/ dynamic packet filtering functionality.	
iii	The Solution must have the ability to help the administrator to create policies based on – User defined, Adaptive mode and Learn mode.	
iv	Solution rules must have capability to filter traffic based on source and destination IP address, port, MAC address, etc.	
v	The Solution must support multiple virtualization platforms to secure workloads regardless of where it resides and must protect entire GIC Re infrastructure including legacy systems that cannot be patched.	
vi	The Solution must have the ability to work in protection and detection mode.	
vii	Solution must detect reconnaissance activities such as port scans.	
viii	Solution must provide policy inheritance exception capabilities.	
ix	Solution must have the ability to lock systems (prevent all communication) except with management server.	
x	Solution must support Security Profiles that allows Firewall rules to be configured for groups of systems, or individual systems.	
xi	The Solution must provide adequate information to the SOC Team to carry out the investigation of security incidents	
5	File Integrity Monitoring	Compliance (Yes / No)
i	The Solution must be able to monitor System Services, Installed Programs and Running Processes for any changes.	
ii	The Solution must be capable of detecting or tracking read, write, execute, delete & change permissions on specified file(s)/ folder(s)/ Network Share(s).	
iii	The Solution must perform integrity checking of files by file hashing.	
iv	Solution must be able to track addition, modification, or deletion of Windows registry keys and values, access control lists, or web site files.	
v	The Solution must perform file hashing locally rather than transferring the file across a network to be hashed on a central server and thus impact network bandwidth.	
vi	In the Event of unauthorized file change, the Solution shall report what changed, who made the change, how they made it and precisely when they did so.	
vii	The Solution must offer intelligent filters which are pre-configured to track the relevant objects on the system, for each standard Operating System covering systems files including Windows, RHEL, etc. It must also include application filters for Apache, Tomcat, WebSphere and JBOSS, IIS, WebLogic, WebSphere, etc., and must be customizable.	
6	Application Whitelisting	Compliance (Yes / No)
i	The Solution must be capable of whitelisting applications by executable name or hash values or file signature flags.	
ii	The Solution must be capable of whitelisting applications using a dynamic trust model and innovative security features without requiring signature updates or labor-intensive list management.	
iii	The Solution must be able to create inventory of a target system and hence report on installed software and applications on client machines.	

iv	The Solution must be capable of securing whitelisted applications within permission-controlled sandboxes or use virtual patch to protect files.	
v	Solution must protect the operating system whilst at the same time allowing for Whitelisting and Blacklisting functionality for Applications.	
vi	The Solution must be able to protect whitelisted applications including their data, logs, and configuration files.	
7	Log Inspection	Compliance (Yes / No)
i	Solution must have a Log Inspection module which provides the ability to collect and analyze operating system, databases and applications logs for security events.	
ii	Solution must provide predefined out of the box rules for log collection from standard applications like OS, Database, Web Servers etc. and allow creation of custom log inspection rules as well.	
iii	Log Inspection rules must allow setting of severity levels to reduce unwanted event triggering.	
iv	Solution must have ability to forward events to SIEM system for correlation, reporting and archiving.	
v	Solution must have Security Profiles allowing Log Inspection rules to be configured for groups of systems, or individual systems.	
8	Management and General Features	Compliance (Yes / No)
i	The Solution must support for following platforms: o Windows o RHEL o Linux	
ii	Solution must be able to manage all physical, virtual and cloud infra through centralized single management console.	
iii	The Solution must be able to deliver all the features i.e., Antimalware, FW& HIPS, Application whitelisting, FIM and event logging through a single agent.	
iv	The Solution must have a small overhead footprint such that it minimizes impact on system resources.	
v	Once the policies are deployed, the agents must continue to enforce the policies whether the management server is available or not.	
vi	The Solution must provide System Events to view a summary of security-related events, primarily for the Management server and including Agents' system events. All administrative actions must be audited within the System Events.	
vii	The Solution must support forwarding of alerts through SMS and E-Mail.	
viii	Solution must allow creating multiple dashboard views.	
ix	Solution must maintain full audit trail of administrator's activities.	
x	The Solution must have Deep Packet Inspection capabilities to protect operating systems, off-the-shelf applications, and custom web applications against attacks such as SQL injections, cross-site scripting, etc.	

xi	The Solution must be able to enforce a server system in a “gold image” as decided by the Selected Bidder's team.	
xii	The Solution must allow Selected Bidder's team to remote view the constituents of a system image and hence compare the image with a well-defined gold image.	
xiii	In the absence of a gold image, the Solution must provide for the capability to enforce a current good state as decided by the Selected Bidder's team.	
xiv	The Solution must provide Selected Bidder's & GIC Re's team gain visibility into the security status of all VMs and can monitor hypervisor-to-VM relationships in near real time.	
xv	The Solution must have capability to secure unpatched applications and systems running on legacy and End-of-life platforms using virtual patching.	
xvi	The Solution must restrict physical or remote access to the machine to override protection.	
xvii	The Solution must be able to detect and prevent the advanced persistent threats which come through executable files like PDF files, Flash files, RTF files and and/ or other objects.	
xviii	The Solution must provide the dynamic management of execution capability of applications on a server system, prevent unauthorized registry manipulation and in memory protection of application.	
xix	The Solution must support unique real time update based on over the web cloud technology to provide real time signatures for dynamic and latest threats to reduce the dependency on Daily Signature updates.	

M	NGFW, IPS & Proxy	
1	Solution	Compliance (Yes/No)
i	The Selected Bidder shall provide name and other details of the Solution.	
ii	The Solution vendor must be in Leader's quadrant of Gartner Enterprise Solution report of 2021.	
iii	The Solution must be Virtual based, Reliable, purpose-built, hardened operating system supporting State, full policy inspection technology.	
iv	The Solution must support NAT64, NAT46, DNS64 & DHCPv6.	
v	The Solution must support WAN links load balancing and fail-over for at least 4 links.	
vi	The Solution must support load balancing and fail-over based parameters such as Latency, Jitter, Packet-Loss, etc.	
vii	The Solution must have integrated Traffic Shaping functionality.	
viii	The Solution must support Virtualization (Virtual Solution, Security zones and VLAN).	
ix	The Solution & IPSEC VPN module must have ICSA or other equivalent Certification.	
x	The Solution must utilize inbuilt hardware VPN acceleration: o IPSEC (DES, 3DES, AES) encryption/decryption o SSL encryption/decryption	
xi	The system must support 2 forms of site-to-site VPN configurations: o Route based IPSEC tunnel o Policy based IPSEC tunnel	
xii	The Solution must support IPSEC site-to-site VPN and remote user IPSEC VPN in transparent mode.	
xiii	The Solution must provide IPv6 IPSEC feature to support for secure IPv6 traffic in an IPSEC VPN.	

xiv	NGFW Solution must not require reboot to push security policies or any signature (IPS, Anti-malware etc.) update.	
2	Intrusion Prevention System	Compliance (Yes/No)
i	The Solution must be able to inspect SSL sessions by decrypting the traffic.	
ii	The Solution must have at least 13,000 signatures.	
iii	IPS Signatures must be updated in different ways: manually, via pull or push technology. Selected Bidder's Team must schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available.	
iv	In event if Solution must cease to function, it must fail over by default and be configurable so that crucial network traffic must not be blocked, and system must continue to operate while the IPS problem is being resolved.	
v	The Solution must have capability to protect against Denial of Service (DOS) and DDOS attacks. must have flexibility to configure threshold values for each of the Anomaly. DOS and DDOS protection must be applied, and attacks stopped before Solution policy lookups.	
vi	IPS signatures must have configurable actions like: o terminates a TCP session by issuing TCP Reset packets to each end of the connection o silently drops traffic in addition to sending an alert and logging the incident.	
vii	Signatures must have severity level defined to it so that the Selected Bidder's Team can understand and decide which signatures to enable for what traffic (e.g., for severity levels: high, medium, low).	
3	Application Control Features	Compliance (Yes/No)
i	The Solution must have at least 4000 application signatures database.	
ii	The Solution must have the intelligence to identify & control popular IM & P2P applications.	
iii	Solution must have capability to do Cloud application-based routing not by means of manually adding IPs and or FQDNs i.e., Solution must have database of O365 readily available to select as destination address in Solution policy and destination address in static route configuration to give ISP path.	
iv	Selected Bidder must keep updating Application's backend FQDNs and IP addresses database on regular basis.	
4	Anti-virus, Anti-bot & Advanced Persistent Threat (APT)	Compliance (Yes/No)
i	The Solution must be able to block, allow or monitor only using AV signatures and file blocking based on Solution policy or Solution authenticated user groups with configurable selection of the following services and their equivalent encrypted versions: HTTP, SMTP, POP3, IMAP, FTP, etc.	
ii	Solution must offer both scanning options - proxy mode and flow (streaming) mode.	
iii	Solution must be able to block or allow oversized file based on configurable thresholds for each protocol types and as per Solution policy.	
iv	Solution must include Anti-bot capability using IP reputation DB, terminate botnet communication to C&C servers also. Selected Bidder must add additional license if it is required.	

v	Solution must have 30000+ botnet definitions in its database and must be updated on regular basis to protect from new definitions.	
vi	The Solution shall include advance malware protection like: o Virus Outbreak Protection o content disarms and reconstruction (CDR)	
vii	Solution must have cloud sandbox functionality to protect environment from Advance Persistence Threats. In case any additional license is required, Selected Bidder must include it in proposal.	
viii	The Solution must utilize a state-full attack analysis to detect the entire infection lifecycle and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.	
ix	Solution must be able to monitor encrypted traffic.	
5	Web Filtering Functionality/ Proxy	Compliance (Yes/No)
i	The Solution must have in-built Web Filtering Functionality.	
ii	The Solution must have in-built Web Proxy functionality.	
iii	Many web sites use HTTP redirects legitimately; however, in some cases, redirects may be designed specifically to circumvent web filtering, as the initial web page could have a different rating than the destination web page of the redirect. The Solution must be able to rate redirected sites.	
iv	The Solution must be capable of rating URLs by domain and IP address which sends both the URL and the IP address of the requested site for checking, providing additional security against attempts to bypass the rating system.	
v	The Solution must have option to rate web resource based on their Domain rating	
vi	The Solution must have an option of redirecting infected machines/ requests to fake portals.	
6	High Availability	Compliance (Yes/No)
i	The Solution must have built-in high availability (HA) features without extra cost/ license or hardware component.	
ii	The Solution must support stateful session maintenance in the event of a fail-over to a standby unit.	
iii	The Solution must maintain event log, send SNMP traps, send alert email when fail-over occurs.	
iv	The Solution must provide high availability clustering features, enhanced reliability and load sharing.	
7	Administration, Management and Logging Functionality Feature Requirements	Compliance (Yes/No)
i	Solution must provide and manage Virtual Machine for centralized management & reporting to store logs and reports.	
ii	Centralized management must show per location/ device WAN links status - latency, delay, packet loss, etc.	

iii	Logs must also show real-time per user statistics which must include sent/ received bytes, no. of sessions, threat score, bandwidth usage, sent/ received packets & source IP of user, destination country detail, etc.	
iv	Solution must have ready-made report template such as Top Users, Top Application, Top Destinations, Interface utilization per device per link, CPU and Memory usage of each device, malware/ threat analysis report, etc.	
v	Solution must also send an alert in case of WAN link failure and recovery.	
vi	Solution must support configuration rollback.	
vii	Solution must be tightly integrated with SIEM.	
viii	All network wide configurations shall be from the centralized management appliance.	
ix	Solution Audit Trail must contain at a minimum: o The name of the administrator making the change o The change made o Time of change made	

N	DDoS Detection & Mitigation	
1	Multi-vendor/ technology-agnostic capability.	Compliance (Yes/No)
i	Please share details of the DDoS technology OEMs used by Selected Bidder that will be used in the detection and mitigation of the DDoS attacks.	
2	Detection of all types of DDoS attacks	Compliance (Yes/No)
i	The Solution must detect attacks in: o Volumetric Layer 3 and layer 4 o Application Layer 7	
ii	The Solution must perform automatic detection & mitigation of DDoS Attacks.	
iii	The Solution must have ability to support full proxy of traffic when using DNS re-direction.	
iv	The Solution must have ability to provide carrier agnostic DDoS mitigation service.	
v	The Solution must support for mitigation events of up to 72 hours in duration with full access to SOC team anytime during the event.	
vi	The Solution must have ability to block traffic based on specific botnet signatures and intelligence feed derived from well-known security research teams.	
vii	The Solution must allow the submission of black or whitelists on demand during mitigation events for application on the mitigation systems.	
3	Capacity and Scale	Compliance (Yes/No)
i	The Solution must have Intelligent mitigation capacity. Intelligent mitigation capacity means protocol analysis driven mitigation engine that performs intelligent anomaly detection, signature-based analysis, protocol aware analysis, and intel driven detection and mitigation of botnet and known bad actors.	
ii	The Solution must be able to deliver DDoS mitigated traffic as close to the destination as possible.	

4	Service Levels	Compliance (Yes/No)
i	The Selected Bidder must provide 99.99% overall service uptime excluding pre-scheduled maintenance windows.	
5	Reporting	Compliance (Yes/No)
i	Post incident reports must be delivered after every mitigation event and include specific details about the event, date, time, traffic passed and dropped.	
ii	During mitigation events, ongoing status messages must be provided at minimum of every 2 hours.	
iii	A dedicated portal must be available to view DDOS alerts and extract reports.	
iv	On demand during or after a mitigation event, GIC Re must be able to request and receive screen shots/ details from the intelligent mitigation system being used to perform the mitigation.	
v	On demand during a mitigation event, GIC Re may request and receive list of source IP addresses that are dynamically being blacklisted in the mitigation.	
vi	Attack and mitigation notification by means of E-mail, phone must be available.	

O	SD-WAN	
1	Solution Architecture	Compliance (Yes / No)
i	The Selected Bidder shall provide name and other details of the Solution.	
ii	The Solution must allow network service insertion & service chaining to expand the agility and utility of the network. The Solution must have ability to do services chaining with external PNFs or hosted VNFs. The VNF capability must be available on any SD-WAN edge devices.	
iii	The Solution must be able to load balance across links simultaneously.	
iv	The Solution must support end-to-end packet classification, marking, and bandwidth allocation.	
v	The Solution must support native firewall to secure the Branch/ Spoke/ Hub locations against malware attacks.	
vi	The Solution must support advance security features like: NGFW, Intrusion Prevention System (IPS), Anti-virus, Malware protection, DNS/HTTP proxy, etc.	
vii	The Solution must build dynamic IPSEC tunnels using Asymmetric encryption (DH group) and must generate unique key for each site for better security.	
viii	The Solution must support Hub-Spoke, Full-Mesh, Spoke-Hub-Hub-Spoke and Partial Mesh topologies.	
ix	The Solution must support CODEC based Voice and Video traffic analysis and traffic management.	
x	The Solution must only allow dynamic tunnels to be created without any static overlays between branch devices and the hub device. SLA probes shall be originated based on the data traffic availability for the branch location.	

xi	The Solution must support interchangeable WAN & LAN ports on the devices to achieve better scalability.	
xii	The Solution must implement a NGFW with Access Lists and/or Time-based Access lists to provide supervision and control on the branch device that can be centrally provisioned and managed from the software defined network controller.	
xiii	The system must be able to monitor, and report top 10 applications by usage across all branch locations, in one branch location along with the data rate and flow usage.	
xiv	The Solution must support both packet & flow-based load sharing across all links simultaneously to achieve better application performance.	
xv	The Solution must allow definition and enforcement of traffic load balancing policies that allow utilization of all the available WAN links simultaneously.	
2	Security	Compliance (Yes / No)
i	Whether Solution supports end-to-end encryption?	
ii	Whether Solution supports web proxy for each branch/ spoke location?	
3	CPE capabilities	Compliance (Yes / No)
i	Bidders will describe the types of CPEs used in their different Solutions especially on: o Brands & models o Capacities o CPE catalogue covering different access line types such Ethernet, optical fiber, etc., o Max number of VNFs that can be installed on one CPE o others	
4	SD-WAN Infrastructure	Compliance (Yes / No)
i	The Solution must have Data and control planes separation.	
ii	Please describe how your SD-WAN Solution enables the separation of the data and control planes.	
iii	Provide detailed High- & Low-Level Architecture Diagram.	
iv	Describe the architecture of SD-WAN deployment? Number of controllers, redundancy, and high availability, etc.	
v	Describe: o How protection of the control plane is achieved for your proposed SD-WAN Solution o Security protection for the central infrastructure, i.e., firewall, DDOS, etc. o Advanced security protection for the SDWAN infrastructure.	
vi	The Solution must provide Secure and reliable access to Cloud and Internet breakout.	
vii	The Solution must have the ability to provide application visibility on the network and Analytics Reporting.	
viii	The Solution must have minimum 6 months of Data/ log retention.	
ix	The Solution must support interoperability with switches, routers, other devices of any OEM(s).	