RFP Document
for
Cybersecurity Maturity Assessment, Architecture Design, Policy Framework and Compliance Certification processes as per ISO 27001 guidelines

RFP No.
GMDC/CO/IT/Cybersecurity/01/2023-24

Last date for submission of queries	**:**	31-08-2023 UPTO 18:00 HRS
Last date for submission of online bid	**:**	15-09-2023 UPTO 18:00 HRS
Last date for submission of physical documents	**:**	15-09-2023 UPTO 18:00 HRS
Technical bid opening date & time	**:**	15-09-2023 UPTO 18:30 HRS

Gujarat Mineral Development Corporation Limited

(A Government of Gujarat Enterprise)
CIN No.: L14100GJ1963SGC001206
Khanij Bhavan, 132 ft. Ring Road, Nr Gujarat University Ground,
Vastrapur, Ahmedabad- 380052 India

INDEX

ACRONYMS 6

SECTION -1 INTRODUCTION 9

SECTION – II PROJECT BRIEF AND DETAILS 10

PROJECT BRIEF 10

TYPES OF CYBERSECURITY RISK ASSESSMENTS 10

Cloud Security 10

Third-Party 10

Ransomware Simulator 11

Incident Response Readiness 11

Vulnerability Assessment 11

Penetration Testing 11

GMDC CYBERSECURITY ASSESSMENT – OBJECTIVES 11

SECTION 3- SCHEDULE OF PROPOSED PROJECT AND BIDDING DETAILS 13

Project Implementation Timelines 13

Completion details 13

Bidding option for the ISA 13

RFP notice and information for online bidding 13

SECTION 4- DETAILS OF EXISTING LOCATIONS, USERS AND IT INFRASTRUCTURE 18

SECTION 5 – SCOPE OF WORK 20

SECTION 6 – PRE-QUALIFICATION CRITERIAS 22

SECTION 7 - INSTRUCTION TO ISAs 25

Section Details: - 25

Cost of bidding 25

Bidding documents 25

Due Diligence 26

Clarification on bidding documents 26

Amendment of bidding documents 26

Contact Details 26

Language of bid 26

Consortium / Joint Venture: 27

Statutory Obligations 27

Section comprising the bids 27

The Bid Security (Physically Submission at GMDC) 27

Technical Section 27

Price bid Section 28

Bid forms 28

Fraudulent & corrupt practice 28
Lack of information to ISA 28
Work Order obligations 28
Bid price 28
Bid currency 29
Period of validity of bids 29
Format and signing of bid 29
Bid due date 30
Late bid 30
Modification and withdrawal of bid 30
Opening and evaluation of bids 30
Evaluation process 30
Evaluation of bid 30
Evaluation of technical bid 31
Announcement of bids 31
Bids not considered for evaluation 31
Criteria for evaluation of bids 31
QCBS (Quality cum Cost Basis Selection) introduction and details related to the same 32
Criteria for evaluation and comparison of technical bids. 32
Opening and comparison of the financial bids 34
Contacting GMDC 35
Rejection of bids 35
Choice of Firm: 35
Procurement Process 35
Award of work order 35
Notification of award, signing of Service Level Agreement and Signing of Non-Disclosure Agreement(NDA) 35
Purchase order issuance 36
Force majeure 36
  Force majeure event 37
  Force majeure exclusions 38
  Procedure for calling force majeure 38
Service Level Agreement obligations 38
Amendment to the Service Level agreement 38
Use of Service Level Agreement documents and information 38
Assignment & sub contracts 38
  Assignment by ISA 38
Resolution of disputes 39

Arbitration 39
Jurisdiction 39
Taxes & duties 39
Service Delivery norms 39
Bankruptcy 39
Payments terms 40
Service terms 40
Penalty clause 40
Project implementation 41
Software licenses (wherever applicable) 42
Installation of additional hardware (wherever applicable) 42
Support from external agency (if applicable) 42
Limitation of liability: 42
Termination for convenience: 42
Risk purchase: 42
Foreclosure: 43
Participation of ISA in the SITC RFP for procurement of Security Services and Hardware 43
SECTION – 8 SPECIFICATIONS AND PROCESS DEFINATIONS FOR TASK DEFINED IN SOCOPE OF WORK 44
IT Asset Discovery (For existing infrastructure at all locations) 44
Security Hardening (Policy review and Assessment) 44
Vulnerability Assessment and Penetration Testing 44
Vulnerability assessment and Penetration Testing for Network and Security Infrastructure 44
Vulnerability assessment and Testing for Application Testing (Web based/ ERP/ Website/ Database /APIs) 45
Vulnerability assessment and Testing for Cloud based services (SAAS/PASS/IAAS) 48
Vulnerability assessment and Testing of End Points (Desktops/Laptops/Tablets/BYOD devices getting connected to the network) 49
Vulnerability assessment and Testing of CCTV NVRs/CCTV Servers, Access and Biometric, IP Phones, IP SCADA systems in mines and all IOT devices getting connected to the network 50
Vulnerability Assessment and PET if required for indoor wireless solutions at Head Office and RF Links installed in mines 52
Assessment for Security gaps and enhancement recommendation for Microsoft 365 Email 52
Red Team Testing activity post VAPT and implementations of Audit recommendations 53
Digital Forensics Readiness Assessment 54
Compromise Assessment 55
SECTION -9 ARCHITECTURE, POLICY AND FRAMEWORK FORMULATION FOR Additional SECURITY SOLUTIONS 56
Security Architecture 56

Monitoring and Management 56
Analytics for Security Operations centre 57
Incident Response, Business Continuity and Disaster Recovery Plans 57
Project Management (during procurement and implementation of hardware / software as per architecture recommendations) 58
SECTION -10 USER TRAINING FOR CYBERSECURITY AWARNESS, POLICY IMPLEMENTATION 59
SECTION -11 AUDIT COMPLIANCE CERTIFICATIONS (TO BE INITIATED POST COMPLETION OF AUDITS/CORRECTIONS/DEPLOYEMENT OF ALL HARDWARE AS RECOMMENDED) 60
Structure of the standard 60
Mandatory requirements for certification 61
SECTION -12 UNPRICED BOQ FOR TECHNICAL DETAILS OF TOOLS, MANPOWER DETAILS 63
Vulnerability Assessment and PET if required for indoor wireless solutions at 64
Assessment for Security gaps and enhancement recommendation for Microsoft 365 Email solutions being used by GMDC 64
SECTION -13 PRICED BOQ FOR TECHNICAL DETAILS OF TOOLS, MANPOWER DETAILS 66
Vulnerability Assessment and PET if required for indoor wireless solutions at 67
Assessment for Security gaps and enhancement recommendation for Microsoft 365 Email solutions being used by GMDC 67
SECTION-14 ANNEXURES 69
Annexure – I - Format of Earnest Money Deposit in the form of Bank Guarantee 69
Annexure – II: Performance Bank Guarantee Format 71
Annexure – III: Earnest Money Deposit & RFP Fee Details 73
Annexure IV - RFP LETTER FORM 74
Annexure V – DECLARATION FOR NON BLACKLISTING 75
Annexure VI Work Experience details -as mentioned in the Pre- qualification criteria 76
Annexure VII Financial Strength of the ISA 76
Annexure VIII Manpower Details on ISA Roll 77
Annexure IX – Bank List 78

ACRONYMS

List of Acronyms used in the RFP		
Sr. no	**Acronym**	**Full Form**
1	ACL	Access Control List
2	AI	Artificial Intelligence
3	API	Application Programming Interfaces
4	App	Application
5	APT	Advanced Persistent Threats
6	BC	Business Continuity
7	BEC	Business Email Compromise
8	BIOS	Basic Input Output System
9	BOQ	Bill of Quantities
10	BYOD	Bring Your Own Device
11	CCTV	Closed Circuit Tele Vision
12	CERT	Computer Emergency Response Team
13	CMA	Cyber Maturity Assessment
14	CMS	Content Management System
15	CSP	Cloud Service Provider
16	CSRF	Cross-Site Request Forgery
17	CVE	Common Vulnerability and Exposures
18	CVSS	Common Vulnerability Scoring System
19	DDoS	Distributed Denial of Service
20	DoS	Denial of Service
21	DR	Disaster Recovery
22	DSS	Data Security Standard
23	EASM	External Attack Surface Management
24	EHS	Environment Health and Safety
25	EMD	Earnest Money Deposit
26	ERP	Enterprise Resource Planning
27	FTP	File Transfer Protocol
28	FY	Financial Year
29	GMDC	Gujarat Mineral Development Corporation
30	GST	Goods and Services Tax
31	HIPAA,	Health Insurance Portability and Accountability Act
32	HP	Hewlett Packard
33	H-PoE	High Power over ethernet
34	IAAS	Infrastructure As A Service
35	ID	Identification
36	IOA	Indicators Of Attack
37	IOC	indicators of compromise
38	IOT	Internet of Things
39	IP	Internet Protocol
40	IR	Incident Response
41	ISA	Information Security Auditor
42	ISMS	Information Security Management System
43	ISO	International Organization for Standardization

List of Acronyms used in the RFP

Sr. no	Acronym	Full Form
44	ISO	International Organization for Standardization
45	IT	Information Technology
46	LFI	Local File Inclusion
47	LLP	Limited Liability partnership
48	LoI	Letter of Intent
49	MATE	Man, at the end
50	M-Gig	Multi Gigabit
51	MITM	Man in the Middle
52	ML	Machine Learning
53	MPLS	Multi Protocol Label Switching
54	MWhr	Mega Watts per Hour
55	NAS	Network Attached Storage
56	NIST	National Institute of Standards and Technology
57	NVR	Network Video Recorded
58	OS	Operating System
59	OS	Operating System
60	OWASP	Open Web Application Security Project
61	PAAS	Platform As A Service
62	PBG	Performance Bank Guarantee
63	PC	Personal Computer
64	PCI	Payment Card Industry
65	PET	Penetration Testing
66	PF	Provident Fund
67	PMC	Project Management Consultant (PMC)
68	PO	Purchase Order
69	PQ	Pre Qualification
70	PSU	Public Sector Undertaking
71	PTZ	Pan Tilt Zoom
72	QCBS	Quality cum Cost Basis Selection
73	RFI	Remote File Inclusion
74	RFP	Request for Proposal
75	SAAS	Software As A Service
76	SAN	Storage Area Network
77	SCADA	Supervisory control and data acquisition
78	SFTP	SSH File Transfer Protocol
79	SIEM	Security Incident and Event Management
80	SOAR	Security Orchestration Automation and Response
81	SSL	Secure Sockets Layer
82	URL	Uniform Resource Locator
83	VAPT	Vulnerability Assessment and Penetration Testing
84	VPN	Virtual Private Network
85	WAF	Web Application Firewall
86	WAN	Wide Area Network
87	WFA	Works from Anywhere
88	Wi-Fi	Wireless Fidelity
89	CISA	Certified Information Security Auditor

List of Acronyms used in the RFP		
Sr. no	**Acronym**	**Full Form**
90	OSCP	Offensive Security Certified Professional
91	CISSP- ISSAP	Certified Information Systems Security Professional – Information Systems Security Architecture Professional
92	ISO 27000 LA	ISO 27000 Lead Auditor

SECTION -1 INTRODUCTION

Gujarat Mineral Development Corporation Ltd. (GMDC) is one of India's leading mining and mineral processing companies. For more than five decades, we have been engaged in the development of the ample mineral resources of the state. A zero-debt company, we're ranked 486th among India's Fortune 500 Companies (2022) and among the Top-5 organisations by market capitalisation in the mining sector.

GMDC is India's second largest Lignite-producing company. We're the leaders in Lignite exploration and supply in Gujarat. Mining lignite from deposit-rich areas across the state, we market it to various high-growth industries, including textiles, chemicals, ceramics, bricks and captive power

GMDC is involved in the exploration of Bauxite, Fluorspar, Manganese, Silica Sand, Limestone, Bentonite and Ball Clay. They find application across diverse industries, from manufacturing of hydrofluoric acid and purifying water to manufacturing glass and ceramic ware, and drilling oil.

GMDC has a sizeable presence in the energy sector. We have a diversified portfolio of Thermal power projects and renewable power generation projects comprising wind and solar power. We ventured into harnessing renewable sources of energy more than a decade ago and are readying for a sustainable future. Over the years, we've generated 2522416+ MWhr of Green Energy.

GMDC has embarked on a journey of transformation. GMDC has a huge stock of mined out Silica Sand and similar in-situ deposits in one of its upcoming projects. As a part of forward integration, GMDC is seeking to explore new avenues in diversified sector in silica sand as well as other allied industries by value addition for manufacturing of float glass, solar panels, etc. Envisaging suitable market potential, we're investigating new avenues in diversified sector in bauxite and other allied industries by value addition of plant and non-plant grades of bauxite.

As a high demand is being forecast for cement, GMDC is exploring new opportunities for utilisation of cement grade Limestone for cement industry and focusing on capacity augmentation, introduction of alternate market structures, possible diversification prospects, value additions and opportunities that the industry might require.

GMDC's sustained efforts at consolidating their leadership position are complemented by appointing professionals with proven expertise. Additionally, there is an increased focus on working with strategies advisory consultancies and project management consultants. Combined with initiatives in value addition, forward integration and portfolio expansion, they will help augment our financial standing as befitting a stalwart in mining and mineral processing.

GMDC is currently undergoing a transformation journey. It aims to increase the productivity and efficiency of its current mining operations on one hand. It is planning related diversifications in several high value projects on the other hand.

GMDC's Information Technology structure is required to gear up to this transformation. It also needs modernisation and updation to usher in higher productivity and efficiency. Thus, GMDC is in the process of undertaking several IT and digital transformation related projects for which it intends to select System Integrators/ ISAISAs (collectively the "IT Agencies ") through competitive and transparent procurement processes.

With the enhancement in IT part it is necessary to review the Security readiness and enhancements required to support the above-mentioned project. With this objective GMDC is inviting bids for Cybersecurity Maturity Assessment, Architecture Design, Policy Framework and Compliance Certification processes as per ISO 27001 guidelines.

SECTION – II PROJECT BRIEF AND DETAILS

PROJECT BRIEF

Advances in information technology have allowed businesses to enhance collaboration between team members, improve productivity, and generate more revenue. While the impacts of these advances have primarily been positive, increased reliance on digital assets has also given way to a sharp rise in cyberattacks. Considering the above fact, it is important for the organizations be cyber resilient.

Cyber Resiliency is the ability to anticipate, protect against, withstand, and recover from adverse conditions, stresses, attacks, and compromises of cyber-enabled business.

Assessments and Audit form an important part of the organization move towards cyber resiliency.

As the name suggests, a cybersecurity assessment is a thorough review and evaluation process that focuses on an organization's data security protocols. These assessments are designed to analyze the health of a company's cybersecurity infrastructure and identify any potential vulnerabilities that may make it susceptible to a data breach.

Cybersecurity risk assessments not only locate weaknesses in a company's IT architecture but also provide suggestions for remedying said vulnerabilities.

Each cybersecurity assessment will vary in both complexity and scope, depending on the industry that an organization operates within and which firm is conducting the review.

For instance, a company that has a well-established cybersecurity protocol may want to conduct an assessment that analyses its overall resiliency to an attack. Conversely, a business that is not confident in its current cybersecurity strategy might want to conduct a more comprehensive assessment that evaluates all IT components.

TYPES OF CYBERSECURITY RISK ASSESSMENTS

At their core, all cybersecurity risk assessments are designed to help prevent cyberattacks. However, there are several different types of assessments, each of which serves a specific purpose. Some of the most commonly used cybersecurity risk assessments include the following:

Cloud Security

Virtually every major organization relies on cloud-based assets in order to support their IT infrastructure. In light of this fact, it is essential to perform risk assessments that are focused solely on cloud security. These assessments identify potential vulnerabilities in cloud infrastructure and help organizations mitigate these risks via governance and control management protocols.

Third-Party

Unfortunately, partnerships with third-party ISAs can often provide hackers with a means of surreptitiously penetrating an organization's IT infrastructure. However, these partnerships have become essential in our increasingly interconnected global marketplace.

Therefore, third-party risk assessments must be routinely conducted to identify any vulnerabilities that are created because of these partnerships. These assessments primarily focus on risks related to the sharing of data and network assets.

Ransomware Simulator

Ransomware attacks can be particularly damaging to an organization. During a ransomware attack, hackers will hold a company's assets and data hostage until they pay a ransom, which can be as high as several million dollars.

A ransomware sim is designed to help organizations assess the potential impact of a successful ransomware attack. These simulations provide valuable information, such as the average time it takes to detect an attack and how long it takes the company to respond.

Incident Response Readiness

Much like ransomware simulations, incident response readiness assessments can help a business analyze its ability to mitigate the impacts of a successful cyberattack.

By conducting this type of assessment, organizations can gain detailed information regarding their response capabilities to resist viruses, malware, and other types of attacks. Cumulatively, the information gathered from simulations and readiness assessments will significantly improve a company's ability to respond to cyber threats.

Vulnerability Assessment

Perhaps the most frequent type of cybersecurity assessment is a general "vulnerability assessment." This automated form of testing is used to locate flaws within a specific asset or group of assets. The information obtained from vulnerability assessments is used to develop updates or patches.

Penetration Testing

Once a vulnerability assessment is completed, penetration testing can be performed to exploit any security flaws that were identified. Penetration testing can reveal how effective a hacker would be if they attempted to breach a network using existing vulnerabilities.

Post Assessment based on the Audit report

- Necessary configuration changes will be made by GMDC in the existing infra
- The ISA needs to design a security architecture based on the latest cybersecurity architectures for which detailed scope is defined
- Considering the new architecture designs and gaps identified in the audit report GMDC will procure and install the necessary hardware software. The ISA needs to do the complete project management during the implementation phase of this.
- Post completion of the above second assessment needs to be done
- After that test like Read Team and Compromise assessment need to be done
- On completion of the same the compliance certification process for get the ISO27000 certification needs to be initiated by the ISA

On completion of the above activities GMDC will proceed for the closure of the project.

GMDC CYBERSECURITY ASSESSMENT – OBJECTIVES

GMDC's Objective for conducting Systems audit of Information systems and IT infrastructure is to get reasonable assurance from a third-party auditor that:

- GMDC's information systems, machines, desktops, servers, BYOD and data are secure, and will remain complete, integrated, current, and accurate throughout processing.
- GMDC's information assets / resources (hardware/ software) are secured against unauthorized access / usage /damage / changes.
- GMDC's business continuity planning is adequate to ensure smooth customer Service, despite interruption to technology facilities for a significant amount of time

- GMDC's networks are adequately provided and protected.
- GMDC's computer operations are carried out in a controlled environment.
- GMDC can get independent assurance over effectiveness of controls exercised by out-sourced ISAs for technology services (Facility Management Services ISA)
- GMDC has appropriate controls in its entire systems development life cycle, project management and implementation activities.
- GMDC should comply for all required statutory requirements for ISO 27000 security certification

If the vulnerability reports pinpoints at discrepancies and gaps associated to systems configurations, application flaws, patch management aspects etc. then based on the recommendations of the audit report necessary changes will be incorporated by GMDC to achieve above mentioned objectives.

Post correction procedures and necessary changes once the above objectives are achieved GMDC in consultation with the ISA will initiate the certification process associated to Compliances.

SECTION 3- SCHEDULE OF PROPOSED PROJECT AND BIDDING DETAILS

Project Implementation Timelines

Sr. No	Deliverables	Tentative Timelines (Weeks) (Actual times lines to be defined by bidder in the unpriced BOQ)
1	Phase I as per the scope of work	04 weeks
2	Phase II as per the scope of work	16 weeks
3	Phase III (Project management activity)	06 weeks
3	Phase IV as per the scope of work (to be initiated post completion of Phase III)	26 weeks
4	Phase V as per the scope of work	15 weeks

Note:-*Weeks = 07 Calendar days*

Completion details

It is proposed to complete these works as per the given schedule. The nature of works broadly comprises as mentioned in Section -5 "Scope of Work"

Bidding option for the ISA

The ISA must bid for all the services and solutions and if the bid is not offered as above then the same will be liable to rejection.

RFP notice and information for online bidding

On behalf of GMDC the General Manager – IT invites online RFPs for RFP Document For Vulnerability Assessment, Penetration Testing **(VAPT),** Security Architecture and Security Policy Frameworks along with Compliance Certification processes as per ISO 27001 guidelines

1. **The schedule for e-bidding is as under:**

Brief Description of work	Cybersecurity Maturity Assessment, Architecture Design and Policy Framework and Compliance Certification processes as per ISO 27001
Project Implementation TimeLine	365 Days; It may further be extended on mutually agreed terms
Availability of RFP	GMDC website (www.gmdcltd.com) and nprocure portal (https://tender.nprocure.com) Price Bids shall be required to be submitted online on the nprocure portal (https://tender.nprocure.com).

EMD **(Earnest Money Deposit)**	Rs. 15,00,000 (Rupees Fifteen lacs Only) in any one of following form ➢ DD in favor of GMDC Ltd. Payable at Ahmedabad. ➢ RTGS/NEFT in the following bank account: Account Name: - Gujarat Mineral Development Corporation Limited ICICI Bank, Ahmedabad Branch, Ahmedabad Account Number: 002405019379 IFSC: ICIC0000024 ➢ FD/BG in favor of GMDC Ltd. ***Relaxation in terms of submission of EMD shall be given to the bidder who is holding valid Certificate issued under the MSME Act, 2016 on the date of submission of RFP.***
RFP Processing Fee	➢ Rs. 5000/- (Five thousand only) plus GST @ 18% aggregating to Rs. 5900/- payable by RTGS/NEFT in the following bank account: Account Name: - Gujarat Mineral Development Corporation Limited ICICI Bank, Ahmedabad Branch, Ahmedabad Account Number: 002405019379 IFSC: ICIC0000024 ***Relaxation in terms of submission of RFP Processing Fee shall be given to the bidder who is holding valid Certificate issued under the MSME Act, 2016 on the date of submission of RFP.***
Bid Validity Period	180 days from the date of opening of the preliminary bid, which shall be deemed extended unconditionally for further period of 60 days, if GMDC requires it.
Commencement of RFP	25/08/2023
Last date of submission of written request for clarification for pre-bid.	15/09/2023 up to 18.00 Hours
Pre Bid Meeting	Pre-Bid Meeting will be held on 01/09/2023 at 15.00 Hours. Venue of pre-bid meeting will be Corporate Office, GMDC, Ahmedabad (Gujarat). Maximum two members per Bidder will be allowed for the Pre-Bid meeting.
Last date of submission of Price bid through online	15/09/2023 up to 18.00 Hours
Last date of submission of physical documents i.e.	15/09/2023 up to 18.00 Hours at Corporate Office, GMDC Ahmedabad

EMD, RFP Fee, Technical Bid etc.	
Date for online opening of preliminary bid.	15/09/2023 at 18.30 Hours
General and Important Terms and Conditions	GMDC reserves absolute right/discretion to accept and/or reject any or all the RFPs received or invite fresh bid at any stage or split the work between more than one Bidders as the case may be. The Bidders are required to quote the rate strictly as per the terms and conditions mentioned in the RFP document. Conditional RFP shall not be entertained and will be rejected summarily without assigning any reasons. GMDC may issue amendments/corrigendum in the RFP documents, schedule, forms etc. at any time during the period between publication of notice and submission of bids of the RFP on website. The Bidders in their own interest are advised to visit the website regularly till the last date of submission of the bid. No separate newspaper advertisement will be released for amendments /corrigendum. GMDC reserves the rights to modify or alter any Condition of the RFP. The Bidders are advised to submit their price bid online on https://tender.nprocure.com only. Physical price bid shall not be accepted and shall be rejected summarily without assigning any reasons. Failure to submit bid online in stipulated time due to any reason whatsoever by any Bidder shall result in disqualification of bid. In such circumstances, bid submitted physically along with supporting documents, RFP processing fees, EMD amount etc. shall not be considered as bid submitted and the same will be returned back to the Bidder without opening the same. GMDC reserves the right to take suitable decision in this regard.

2. **Downloading RFP Documents**: RFP documents will be available on the website up to the date and time as shown above. Bidders who wish to participate in this RFP shall have to register on web site https://tender.nprocure.com
3. **Digital Certificate**: Bidders who wish to participate in online Bidding shall have to procure / should have legally valid Digital Certificate (Class III) as per Information Technology Act-2000, using which they can sign their electronic RFPs. Bidders can procure the same from any of the licensed certifying Authority of India or can procure from (n) code solutions – a division of GNFC Ltd, who are licensed Certifying Authority by Govt. of India. All RFPs shall be digitally signed. For details regarding digital signature certificate and related training the below mentioned addressee shall be contacted. In case Bidders need any clarification/assistance or training for participating in online RFP, they can contact the following office:-

(n) Code solutions, A division of GNFC
301, GNFC Info tower, Bodakdev, Ahmedabad – 380 054 (India)
Tel: + 91 26857316/17/18, Fax: +91 79 26857321,
Mobile: 9327084190, 9925117079; E-mail: nprocure@gnvfc.net

4. Bidders who already have a valid Digital certificate need not procure new Digital certificate.
5. **Online Submission of RFP**: Bidders can prepare and add on their bid *n* number of times prior to the last date and time prescribed for RFP submission. However, the RFP shall not be permitted to be edited in any case after the last date and time prescribed for submission of RFP as specified hereunder.
6. No written or online request in this regard shall be entertained. Bidders shall submit their RFP in electronic format only on above mentioned website and prior to the date and time mentioned above, and each RFP shall be digitally signed by the authorized person of the bidder. RFP documents shall be accepted in the electronic format online on nprocure.com. However, ISA have to submit copy of **physical technical bid with proper spiral biding, page number and indexing within time limit**.
7. A scan copies of all details as required shall be uploaded in electronic format only. During the opening of online technical bid if it is found that above details as mentioned are not submitted in electronic format, RFPs of such bidder shall not be considered.
8. The online RFPs can be up loaded as per time limit mentioned in the schedule. The RFP document comprises of two RFPs i.e. (i) Technical bid and (ii) Commercial bid.
9. In case of queries regarding RFP documents, the list of queries may be sent through email to: **tenderit@gmdcltd.co.in in prescribed format only as under:**

Sr. No	Bid Page no	Existing Clause no	Existing Clause	Query	Clarification/ Justification

Queries should be submitted in the XLS format. No other format of the file will be accepted.

10. **Opening of Technical RFP**: Technical RFPs shall be first opened online as per schedule mentioned in RFP.
11. Technical bid shall be evaluated as per procedures mentioned in the RFP documents. The decision of the committee on evaluation of the bids shall be final and binding to every Bidder.
12. **Opening of Commercial bid**: Commercial bid of only qualified Bidder whose technical bid is accepted shall be opened.
13. Bidder must invariably quote the rate online on every Commercial bid, failing which they shall not be allowed to participate in on line auction.
14. **Contacting Officer**: Further details/clarification if any will be available from the GMDC HO, GM IT (I/c) 3rd Floor, Khanij Bhavan,132 ft. Ring Road, Nr Gujarat University Ground, Vastrapur, Ahmedabad- 380052 India
15. RFPs without RFP fees, EMD and which do not fulfil all or any of the conditions of RFP document shall be rejected outright. RFP with incomplete details in any aspect shall also be rejected.
16. Conditional RFP shall not be accepted.
17. This RFP notice shall form a part of RFP document.

18. **The Bidders are advised to read carefully all the Instructions and conditions stipulated in the RFP documents.**
19. GMDC reserves the rights to reject any or all RFPs without assigning any reason thereof.
20. Bidders are bound by Government rules and regulations being issued from time to time.
21. Any kind of amendments / corrigendum shall be published only on-line and shall be final and binding to all Bidders.
22. The details of RFPs can be seen on website www.nprocure.com, https://tender.nprocure.com
23. The bid submitted by the Bidder shall have valid digital signature certificate.
24. Every Bidder shall mention his e-mail address in technical bid.

SECTION 4- DETAILS OF EXISTING LOCATIONS, USERS AND IT INFRASTRUCTURE

GMDC offices are located at Ahmedabad and other locations as mentioned below. Of the total locations mentioned in the above BOQ

LOCATION AND IT USERS DETAILS (TOTAL AND APPLICATION WISE) FOR EACH LOCATION

Sr._ no.	Location	Mining for	District	Total Endpoints
1	Head Office		Ahmedabad	700
2	Umarsar	Lignite	Kutch	
3	Panandhro	Lignite	Kutch	
4	Mata no Madh	Lignite	Kutch	
5	Gadhsisa	Bauxite	Kutch	
6	Surkha	Lignite	Bhavnagar	
7	Tadkeshwar	Lignite	Kutch	
8	Rajpardi	Lignite	Bharuch	
9	Kadipani	Flourspar	Chottaudepur	
10	Shivrajpur	Manganese	Panchmahal	
11	Bhatia	Bauxite	Dwarka	
12	Ambaji	Multi Metal	Banaskanta	
13	Akrimota	TPP	Kutch	
14	Guniyasar	Bauxite	Kutch	
15	Ratadiya	Bauxite	Kutch	
16	Daban	Bauxite	Kutch	
17	Roha Kotra	Bauxite	Kutch	
18	Maliya	Wind Power	Rajkot	Not connected to the GMDC Network
19	Godhsar	Wind Power	Porbandar	
20	Jodiya	Wind Power	Jamnagar	
21	Bada	Wind Power	Kutch	
22	Bhanwad	Wind Power	Jamnagar	
23	Rojmal	Wind Power	Bhavnagar, Amreli & Rajkot	
24	Panandhro	Solar	Kutch	
25	Lakhpat Punrajpur	Lignite	Kutch	Upcoming Mines that will be connected to the GMDC Network
26	Bharkhandham	Lignite	Kutch	
27	Damal Padia	Lignite	Bharuch	
28	Valia (EFG)	Lignite	Bharuch	
29	Ghala	Lignite	Surat	

As seen above there are 1000 users that are using different applications as mentioned in the matrix.

The details of the infrastructure, applications and websites that needs to be assessed are mentioned in the below table:

DETAILS OF ALL IP INFRASTRUCTURE LOCATED AT DIFFERENT LOCATIONS			
Sr. No.	**Location**	**HARDWARE CATEGORY**	**QTY**
1	**Head Office**		
	Data Centre and Hub rooms located at each floor	Core Switches	2
		Server Switches	2
		H-PoE M-Gig switches edge (Hub room)	8
		Smart switches edge Non-POE	8
		ERP Servers	3
		ERP SAN Switch	2
		ERP Storage	1
		Server SAN Management Console	1
		Tape Drive	1
		Blade Servers with 16 Blades	1
		NAS BOX	1
		Firewall	1
		Firewall Analyzer	1
		Rack Server	1
		Access Points	38
		Video Conferencing Codecs	1
		Biometric readers	3
		Link Load Balancers	3
		MPLS Router	2
		Primary MPLS Link	1
		Secondary MPLS Link r	1
		Internet Leased Line with router	1
		Internet Leased Line with router	1
		Weigh Bridge App API (Hosted in the Data center)	1
		Attendance Time and Management (Hosted in the data center)	1
		Customer Portal (Hosted in datacenter)	1
		Website (Hosted in cloud)	1
		Data Mining Software (Hosted in Data center)	1
		APAR Appraisal Software (hosted in Data Center)	
		PF Software (Hosted in Cloud)	1
		Link Load Balancers	3

SECTION 5 – SCOPE OF WORK

The scope of work with time schedule is defined in the table below

Sr. no.	Description of Task and Sub Tasks	Tentative Completion period in weeks . Actual timelines to be defined by the ISA
	PHASE I	
01	Review of IT Assets discovered and managed by GMDC through the appropriate tools. Post review if the ISA feels the needs of asset discovery in their tools then they can do the same or else use GMDC's data available in their tool	01
02	Security Hardening (Policy review and Assessment)	03
	PHASE II	
03	Vulnerability Assessments and Penetration Testing	12
3.1	Vulnerability assessment and Penetration Testing for Network and Security Infrastructure	
3.2	Vulnerability assessment and Testing for Application Testing (Web based/ ERP/ Website/ Database /APIs)	
3.2	Vulnerability assessment and Testing for Cloud based services (SAAS/PASS/IAAS)) for all hosted applications working in Cloud. Define the parameters and ways to check applications hosted in the cloud using SAAS model	
3.4	Vulnerability assessment and Testing of End Points (Desktops/Laptops/Tablets/BYOD devices getting connected to the network)	
3.5	Vulnerability assessment and Testing of CCTV NVRs/CCTV Servers, Access and Biometric, IP Phones, IP SCADA systems in mines and all IOT devices getting connected to the network	
3.6	Vulnerability Assessment and PET if required for indoor wireless solutions at Head Office and RF Links installed in mines	
3.7	Assessment for Security gaps and enhancement recommendation for Microsoft 365 Email solutions being used by GMDC	
04	Architecture, policy and framework formulation for additional security solutions that includes - Security Architecture design - Information Security Management system design - Security Operation Center design along with Analytics - Disaster recovery (DR) site design - Incident response, Business Continuity and Disaster recovery plan	04
	PHASE III	
05	Project Management Consultancy - Specification Review	16-20 week

Sr. no.	Description of Task and Sub Tasks	Tentative Completion period in weeks . Actual timelines to be defined by the ISA
	- Installation (Design Review), Configuration (Policy Review) of the newly Procured Equipment/ Software Licence / Solution. , Installation and Configuration of additional components as per the recommendation of the audit report and design of the security architecture (Procurement of Hardware and Software will be done through a separate bid) - Configuration changes as per the VAPT Audit report recommendations (Changes will be done by respective SI onboarded for new RFP)	
06	Primary User Awareness training as per the Training Module designed by the ISA (scheduled offline session to be conducted at all locations)	04-06
	PHASE IV	
07	Second round of VAPT audits post readiness of infrastructure as per the audit recommendation and security architecture	04-06
08	Compromise Assessment Audit	04
09	Digital Forensic Readiness Assessment	04
10	Red Team testing to check resilience of the complete infrastructure to cyber attacks	08
11	Mock Drill for Incident management and Business continuity using DR site	02
12	Publishing of complete ISMS policy post management approval and user training for creating awareness	04
	PHASE V	
13	Compliance certification process for ISO 27001 certificate (ISA will remain onboarded till the certificate is issued)	12-15

For all the tasks mentioned above works needs to be done as per the details given in the specifications sections and apart from the details the ISA should adapt the industry best practices for design, execution and project management if any of the details are missing

The phases defined is just for the understanding purpose of the ISAs. As such this is a single project and closure will be done post the completion of all the phases.
If between two phases some tasks of other phase can be done in some other phase parallelly then the ISA can work on that tasks.

SECTION 6 – PRE-QUALIFICATION CRITERIAS

PRE QUALIFICATON-CRITERIA TABLE		
	Criteria	**Supporting to be given**
1	**LEGAL ENTITY**	
	ISA should be a legal entity registered in India, since last 10 (Ten) years under either Indian Companies Act 1956/2013 or LLP Act 2008.	A copy of the Certificate of Incorporation
2	**GST REGISTRATION**	
	The ISA should have valid GST registration in India	GST Registration certificates issued by competent authority
3	**POWER OF ATTORNEY/ BOARD RESOLUTION**	A Board Resolution / authorization letter from the board of directors or Power of Attorney authorizing the RFP signing authority.
	The ISA should submit an authorization letter for authorizing the RFP signing authority for signing and submission of the RFP	
4	**Experience of Executing similar works associated to VAPT, Gap Analysis, Cybersecurity architecture Design, Cyber Security Policy Framework design, Compliance certification domain expertise and training management for cybersecurity in Government, PSUs and Corporates in India within the last three years** One project of similar nature costing not less than 5 Cr value of assignment to be awarded	Copy of Work Orders / Contracts AND Copy of Completion certificate from Client along with the copy of purchase Order.
5	**FINANCIAL CAPABILITY**	
	The ISA should have overall average annual turnover of at least INR 50 Crore in last 3 financial years (FY20-21, FY 21-22, FY 22-23). **The revenues of 50 Cr should be from the service revenue generated from services associated to cyber**	Certificate(s) from statutory auditor with all relevant details from the ISA. The ISA shall provide a copy of each of audited annual report to ascertain its turnover & net-worth.

PRE QUALIFICATON-CRITERIA TABLE

	Criteria	Supporting to be given
	security audits and security architecture designs	
6	**NON- BLACKLISTING/H OLIDAY LIST/NON-LIQUIDATION / COURT RECEIVERSHIP**	Self-Certification from the authorized signatory of the ISA
	The ISA should not have been blacklisted or placed on Holiday List or under Non-Liquidation or under Court Receivership by any Indian or International Government (Central/ state /PSU) Organization as on the date of bid Submission	
7	**CERTIFIED MANPOWER** The ISA should have the following certified manpower onboard - 07 Certified (CISA or equivalent & OSCP or equivalent) cyber security audit professional for audits networks, applications, websites, IOT devices and other - 03 Certified (CEH or equivalent) professional associated to domain expertise in Ethical Hacking practices for conducting tests like Red Team, Compromise assessment etc. - 03 Certified (CISSP-ISSAP or equivalent) Design experts associated to security architecture design - 02 Training experts for conducting cyber security training - 02 Certified (ISO 27000 LA or equivalent) Compliance certification experts for handling ISO27001 certification process - 02 Project management professional - 02 Certified (PMP or equivalent with Security project handling experience) Project	List of all certified professional with certification details like name of the certificate, expiry date, experience of the certificate holder in various domains and details of project handled needs to be given in the format as defined in the annexure post the completion of the sections

PRE QUALIFICATON-CRITERIA TABLE		
	Criteria	**Supporting to be given**
	Professionals for managing the projects - 01 Documentation expert for draft documents like policy frame work etc. -	
08	**The ISA should have the Empanelment of its firm with the CERT -IN**	ISA to submit the necessary details of CERT -IN Empanelment

SECTION 7 - INSTRUCTION TO ISAs

Section Details: -

Section -1	Introduction
Section -2	Project Brief and Details
Section -3	Schedule of the Project and information related to online bidding
Section -4	Details of the Existing infrastructure
Section -5	Scope of Work
Section -6	Bid Pre-qualification Criteria
Section -7	Instruction to the ISAs
Section -8	Specifications for different Tasks defined in the Scope of Work
Section -9	Details for Security Architecture Design and Policy Framework
Section – 10	Details for the User Training Requirements
Section -11	Details for Audit Compliance Certifications
Section -12	Unpriced BOQ format (to be submitted in the technical Bid)
Section -13	Priced BOQ Format (To be submitted online)
Section 14 Annexures	Annexure – I - Format of Earnest Money Deposit in the form of Bank Guarantee Annexure – II: Performance Bank Guarantee Format Annexure – III: Earnest Money Deposit & RFP Fee Details Annexure IV - RFP letter form Annexure V – Declaration for Non-Black Listing Annexure VI - Work Experience details -as mentioned in the Pre- qualification criteria Annexure VII - Financial Strength of the ISA Annexure VIII - Manpower Details on ISA Roll Annexure IX - Bank List

Cost of bidding

The ISA shall bear all costs associated with the preparation and submission of the Bid and GMDC will in no case be responsible for those costs, regardless of the conduct or outcome of the bidding process.

Bidding documents

ISA can download the bid document and further amendment if any freely available on https://tender.nprocure.com .in and submit the same on N procure on or before due date of the RFP. ISA is expected to examine all instructions, forms, terms, and specifications in the bidding documents.

Failure to furnish all information required by the bidding documents or submits a Bid not substantially responsive to the bidding documents in every respect may result in the rejection of the Bid.

Due Diligence

The Bidder is expected to and shall be deemed to have examined all instructions, forms, terms and specifications and other information in this RFQ Document. The bid should be precise, complete and in the prescribed format as per the requirement of the RFP Document. Failure to furnish all information required by the RFQ Document or submission of a bid not responsive to the RFQ Document in every respect will be at the Bidder's risk and may result in rejection of the bid. GMDC LTD. shall at its sole discretion be entitled to determine the adequacy/ sufficiency of the information provided by the Bidder.

Clarification on bidding documents

ISAs can seek written clarifications from date of issue of the RFP document, to: General Manager IT 3rd Floor Khanij Bhavan during office hours, E-mail: tenderit@gmdcltd.com in prescribe format.

Amendment of bidding documents

At any time prior to the deadline for submission of bids, GMDC, for any reason, whether at its own initiative or in response to the clarifications requested by prospective ISAs may modify the bidding documents by amendment.

All prospective ISAs will be notified of the amendment and such modification will be binding on them. ISAs are also requested to browse the website of GMDC i.e. www.gmdcltd.com or tender.nprocure.com for further amendments if any.

In order to allow prospective ISAs a reasonable time to take the amendment into account in preparing their bids, GMDC, at its discretion, may extend the deadline for the submission of bids.

Contact Details

All inquiries concerning this procurement are to be addressed to the following;

General Manager (IT)
Gujarat Mineral Development Corporation Ltd.
Khanij Bhavan, 132' Ring Road, University Ground,
Vastrapur, Ahmedabad 380 052
(EPABX :079-27913501, 27913200)
E-mail : tenderit@gmdcltd.com

Language of bid

The Bid prepared by the ISA, as well as all correspondence and documents relating to the Bid exchanged by the ISA and GMDC shall be in English. Supporting documents and printed literature furnished by the ISA may be in another language provided they are accompanied by an accurate translation of the relevant pages in English. For purposes of interpretation of the bid, the translation shall govern.

Consortium / Joint Venture:
Consortium / Joint Venture are not allowed.
GMDC is authorized to take suitable decision and action in case of requirement to amend/alter the contract conditions/quantities of the items.
The Successful bidder shall not change the constitution of the Bidder/name during the currency of the contract without prior approval of GMDC. Upon such change in constitution and/or name, Supplementary agreement to that effect shall be executed and if the SD is submitted in form of BG/FD than fresh BG in the name and/or constitution shall be submitted failing which necessary action as deemed fit by GMDC shall be taken.

Statutory Obligations

If any amount becomes payable by GMDC **because of** any claim or application in terms of the provisions or non-compliance of provision of the any Acts and the Rules and Regulations, By-laws or the Orders made there under, applicable from time to time, such amounts shall be recoverable from the Successful Bidder for which GMDC will not be responsible for any compensation.

The Successful Bidder shall also indemnify the GMDC against any claims, compensations, damages, loss, liquidated damages etc. for breach and / or non-fulfilment of the prevailing Rules and Regulations and other statutory provisions in force from time to time and applicable to the work during the currency of contract.

Section comprising the bids

The quotation should be scan-able and distinct without any option stated in. The bid submitted shall have the following documents:

The Bid Security (Physically Submission at GMDC)

The bid security to be furnished to GMDC office on or before due date. The details are required to be filled in this section. A non-interest-bearing Earnest Money Deposit ₹ 15,00,000.00
in any of the following forms:
Demand Draft in favour of GMDC Limited Payable at Ahmedabad.
OR
Fixed Deposit / Bank Guarantee from Banks approved by Govt. Of Gujarat (except Co-operative Bank) duly pledged in **favour** of GMDC for a period of not less than 6 (six) months from the last date of submission of bid and shall be renewed from time to time in case of requirement.
OR
Bank details for submitting RFQ Processing Fees and EMD through NEFT/RTGS:
Bank Name: ICICI Bank
Name of beneficiary: GUJARAT MINERAL DEVELOPMENT CORPORATION LTD. Address: JMC house Branch, Ambawadi, Ahmedabad
Account No: 0024050193 79 IFSC Code: I C I C 0 0 0 0 0 2 4

Technical Section

(To be uploaded with supporting on the NPROCURE website and Physically Submission at GMDC)

- Clause by clause Compliance statement for Bid document including all annexure to be submitted.

- All annexure / Table, duly filled-in with necessary proofs, as required and stated in the bid document
- Letter of Authority for signing the bid.
- Document having the details of ISAs visibility to approach the project with methodology details, skill sets required and other things associated to the project

Price bid Section

(To be uploaded with supporting on the https://tender.nprocure.com website)

Priced bid (in the prescribed format only)

Bid forms

Wherever a specific form is prescribed in the Bid document, the ISA shall use the form to provide relevant information. If the form does not provide space for any required information, space at the end of the form or additional sheets shall be used to convey the said information. Failing to submit the information in the prescribed format, the bid is liable for rejection.

For all other cases, the ISA shall design a form to hold the required information.

GMDC shall not be bound by any printed conditions or provisions in the ISA's Bid Forms

Fraudulent & corrupt practice

Fraudulent practice means a misrepresentation of facts in order to influence a procurement process or the execution of a Contract and includes collusive practice among ISAs (prior to or after Bid submission) designed to establish Bid prices at artificial non-competitive levels and to deprive the GMDC of the benefits of free and open competition.

"Corrupt Practice" means the offering, giving, receiving or soliciting of anything of value, pressurizing to influence the action of a public official in the process of Contract execution

GMDC will reject a proposal for award and may forfeit the E.M.D. and/or Performance Guarantee if it determines that the ISA recommended for award has engaged in corrupt or fraudulent practices in competing for, or in executing, contract(s).

Lack of information to ISA

The ISA shall be deemed to have carefully examined all contract documents to his entire satisfaction. Any lack of information shall not in any way relieve the ISA of his responsibility to fulfil his obligation under the Contract.

Work Order obligations

If after the award of the work order, the ISA does not sign the Service Level Agreement or fails to furnish the Performance Bank guarantee within fifteen (15) working days along with the inception report and working schedule as per the RFP requirements & if the operation is not started within fifteen(15) working days after submission of P.B.G. as mentioned, GMDC reserves the right to cancel the contract and apply all remedies available to him under the terms and conditions of this contract.

Bid price

For services costs offered in in INR the prices should be exclusive of all taxes and inclusive of all duties

The priced bid should indicate the prices in the format/price schedule only.

Any effort by ISA or ISA's agent / consultant or representative howsoever described to influence the GMDC/ in any way concerning scrutiny / consideration / evaluation / comparison of the bid or decision concerning award of work order shall entail rejection of the bid.

Unit rates should be quoted separately for each item. Quantities can be increased or decreased by purchaser and ISA must supply deviated quantities at the rates prescribed and approved by the purchaser in the RFP document.

Bid currency

The prices should be quoted in Indian Rupees. Payment for the services as specified in the agreement shall be made in Indian Rupees.

Unsuccessful ISA's Bid security will be refunded within thirty (30) days from the award of work to the successful ISA.

The successful ISA's Bid security will be discharged upon the ISA signing the Service Level Agreement, and furnishing the Performance Bank Guarantee.

The Bid security may be forfeited at the discretion of GMDC, because of one or more of the following reasons:

The ISA withdraws their Bid during the period of Bid validity specified by them on the Bid letter form.

ISA does not respond to requests for clarification of their Bid.

ISA fails to co-operate in the Bid evaluation process, and In case of a successful ISA, the said ISA fails:

- To sign the Service Level Agreement in time
- To furnish Performance Bank Guarantee

Period of validity of bids

Bids shall remain valid for 180 days after the date of Bid opening prescribed by GMDC. A Bid valid for a shorter period shall be rejected as non-responsive.

In exceptional circumstances, GMDC may solicit ISA's consent to an extension of the period of validity. The request and the responses thereto shall be made in writing. The Bid security shall also be suitably extended. A ISA granting the request is not required nor permitted to modify the Bid.

Format and signing of bid

The documents to be uploaded shall be typed or written in indelible ink and shall be signed by the ISA or a person duly authorized to bind the ISA to the Contract/ Concession Agreement. All the pages to be uploaded, shall be signed by the person or persons signing the bid.

The complete bid shall be without alteration or erasures, except those to accord with instructions issued by the GMDC or as necessary to correct errors made by the ISA, in which case such corrections shall be initialized by the person or persons signing the bid.

Bid due date

Bid must be uploaded by ISA at given N procure website not later than the bid submission date specified in the RFP.

The GMDC may, at its discretion, on giving reasonable notice by fax, e-mail, website upload or any other written communication to all prospective ISAs who are planning to bid and extend the bid due date, in which case all rights and obligations of the GMDC and the ISAs, previously subject to the bid due date, shall thereafter be subject to the new bid due date as extended.

Late bid

Any bid received by the GMDC after the bid due date/time prescribed in RFP shall be rejected.

Modification and withdrawal of bid

The ISA may modify or withdraw his bid before the last date of submission of bids through the e-Bidding website https://tender.nprocure.com.

No bid may be modified after the deadline for submission of the bids.

No bid may be withdrawn in the interval between the deadline for submission of bids and the expiration of the period of the bid validity specified by the ISA on the Bid Form. Withdrawal of a bid during this interval shall result in the ISA's forfeiture of its bid EMD.

Opening and evaluation of bids

An evaluation committee has been formed for the evaluation of the bids. Decision of the committee would be final and binding upon all the ISAs.

GMDC will open all bids (only Technical Bids at the first instance) through the e-Bidding website of in the presence of ISA or his representative who choose to attend, and at the following address in the presence of the representatives of the ISAs who choose to attend, at the time, date and place, as mentioned in RFP Document.

In the event of the specified date of Bid opening being declared a holiday for the GMDC, the Bids shall be opened at the appointed time and location on the next working day. It is, therefore, advised to send a responsible, authorized and senior representative so that clarifications, if any, can be given on the spot.

The ISA's names, modifications, bid withdrawals, and the presence or absence of the requisite EMD and such other details considered appropriate will be announced at the bid opening.

Evaluation process

The evaluation process of the RFP, proposed to be adopted by the GMDC is indicated under this clause. The purpose of this clause is only to provide the ISAs an idea of the evaluation process that the GMDC may adopt. However, the GMDC reserves the right to modify the evaluation process at any time during the RFP process, without assigning any reason, whatsoever and without any requirement of intimating the ISAs of any such change.

Evaluation of bid

ISAs need to fulfil all the Technical criteria and conditions mentioned in RFP document. GMDC will examine the bids to determine whether they are complete, whether the bid format confirms to the RFP's requirements, whether any computational errors have been made, whether required EMD has been furnished, whether the documents have been properly signed, and whether the bids are generally in order including Techno commercial compliance.

A bid determined as not substantially responsive will be rejected by the GMDC and may not subsequently be made responsive by the ISA by correction of the nonconformity.

The GMDC may waive off any informality or non-conformity or irregularity in a bid which does not constitute a material deviation, provided such waiver does not prejudice or affect the relative ranking of any ISA.

Evaluation of technical bid

Firstly, the technical bid document will be evaluated as per the requirements specified in the RFP and adopting the evaluation criteria spelt out in RFP document

All the ISAs who secure a Technical Score of 80% or more will be declared as technically qualified. The commercial bids of only the technically qualified ISAs will be opened for further processing. It is however, clarified that, subject to other provisions of this document, every ISA will have to fulfil the minimum technical specifications laid down in the RFP for being qualified technically.

In order to assist in the examination, evaluation and comparison of Bids, GMDC may at its discretion ask the ISA for a clarification regarding its Bid. The clarification shall be given in writing immediately, but no change in the price shall be sought, offered or permitted. However, while giving a clarification, a ISA may offer a higher specification or model without any impact on Financial Bid to be opened subsequently.

Announcement of bids

The ISA names, bid modifications or withdrawals and such other details as the GMDC at discretion may consider appropriate, will be announced at the bid opening.

Bids not considered for evaluation

Bids that are rejected during the bid opening process due to incomplete documentation or late receipt shall not be considered for further evaluation.

Criteria for evaluation of bids

A three-stage procedure will be adapted for evaluation of proposals, with the technical qualification being completed before the commercial evaluation and there after financial proposal being opened and compared. Pursuant to the Technical qualification criterion ISAs will be short-listed for opening of commercial bid. The technical bids for the disqualified ISAs will be returned unopened at the address mentioned on the envelopes containing the technical bid.

Conditional bids are liable to be rejected.

GMDC will review the technical bids of the short-listed ISAs to determine whether the technical bids are substantially responsive, is fitting in the Technical evaluation score of more than 80 Marks out of 100 marks. Bids that are not substantially responsive are liable to be disqualified.

Post that Quality Cum Cost Basic selection criteria as per the details given below will be applied for the selection among the technically qualified ISAs

QCBS (Quality cum Cost Basis Selection) introduction and details related to the same

- QCBS (Quality cum Cost Basis) is increasingly being employed for awarding various e-governance contracts. It is a methodology which tries to give weightage to both quality and cost. The weights are usually more for technical (or quality) and less for commercial (or cost) aspects of the bid (usually 60:40 or 70:30 or sometimes even 80:20).
- The financial scores are usually calculated through a normalization process where the lowest ISA is given 100 and scores of all other ISAs are normalized against this. For example – If A is the lowest ISA who has bid 20 crores for a project and B and C are the other 2 ISAs with bids of 40 crores and 60 crores, normalized scores of A is taken as 100, B is taken as (100*20/40=50) and C is taken as (100*20/60=33.3).
- Technical scores are calculated based on a variety of parameters such as experience in similar projects, quality of resources to be deployed (usually based on number of qualifications, no of projects worked on, no. of years of experience etc.), write up or presentation on approach and methodology, average annual turnover etc. with scoring being done for each factor separately and final technical score being a summation of these scores.
- After calculating technical and financial scores, they are multiplied by respective weightages to find the total score and the ISA with the highest total score is supposed to be awarded the contract.
- On the face of it, this system appears to be a very sound one and it gives higher weightage to the technical parameters which is as it should be. And it does work quite well as long as companies bidding for a project quote more or less in the same price range.
- The evaluation will be made based on Quality –cum- Cost Based Selection with a weightage to quality of services, technical feasibility and cost in the ratio of 70:30
- The ranking of ISAs shall decide based on total bid amount for all the items & most technically suitable economical option will be considered as L1
- GMDC will assign points (quality of services score) to the technically qualified ISAs based on the technical evaluation criterion approved by GMDC. The commercial bids for the technically qualified ISAs will then be opened and reviewed to determining whether the commercial bids are substantially responsive.

Criteria for evaluation and comparison of technical bids.

The Following criteria shall be used to evaluate the technical bids. All the bids scoring 80 and above in the technical will be qualified for commercial bid opening.

TABLE SHOWING THE DETAILS OF MARKING PER CRITERIA WHICH WILL BE USED FOR THE TECHNICAL QAULIFICATION OF THE ISA				
Sr. No	**Criterion**	**Conditions**	**Max. Marks**	**Total Marks for the Sub head**
1	**Organizational Strength: Turnover and Employee Strength; Implementation References & Certifications**			**60**
1.1	Average Annual Turnover (As mentioned in the PQ section revenue	> = 50 Crores as per the PQ req.	4	
		> = 65 Crores as per the PQ req.	6	
		> = 80 Crores as per the PQ req.	8	

TABLE SHOWING THE DETAILS OF MARKING PER CRITERIA WHICH WILL BE USED FOR THE TECHNICAL QAULIFICATION OF THE ISA				
Sr. No	**Criterion**	**Conditions**	**Max. Marks**	**Total Marks for the Sub head**
	earned from Cybersecurity services will be considered) of the ISA			
1.2	No. of Certified Personals for Cyber security services as per the PQ.	> = 20 Employees in security domain as per the PQ requirement	3	
		> = 60 Employees in security domain	5	
		> = 100 Employees in security domain	7	
1.3	Experience of Executing similar works associated to VAPT, Gap Analysis, Cybersecurity architecture Design, Cyber Security Policy Framework design, Compliance certification domain expertise and training management for cybersecurity in Government, PSUs and Corporates in India within the last three years	> = 1 Purchase orders of similar nature and value not less than 5 Cr	10	
		> = 10 Purchase orders of similar nature and value not less than 5 Cr	15	
		> = 20 Purchase orders of similar nature and value not less than 5 Cr	20	
1.4	Valid Certifications owned by the ISA's organization	ISO 9000 – Quality 2 Marks ISO 27000 - ISMS 4 Marks	06	
1.5	ISA Firm Global Presence	Operation outside India in >= 2 countries 2 marks >=4 countries 4 marks	04	
1.6	ISA's domain expertise in Government and PSU Vertical	>= 10 order in the time frame defined in the PQ section	**05**	
		>= 20 order in the time frame defined in the PQ section	**10**	
		>= 30 order in the time frame defined in the PQ section	**15**	
2	**Technical Solution Offered: ISA to submit the complete document with Approach Methodology mechanism on task to be**			**40**

TABLE SHOWING THE DETAILS OF MARKING PER CRITERIA WHICH WILL BE USED FOR THE TECHNICAL QAULIFICATION OF THE ISA

Sr. No	Criterion	Conditions	Max. Marks	Total Marks for the Sub head
	executed, tentative proposed Architectures for Cybersecurity, Policy frameworks, Training module etc. and highlight the solutions USPs that with benefit GMDC in the long run (ISA to submit the document and GMDC will invite for the presentation)			

Note: The financial bids of only those ISAs will be opened and considered who have scored at least 80 Marks of the sum of the total maximum marked specified for all above mentioned attributes in the technical bid evaluation process.

Opening and comparison of the financial bids

The financial bids will be opened, in the presence of ISAs' representatives who choose to attend the financial bid opening on the date and time to be communicated to all the technically qualified ISAs. The ISAs' representative who are present shall sign a register evidencing the attendance. The name of the ISA, Bid Prices, and Discount etc. will be announced in the meeting.

QCBS methodology will be used for deciding the ISA to whom the bid will be awarded and the same will done using quality and cost and as mentioned in the QCBS section the ratio to technical to commercial will be **70: 30**. The table below explains the formula which will be used to decide the L1 ISA.

Price Evaluation Criteria: **ISA with Highest Score as per below techno commercial formula as Outcome of " L " will be the L1 ISA for the award of contract.**
Formula for calculation the ISA point: L= {Cmin *Wt1/Cquoted} + {Tscored*Wt2/Tmax}
Cmin = Minimum (L1 ISA) quoted cost for the entire scope of work of
Cquoted = Quoted cost (Cost of the ISA whose bid is being evaluated)
Tscored = Marks scored in the technical evaluation whose bid is being evaluated
Tmax = Maximum marks in the technical evaluation
Wt1 = 30% - Commercial Weightage
Wt2 = 70% - Technical Weightage

As mentioned above ISA will be decided based on the commercial calculation which will be done as per the above table.

Contacting GMDC

ISA shall not approach GMDC officers outside of office hours and/ or outside GMDC office premises, from the time of the Bid opening to the time the Contract is awarded.

Any effort by a ISA to influence GMDC officers in the decisions on Bid evaluation, bid comparison or contract award may result in rejection of the ISA's offer. If the ISA wishes to bring additional information to the notice of the GMDC, it should do so in writing.

Rejection of bids

GMDC's right to reject any or all bids: GMDC reserves the right to reject any Bid, and to annul the bidding process and reject all bids at any time prior to award of Contract, without thereby incurring any liability to the affected ISA(s) or any obligation to inform the affected ISA(s) of the grounds for such decision.

Choice of Firm:

Final Choice of Firm / Firms, to execute this project shall be made based on conformity to technical and operational requirements, time schedule of execution and appropriateness of priced bid from the point of view of cost competitiveness. GMDC, however, will have the discretion to choose to enter into any price negotiations or not. GMDC may ask ISA to match L1 prices under each item / head.

Procurement Process

One the ISA is declared L1 he would be issued the LOI for the entire work order value and post that on submission of the Bank Guarantee the ISA would be issued the work order

Award of work order

Award Criteria: The Criteria for selection will be as the QCBS methodology defined above for technically qualified ISAs.

GMDC's right to vary requirements at time of award: GMDC reserves the right at the time of award to increase or decrease quantity for the service requirements originally specified in the document without any change in Bid rate or other terms and conditions.

In case, if lowest ISA does not accept the award of work order or found to be involved in corrupt and/or fraudulent practices the next lowest ISA will be awarded the work order. In such scenario, the lowest ISA must Bear the difference between lowest prices and next lowest prices.

Notification of award, signing of Service Level Agreement and Signing of Non-Disclosure Agreement(NDA)

Prior to expiration of the period of Bid validity, GMDC will notify the successful ISA to sign the Non-Disclosure agreement (Format and draft of the same will be shared with the successful ISA) and post

NDA signoff GMDC will issue a LOI after which the ISA needs to submit the PBG and sign the Service Level agreement in line with the bidding documents. Within Six (6) working days of receipt of the Service Level Agreement,

The successful bidder shall submit security deposit of 10% of the total contract value excluding Goods & Service Tax (GST) within 15 days from the date of receipt of LOI in any one of following form

Demand Draft in **favour** of GMDC Limited Payable at Ahmedabad.
OR
Fixed Deposit from Banks approved by Govt. Of Gujarat (except Co-operative Bank) duly pledged in **favour** of GMDC for a period of not less than **1**5 (**Fifteen** months) months from the date of receipt of LOI and shall be renewed from time to time in case of requirement.
OR
Bank Guarantee issued by banks approved by Govt. Of Gujarat from time to time (except Co-Operative bank) in the form and manner acceptable to GMDC (Govt. GR for approved bank). It should be valid for a period of not less than **1**5 **(Fifteen** months) from the date of receipt of LOI and shall be renewed from time to time in case of requirement.

Security deposit shall not bear any interest under any circumstances.

GMDC will reserve the right to recover the charges or the liquidated damages from the Security Deposit in the following circumstances-

a. If the successful bidder or its employees causes any damage or destroy any property belonging to GMDC.
b. The shortfall amount of all compensations, penalties and other sums of money payable by the successful bidder or recoveries to be made under the terms of this contract which is due but not paid by the successful bidder in full, etc.
c. Any other dues because of statutory compliance.

Upon the successful ISA's furnishing of Performance Bank Guarantee and signing of Service Level Agreements, The Bid Security of all unsuccessful ISAs will be refunded. Once the acceptance of LOI is done and PBG is submitted by the ISA, GMDC will issue the purchase order as per the quantities decided jointly by the ISA and GMDC team post the kick off meeting.

Purchase order issuance

For services whose value is quoted in INR GMDC will issue one single PO for the same and the payment terms will be as per the payment table mentioned below under the payment terms header

Force majeure

Force majeure is herein defined as any cause which is beyond the control of the Successful Bidder or the GMDC as the case may be which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affect the performance of the contract, such as:

Natural phenomena such as floods, draughts Cyclone, earthquake and epidemics, declaration of war.

Acts of any government, including but not limited to war, declared or undeclared priorities, quantities, embargoes, providing either party shall within fifteen (15) days from the occurrence of such a cause notify the other in writing of such cases.

The Successful Bidder will advise, in the event of his having resort to this clause by a registered letter duly certified by the statutory authorities, the beginning and end of the cause of delay, within fifteen days of the occurrence and cessation of such Force Majeure condition. In the event of delay lasting over two months, if arising out of Force Majeure, the contract may be terminated at the discretion of the GMDC.

For delay arising out of Force Majeure, the Successful Bidder will not claim extension in completion date for a period exceeding the period of delay attributable to the causes of force Majeure and neither company nor the Successful Bidder shall be liable to pay extra costs (like increase in rates, remobilization, advance, idle charges for labour and machinery etc.) provided it is mutually established that the Force Majeure conditions did exist.

If any of the Force Majeure conditions exists in the place of operation of the Successful Bidder even at the time of submission of bid, he will categorically specify them in his bid and state whether they have been taken into consideration in their quotations.

The Successful Bidder or the GMDC shall not be liable for delays in performing his obligations resulting from any force majeure cause as referred to and/ or defined above. The date of completion will, subject to the hereinafter provided, be extended by a reasonable time.

Force majeure event

The Force Majeure circumstances and events shall include the following events to the extent that such events or their consequences (it being understood that if a causing event is within the reasonable control of the affected party, the direct consequences shall also be deemed to be within such party's reasonable control) satisfy the definition as stated above.

Without limitation to the generality of the foregoing, Force Majeure Event shall include following events and circumstances and their effects to the extent that they, or their effects, satisfy the above requirements:

Natural events (“Natural Events”) to the extent they satisfy the foregoing requirements including:

Any material effect on the natural elements, including lightning, fire, earthquake, cyclone, flood, storm, tornado, or typhoon;

Explosion or chemical contamination (other than resulting from an act of war);

Epidemic such as plague;

Any event or circumstance of a nature analogous to any of the foregoing.

Other Events (“Political Events”) to the extent that they satisfy the foregoing requirements including: Political Events which occur inside or Outside the State of Gujarat or involve directly the State Government and the Central Government (“*Direct Political Event*”), including:

Act of war (whether declared or undeclared), invasion, armed conflict or act of foreign enemy, blockade, embargo, revolution, riot, insurrection, civil commotion, act of terrorism or sabotage;

Strikes, work to rules, go-slows which are either widespread, nation-wide, or state-wide and are of political nature;

Any event or circumstance of a nature analogous to any of the foregoing.

Force majeure exclusions

Force Majeure shall not include the following event(s) and/or circumstances, except to the extent that they are consequences of an event of Force Majeure:

Unavailability, late delivery (man, material, machine and other resources needed at site etc.)

Delay in the performance of ISA

Procedure for calling force majeure

The Affected Party shall notify to the other Party in writing of the occurrence of the Force Majeure as soon as reasonably practicable, and in any event within 5 (five) days after the Affected Party came to know or ought reasonably to have known, of its occurrence and that the Force Majeure would be likely to have a material impact on the performance of its obligations under the Service Level Agreement.

Service Level Agreement obligations

Once a Service Level Agreement is confirmed and signed, the terms and conditions contained therein shall take precedence over the ISA’s bid and all previous correspondence**.**

Amendment to the Service Level agreement

Amendments to the Service Level Agreement may be made by agreement by both the Parties. No variation in or modification in the terms of the Service Level Agreement shall be made except by written amendment signed by both the parties. All alterations and changes in the Service Level Agreement will consider prevailing rules, regulations and laws.

Use of Service Level Agreement documents and information

The ISA shall not without prior written consent from GMDC disclose the Service Level Agreement or any provision thereof or any specification, plans, drawings, pattern, samples or information furnished by or on behalf of GMDC in connection therewith to any person other than the person employed by the ISA in the performance of the Service Level Agreement. Disclosure to any such employee shall be made in confidence and shall extend only as far as may be necessary for such performance.

The ISA shall not without prior written consent of GMDC make use of any document or information made available for the project except for purposes of performing the Service Level Agreement.

All project related documents issued by GMDC other than the Service Level Agreement Itself shall remain the property of GMDC and Originals and all copies shall be returned to GMDC on completion of the ISA's performance under the Agreement, if so required by the GMDC.

Assignment & sub contracts

Assignment by ISA

The ISA shall not assign or sub-contract, in whole or in part, its rights and obligations to perform under the Service Level Agreement to a third party.

Resolution of disputes

If any dispute arises between the Parties hereto during the subsistence or thereafter, in connection with the validity interpretation, implementation or alleged material breach of any provision of the Agreement or regarding a question, including the questions as to whether the termination of the Contract Agreement by one Party hereto has been legitimate, both Parties hereto shall endeavour to settle such dispute amicably. The attempt to bring about an amicable settlement is considered to have failed as soon as one of the Parties hereto, after reasonable attempts [which attempt shall continue for not less than 30 (thirty) days], give 15 days' notice thereof to the other Party in writing.

In the case of such failure the dispute shall be referred to a sole arbitrator or in case of disagreement as to the appointment of the sole arbitrator to three arbitrators, two of whom will be appointed by each Party and the third appointed by the two arbitrators.

Arbitration

All questions, disputes, differences whatsoever which may at any time arise between the parties to this RFQ and subsequent contract in connection with the RFQ and subsequent contract or any matter arising out of or in relation there to, shall be referred to Sole Arbitrator as per the provisions of Arbitration and Conciliation Act, 1996 and subsequent amendment thereto and the venue of arbitration proceedings shall be at Ahmedabad only. The Language of the Arbitration shall be in English only

Jurisdiction

The matter related to any dispute or difference arising out of this RFQ and subsequent contract shall be subject to the exclusive jurisdiction of Court at Ahmedabad only.

Taxes & duties

ISA is liable for all taxes and duties as in force from the time of the signing of agreement till performance liability period expires, may arise by any law comes to the notice of GMDC or comes in force etc. This must be noted for compliance at any time.

Service Delivery norms

All services to be delivered should be in accordance with the model specifications and procedures mentioned in the specification's sections and further to this if the ISA can offer services with better specifications and methodology the same can be done after the acceptance of the details by GMDC.

If the service delivery does not meet the specifications and/or are not in accordance with the details mentioned in this order, and re work is required at site, GMDC shall notify the ISA giving full details of difference. The ISA shall attend the site within three (3) days of receipt of such notice to meet and agree with representatives of GMDC, the action required to correct the deficiency. Should the ISA fail the attend meeting at site within the time specified above, GMDC shall be at liberty to rectify the work/materials and ISA shall reimburse GMDC all costs and expenses incurred in connection with such trouble or defect.

Bankruptcy

If the Successful Bidder commits an act of Bankruptcy or goes into liquidation except for construction purposes, or if its business is carried on by a receiver, such receiver, liquidator or any person in whom the contract may become vested shall forthwith give notice thereof in writing to GMDC and in reasonable time during which he shall take all reasonable steps to prevent stoppage of performance of the contract, have the option of carrying out the contract subject to his or their providing such guarantees as may be required by GMDC but not exceeding the value of the work for the time being remaining unexecuted.

In the event of stoppage of performance under the contract, the period of option under this clause shall be decided by GMDC considering the situation, provided that the above option is not exercised, GMDC may terminate the contract by serving notice in writing to the Successful Bidder. The power and provision so reserved to GMDC on taking of the work out of the Successful Bidder's hands shall apply as far as they may be when the contract is so terminated

Payments terms

	INR
1	No advance payment will be made
2	Payment will be released as per the completion of the phases mentioned in the work order. The %age for each phase is mentioned below: - For completion of works as mentioned in Phase I - 100% of the quoted value - For completion of work as mentioned in Phase II - 100% of the quoted value - For PMC services for works mentioned in Phase III – 100% of the quoted value - For completion of works mentioned in Phase IV - 100% of the quoted value - For completion of works mentioned in Phase V - 100% of the quoted value

Payment will be made for those tasks which are executed by the ISA in the different phases

The bills, submitted at the office of General Manager (IT) will be processed within 30 days considering the following deductions.

Income tax as per provision of Income Tax Act, and other Taxes (and surcharges) applicable in force from time to time
Cost of any other services provided / material supplied, if any, by the GMDC.
Liquidated damages,
Penalties &
Other deductions, if any.

Service terms

The entire scope of the work depends on the technical skill and experience in management of the same level or kind of infrastructure.

It is mandatory for ISA to deploy qualified professional to install, commission & maintain the equipment, as defined under scope of work.

The ISA must submit regular schedule of man power availability & get it approved by GMDC.

Penalty clause

Penalties for delay in implementation:

Failure to complete the Service Delivery: If the ISA fails to complete the Service Delivery within the time (s) specified in the LOI/Order/Instruction **GMDC may, without prejudice to its other remedies under the Agreement, levy as Penalties, a sum equivalent to 1% of the algebraic sum of the cost for the services to be delivered in phases, for each week or part thereof of delay, until actual delivery of performance. The maximum aggregate penalty will not exceed 10% of the algebraic sum of the cost for the service to be delivered at that site.** If the delay continues beyond 10 weeks, GMDC may terminate the Agreement. However, GMDC may consider extension of time for completion of the assigned job with justification thereof.

Project implementation

The ISA will implement the project strictly as per the plan approved by GMDC.

GMDC will form committee for Project and all inspection, installation; commissioning and acceptance of work will be undertaken by ISA which will be approved by appointed committee. All Invoices, Vouchers, Bills for services by the ISA under the scope of the work will be verified vetted and accepted by the GMDC committee for release of payment.

As part of implementation the ISA shall provide details of tools and manpower required.

The ISA shall provide, log analysis and other associated training required to monitor the security infrastructure to GMDC Personnel at no cost to GMDC. The training schedule, content and modalities will be defined jointly by both the parties. If Certification is required ISA should consider the training costs to train 04 GMDC team members for the same.

In case the service delivery is rejected owing to its non-conformity to the specifications or due to the poor quality of workmanship, the same shall be done again promptly. No additional cost for the same will be paid by GMDC

ISA shall treat all matters connected with the contract strictly confidential and shall undertake not to disclose, in any way, information, documents, technical data, experience and know how, without prior written permission from GMDC.

The ISA shall have to furnish the documentation of the work undertaken in consultation with official-in-charge/GMDC rep. 1 sets of such documentation should be provided before the issue of completion certificate.

It is a turnkey project. The ISA shall be fully responsible for implementing the Project in totality and should include the items and their prices, if not included in Schedule of Requirement to complete the project on turnkey basis. Any claim whatsoever in this regard will not be entertained later.

In the event of the delay in delivery services is not satisfactory the purchaser may procure services from else where as prescribed in bid and ISA shall be liable without limitations for the difference between the cost of such substitution and the price set forth in the contract for the goods involved i.e. at the risk and cost of the ISA.

The ISA shall be responsible and take required insurance for all their representatives working on the site at their own cost. GMDC will not be responsible for any injury, loss or damage to any of the representatives of the ISA during the said contract. The ISA should strictly comply to GMDC EHS (Environment Health and Safety policy) and should start work execution post submission of the necessary documents and safety evidences as per the requirement of EHS officer on Site. This should be strictly followed in the Mines area.

All work shall be performed and executed by the ISA in strict conformity with the engineer-in-charge / representative from GMDC and any relative instruction issued to the ISA by the Engineer in- charge from time to time.

Software licenses (wherever applicable)

The ISA shall be responsible for providing Software (System Software, Application Software, Device Drivers, IOS, etc.) required, if any, to meet any additional requirements during the currency of the Agreement without any additional cost to GMDC. All license software must be in the name of GMDC. The ownership of any customized software involved will be of the GMDC.

Installation of additional hardware (wherever applicable)

During the currency of the Agreement, for any additional requirement of equipment including interface equipment, the specifications will be provided by the ISA. GMDC/The Third-Party Agency will verify suitability of the specifications submitted by ISA and recommend to GMDC for acceptance. The ISA will be obligated to undertake integration, operation and maintenance for all additional equipment if required.

Support from external agency (if applicable)

In case, if ISA wish to have support from any external agency, it’s necessary to inform GMDC in written prior to allow them to work on GMDC infrastructure. The information should contain all respective information about the company from whom support has been extended, the person/group of people and the segment in which services has been taken. On completion of the task, another report should be submitted by mentioning action taken by this person/group of people from external agency, with duration. The ISA is sole responsible for the action taken by such agency on their behalf. No Data/ Information should be sent out of the premise without obtaining prior written confirmation from the GMDC.

Limitation of liability:

ISA's cumulative liability for its obligations under the contract shall not exceed the contract value and the ISA agency shall not be liable for incidental, consequential, or indirect damages including loss of profit or saving.

Termination for convenience:

Either party may terminate the said Service Level Agreement at any time by giving sixty (60) days prior written notice to the other Party. Upon termination, the GMDC shall pay to Successful ISA all undisputed amounts for all products and services delivered up to the date of termination.

Risk purchase:

GMDC on identifying any material breach of contract by ISA, shall give ISA a cure period of 90 days to correct the breach. If ISA fails to cure the breach in the agreed duration and accept its inability to correct, GMDC may terminate the part of the contract that is breached and employ a third party to do the work on behalf of Customer, at no risk & cost of ISA. ISA shall not be liable for any compensation for the work executed this way. ISA shall execute the balance part of work as agreed under the contract.

Foreclosure:

In case of any necessity arising due to working conditions or any unforeseen reason not in the control of the GMDC or any reason what so ever GMDC shall be at liberty to Fore close the contract without assigning any reasons or notice there for.

Participation of ISA in the SITC RFP for procurement of Security Services and Hardware

The Selected ISA who will act as an PMC for GMDC procurement of Security Hardware, Software and associated accessories shall not participate in the procurement RFP that will be floated post this RFP

SECTION – 8 SPECIFICATIONS AND PROCESS DEFINITIONS FOR TASK DEFINED IN SOCOPE OF WORK

IT Asset Discovery (For existing infrastructure at all locations)

- GMDC is managing all its IT assets through the tools they are using.
- ISA can review the information available in the tool and use the same for further tests associated to assessments etc.
- In case the ISA feels that they need the information in their tool then they can conduct the discovery process using their tools

Security Hardening (Policy review and Assessment)

Under this scope the following things mentioned below needs to be audited and based on the flaws in the systems if any the recommendations need to be done in the audit report

- Active Directory configuration checks and recommendations
- Operating system hardening (All OS which are functional on the server in standalone/virtualized environments, OS installed on PC/Desktop/Laptops/Endpoints like CCTV, Biometric device, Access points etc. and OS of all IP devices using the GMDC network)
- Application Hardening (ERP Oracle-EBS, Weighbridge API, Attendance App, Customer portal, PF App and Data Mining software)
- Networking hardening (Assessment of all configuration at HO post Alcatel upgrade, WAN Link infrastructure assessment and assessment of all Networking and Security infra at Head office and all operational mines as mentioned in the existing infrastructure)
- User account Hardening (Assessment of all user and equipment access credentials)
- Patch management (Assessment of all Servers, other IT devices and all IT endpoints)
- ACL are not being used by GMDC but ISA post the assessment and study should recommend a policy framework for ACL implementation in the report

Vulnerability Assessment and Penetration Testing

The Vulnerability assessment needs to be performed through appropriate tools installed in the cloud/on premise and based on the assessment reports should be submitted to GMDC with the necessary change recommendation based on which GMDC will do the changes to eliminate the identified vulnerabilities. Post change management the VA will be done to check if vulnerabilities are eliminated or not and the report will be stored for further compliance

The parameters defined for VAPT Testing of Networking, Applications, Cloud Services, Endpoints, IOTs (CCTV, Biometric readers, IP Phones etc.), Wi-Fi and Radio devices and hosted Email solutions are indicative and bear minimum. The vendor should not restrict the testing to this parameter only but adapt best industry practices which conducting VAPT of all the above

Vulnerability assessment and Penetration Testing for Network and Security Infrastructure

- Net Scanning - Threat and Vulnerability Assessment: It is the process of measuring and prioritizing the risks associated with network- and host-based systems and devices to allow rational planning of technologies and activities that manage business risk.
- Password Cracking

- Firewall Testing
- Router Testing
- Denial of Service (DOS) Testing
- Distributed DOS Testing
- Containment Measures Testing
- While doing the penetration test on Servers in live environment the ISA should ensure optimum performance of the systems.
- Network Infrastructure Review: Network infrastructure at Data Centre, Mines site, and Cloud locations hosting different applications.
- Network Security Audit
  - ➢ Physical and logical security measures, tools and processes implemented to protect unauthorized entry into corporate network are to be reviewed. Configuration of Firewalls & Routers and automated audit trial of all the users of network are the key areas that should undergo review. Check if adequate security is available in the various Network connectivity provided to ensure only authorized users are accessing the system.
  - ➢ Focus should be on detecting the system vulnerabilities arising out of multiple access levels. Standard tools to scan various entry points to the network are to be used and an exhaustive analysis of security targets are to be provided. The scope includes operating system, databases, firewalls, routers, remote access devices and switches.
  - ➢ Review the activities of Network Administrator/System Administrator and suggest Improvements and controls, if any, required.
- Security Device Audit
  - ➢ Configuration, policy/rule sets, signatures, Inspection, Logging, Location, redundancy, port restrictions, patches & updates, Administration & Management
  - ➢ Firewalls (FortiGate)

Post updation of the configuration and addition of the hardware (if required) as per the recommendations in the audit report the ISA needs to conduct the second round of assessment and submit the final audit reports which will be used for applying for compliance certifications

Vulnerability assessment and Testing for Application Testing (Web based/ ERP/ Website/ Database /APIs)

Test should be done using Black Box testing to assess the functional operating effectiveness and for Application that has various roles defined for various user's ISA needs to carry role-based functionality testing to ascertain any security flaws. The standard to be used for Web Application Testing is OWASP (Open Web Application Security Project)

The First level Application Audit should highlight the vulnerabilities in the Application like, Buffer Overflows, Invalidated Inputs, insecure storage etc. Over and above the at least following checks as mentioned below should be done

Sr. No.	Parameter	Details of checks that needs to be done
01	Domain Reputation	Check if a domain name is classified as potentially malicious or phishing by multiple well-known domain blacklists
02	Port Scans	Check for open ports that are not required as they could be a potential threat
03	SQL Injection	Check for poorly filtered or in-correct escaped SQL queries into parsing variable data received from user input
04	Malware Scans	Check the pages for Page defacement and JavaScript's codes against generic signatures
05	RFI Scans	Scan and sanitize pages to avoid RFI and LFI attacks on websites
06	LFI Scan	
07	Cross Site Scripting (XSS)	Scan forms for GET and POST requests to detect XSS requests
08	URL monitoring	
09	CMS scan	Scan the associated CMS in which the website is designed to check for vulnerabilities
10	OS Detection	Verification of OS and its versions against the Malware databases
11	Click Jacking	Check if any Defense mechanisms are available to counter Click jacking (a practice of manipulating a website user's activity by concealing hyperlinks beneath legitimate clickable content)
12	CSRF (Cross-Site Request Forgery)	Check for Cross-Site Request Forgery (CSRF) vulnerability in the website that forces an end user to execute unwanted actions on a web application in which they're currently authenticated
13	SSL Scan	Check if SSL certificates being used are authentic, not expired and scan the algorithm of the SSL certificate being used for vulnerabilities if any
14	WAF Detection	Check if website/web applications are protected by WAF or not
15	Content Change Monitoring	Monitor changes in your websites by comparing original content for change management
16	Banner Grabbing	Check for Banner Grabbing vulnerabilities if any

Apart from the above parameters the application should be tested for top 10 OWASP Vulnerabilities as mentioned in the table below

Vulnerability name	Description in Brief
A1- Broken Access Control	Restrictions on what authenticated users can do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
A2- Cryptographic failures (earlier known as Sensitive Data Exposure	Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
A3-Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A4- Insecure Design	This focuses on risks related to design flaws. If we genuinely want to "move left" as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures
A5- Security Misconfiguration	Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.
A6- Vulnerable and Outdated components	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defense and enable various attacks and impacts.
A7- Identifiacation and Authentication	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
A8- Software and Data Integrity Failures	A new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category
A9- Security, Logging and Monitoring features	This is associated with the concerns related to the application's weaknesses in detecting and responding to security risks. Given that the time taken to attack detection is 197 days on average, attackers have a long enough window to do their bidding.

Vulnerability name	Description in Brief
A10- Server-Side Request Forgery	This vulnerability allows users to access data from remote resources based on user-specified, unvalidated URLs. Even firewall/ VPN-protected servers are prone to these vulnerabilities if unvalidated user inputs are accepted

ISA to give details of the same in the audit report for each applications, website and databases they assess. Based on the same the necessary patch management will be done by development team or the OEM providing the software.

Post updation of the patches and addition of the hardware as per the recommendations in the audit report the ISA needs to conduct the second round of assessment and submit the final audit reports which will be used for applying for compliance certifications

Vulnerability assessment and Testing for Cloud based services (SAAS/PASS/IAAS)

For all Cloud based services which GMDC is using(Details of the same available in Section 4), the ISA needs to do the vulnerability assessment for the following risk defined in the below table:

Risk to assessed	Brief Description/Impact of the Risk
Data Breach	A data breach involves the release of protected or confidential information to unauthorized individuals or groups.
Identity and Access Management checks	Attacks and security breaches can also result from non-usage of multifactor authentication, lack of ongoing automated rotation of cryptographic keys and certificates, as well as weak password usage.
Insecure API checks	As Application Programming Interfaces (APIs) enable the provisioning, management and monitoring of cloud services, their security is of prime importance
System Vulnerabilities	Attackers can infiltrate and take control of the systems in addition to disrupting the service operations, utilizing the system vulnerabilities or exploitable bugs
Account or Service Hijacking	Service hijacking includes attack methods such as phishing, fraud and exploitation of software vulnerabilities that enable attackers to misuse the account access, steal data, impact cloud services and systems, and damage the overall reputation
Malicious Insider Threats	The threat caused by insiders with malicious intent, who might be system administrators having access to critical systems and sensitive information, can have a tremendous impact on a company's security
Advanced Persistent Threats (APTs)	Advanced Persistent Threats (APTs) steal data and Intellectual Property (IP) by infiltrating the IT systems of target companies. The common points of entry for APTs are spear-phishing, direct hacking systems and use of unsecured or third-party networks
Malware Injection	Malware injection attacks are becoming a major security concern in cloud computing. These are malicious scripts or code that enable attackers to eavesdrop, steal data and compromise the integrity of sensitive information
Data Loss	Data loss can occur because of multiple reasons such as a catastrophe like fire or earthquake, or even accidental deletion by the CSP
Abuse of Cloud Services	Malicious attacks that result from issues such as unsecured cloud service deployments, fraudulent account sign-ups and free cloud service trials

Risk to assessed	Brief Description/Impact of the Risk
DoS Attacks	Denial-of-Service (DoS) attacks cause the consumption of disproportionately large amounts of system resources including memory, disk space, network bandwidth and processor power by the targeted cloud services, thereby preventing the users from accessing their data and applications.
Vulnerabilities Caused by Shared Technology	CSPs deliver scalable services by sharing infrastructure, applications and platforms without substantial alterations to the off-the-shelf hardware and software. If the underlying components such as CPU caches and GPUs do not offer strong isolation properties for a multitenant architecture (IaaS), multi-customer applications (SaaS) or redeploy able platforms (PaaS), it could lead to shared technology vulnerabilities.

ISA to give details of the same in the audit report for each cloud services they assess. Over and above this if the ISA feels some additional parameters needs to accesses the same should be included. If gaps are found on the configuration and device front then mitigation measures for each of the gap and discrepancy should be defined clearly with a proposed architecture setup and security policy framework associated to the cloud services

Post updation of the patches and addition of the hardware as per the recommendations in the audit report the ISA needs to conduct the second round of assessment and submit the final audit reports which will be used for applying for compliance certifications

Vulnerability assessment and Testing of End Points (Desktops/Laptops/Tablets/BYOD devices getting connected to the network)

GMDC is Managing desktops using Active Directory to centralize control and streamline administration tasks. Desktops and servers hardening are managed using Active directory and EDR / XDR Solutions. the services implemented are:

- User Account Control and Password management
- Secure Configurations and hardening.
- Group Policy
- Software Distribution and Patch Management
- Application Whitelisting
- Monitoring and Logging

All the Operating Systems, Applications and software are updated to latest versions and security patches are applied as per the respective OEM recommendations on a regular interval.

ISA should review the details available in the software to check the status of the Desktops or other endpoints that getting connected to the network and post review of the same the ISA should recommend if Vulnerability testing of the same is needed with Justifications for the same. Based on the recommendations and justification GMDC would decide and permit the ISA to conduct the VA for desktops. And for the same ISA should give the plan and parameters etc. that needs to be accessed

Vulnerability assessment and Testing of CCTV NVRs/CCTV Servers, Access and Biometric, IP Phones, IP SCADA systems in mines and all IOT devices getting connected to the network

Physical security and IOT threats have multiple adverse effects on organizations with varying degrees of severity, ranging from business interruptions and property loss, to legal complications, reputational loss and possibly, even a shutdown of business. **These factors have affected businesses throughout the globe making physical security an imperative business process in an organization**

With the entire domain of physical security, migrating to IP and multiple solutions installed to meet different security needs of the organization Vulnerability assessments of

- Security Assets
- Related systems

For all Devices which are getting connected to the GMDC Network the ISA needs to do the vulnerability assessment for the following risk defined in the below table:

Risk to assessed	Brief Description/Impact of the Risk
Device Credentials	Need to check if the device credentials being used by users are strong enough or needs an change
BIOS Version and Licensing	Check if the BIOS being used is using the latest version with necessary patches or it requires an upgrade thru patch management
Transmission compliance	Check for data transmission methodologies between device and application via the network
Application testing	Check of IOT, CCTV, Access control and other IP device applications which manage and store the date coming for the devices as per the Web application testing procedure defined above
Eavesdroppers:	A hacker tries to monitor data that pass through the network level with an aim of achieving that information in the form of plaintext. Check if the device is prone or eavesdropping or not
The Man in the Middle (MITM)	A hacker attempts inappropriate implementation of Secure Sockets Layer (SSL) to redirect all correspondence into his/her stations for observing the network traffics that can be transmitted in form readable text. Check if the device is prone or MITM or not
Man, at the end (MATE)	The attackers try to inspect or tamper the software or hardware of the physical device. Check if the device is prone or MATE or not
Wi-Fi Sniffing	An abuser attempts to find a router key and sign in as a trustworthy member of the system and network to control all the devices that work on that network. Check if the device is prone to Wi-Fi sniffing or not
App developers	User activity may be detected for injecting trackers into the apps or by installing malicious software, or information that leaks. Check if the device is prone to injection tracking or not
Shadow device check	Check if the device installed is properly authorized by the application or it is a shadow device or not

ISA to give details of the same in the audit report for each cloud services they assess. Over and above this if the ISA feels some additional parameters needs to accesses the same should be included. If gaps are found on the configuration and device front then mitigation measures for each of the gap and discrepancy should be defined clearly with a proposed architecture setup and security policy framework associated to the cloud services

Risk to assessed	Brief Description/Impact of the Risk
Device Credentials	Need to check if the device credentials being used by users are strong enough or needs an change
BIOS Version and Licensing	Check if the BIOS being used is using the latest version with necessary patches or it requires an upgrade thru patch management
Eavesdropping to intercept data	This is the act of illegitimately intercepting and receiving information communicated over wireless communication channels, which can possibly result in the affected information or data being compromised. Because the airwave is non-secure, an attacker can hijack the signal over the air from a certain distance
Bandwidth Congestion	Congestion of bandwidth is caused by piggybacking, which is the unauthorised access of a wireless LAN. It involves a practice of accessing a wireless internet connection by someone who uses another subscriber's wireless internet service without the person's explicit knowledge or permission. Piggybacking can also cause service violations, direct attack on your computer and illegal activities by malicious users which may be traced to you.
Wireless Network Sniffing	A wireless sniffer is a piece of software or hardware designed to intercept data as it is transmitted over a network and decode the data into a format that is readable for humans.
Denial-of Service Attacks	This is a situation whereby a wireless user is illegitimately deprived of the services of the network resources by a malicious attacker. The attacker floods the network with unnecessary messages to make the network unavailable to record the codes with some cracking devices during the recovery of the network, thereby breaking the security and gaining unauthorized access to information.
Wireless Spoofing attacks	Spoofing is a type of attack where an attacker uses information obtained by a wireless sniffer to impersonate another machine on the network. Spoofing attacks often target business' networks and can be used to steal sensitive information or run man-in-the-middle attacks against network hosts. Spoofing attacks can be mitigated using firewalls capable of deep packet inspection or by taking measures to verify the identity of the sender or recipient of a message
Traffic Redirection	This involves a change in the traffic route of a computer to that of a malicious attacker by manipulating the media access control (MAC) address as well as the IP address of a wired station
Rogue Access Point or Radio	This is a wireless access point that is installed by an attacker on a secure network without explicit authorization from a local network administrator (usually in public areas such as shared office space, airports, etc.), which accepts traffic from unsuspecting wireless clients to extract sensitive information.
Cafe Latte Attack	This type of attack allows an intruder to break into the WEP key of a remote client by sending a flood of encrypted ARP requests. If the ARP packet of the client is captured, he uses the ARP responses to obtain the WEP in just few minutes
Congestion Problem	Congestion problem is incurred in a communication network when free Random-Access Channel (RAC) is inaccessible by subscribers to either make or respond to a call. Hence, in-coming and outgoing calls experience blockage during congestion. Traffic channels congestions occurs when an Access Grant Channel cannot get any free traffic channel (TCH) to allocate to the request of the mobile terminal through the random-access channel.
Network Injection Attack (Majorly in Radios)	This is an attack whereby a cracker makes use of access points that are exposed to non-filtered network traffic (e.g. broadcasting network traffic) to inject fake networking re-configuration commands. This act can bring down a whole network and will require rebooting or even reprogramming of all intelligent networking devices.

Risk to assessed	Brief Description/Impact of the Risk
Man-in-the middle attack	This is a form of eavesdropping attack, whereby the attacker secretly intercepts a conversation between two parties. The attacker impersonates both parties and gains access to information that the two parties are trying to relay to each other. One type of man-in-the-middle attack relies on security faults in challenge and handshake protocols to execute a "de-authentication attack".

Post updation of the patches and addition of the hardware as per the recommendations in the audit report the ISA needs to conduct the second round of assessment and submit the final audit reports which will be used for applying for compliance certifications

Vulnerability Assessment and PET if required for indoor wireless solutions at Head Office and RF Links installed in mines

ISA to give details of the same in the audit report for each cloud services they assess. Over and above this if the ISA feels some additional parameters needs to accesses the same should be included. If gaps are found on the configuration and device front then mitigation measures for each of the gap and discrepancy should be defined clearly with a proposed architecture setup and security policy framework associated to the cloud services

Post updation of the patches and addition of the hardware as per the recommendations in the audit report the ISA needs to conduct the second round of assessment and submit the final audit reports which will be used for applying for compliance certifications.

Assessment for Security gaps and enhancement recommendation for Microsoft 365 Email

GMDC is using Microsoft Office 365 exchange solutions for email which is hosted in the Microsoft Data Center and the same needs to be accessed for the risks mentioned below:

Risk to assessed	**Brief Description/Impact of the Risk**
Spoofing and Phishing	Spoofing - a cybercriminal sends an email to a user pretending to be someone the user knows. Email spoofing is simple to do and difficult to track back to the original sender. Phishing is another risky tactic used by cybercriminals to obtain personal information such as a bank account or social security numbers by duping users.
Email Security Vulnerabilities	Taking advantage of the vulnerabilities discovered in email services, attacker can infiltrate the target system, expose information, and render systems inaccessible
Domain Squatting	The act of registering, selling, or using a domain name with the intent of profiting from someone else's trademark is known as domain squatting
Client-Side Attacks	The number of attack vectors available to internet users is growing every day. A single link containing malicious content may be enough to infect a device
Malicious Files	When malicious content in an email attachment reaches the user, it can take over the entire computer system and network
Ransomware	If someone becomes infected, a ransom must be paid for all encrypted data

Risk to assessed	Brief Description/Impact of the Risk
Errors in configuration	This is an all-too-common security problem. A badly designed email service can result in a crisis, allowing email to be sent without authentication
Database Exposure	A security breach exposes database information to hacking or theft, which is known as database exposure.
Browser Exploit Kit	Identity theft, data leakage, and access issues are all caused by emails that contain Internet browser vulnerabilities. An abused piece of code can often be found in a link.
Business Email Compromise (BEC) and Spear-Phishing Attacks	Another important point is that a cyber attacker who bypasses all security protocols attacks a device by exploiting the end user's unawareness since most people are unable to recognize a sophisticated phishing email.
File Format Exploits	File format vulnerabilities are quickly becoming one of the most serious information security risks that face many businesses. Attackers who take advantage of these flaws build carefully designed malicious files that trigger program flaws (such as buffer overflows). These vulnerabilities are particularly dangerous because they often affect several platforms.
Social engineering	Cyber attackers deploy psychological manipulation techniques via email to coerce victims into revealing sensitive information, or into downloading malware.
Password security.	One of the biggest email security risks pertains to password security. According to current NIST recommendations, password length, not password complexity is key to password strength
Brand impersonation	One of the most frightening email security risks consists of brand impersonation. Either your brand could be impersonated, or your employees could receive malicious messaging from a brand that is being impersonated.

ISA to give details of the same in the audit report for each cloud services they assess. Over and above this if the ISA feels some additional parameters needs to accesses the same should be included. If gaps are found on the configuration and device front then mitigation measures for each of the gap and discrepancy should be defined clearly with a proposed architecture setup and security policy framework associated to the cloud services

Post updation of the patches and addition of the hardware as per the recommendations in the audit report the ISA needs to conduct the second round of assessment and submit the final audit reports which will be used for applying for compliance certifications

Red Team Testing activity post VAPT and implementations of Audit recommendations

GMDC intends to do Red team testing uses ethical hacking to identify breaches to an organization's security system using real-world techniques like those used for social engineering attacks

GMDC intends to check Vulnerabilities in the following domains as mentioned below:

- **Technology:** using hacking strategies GMDC wants to identify risk areas related to networks, applications, routers and other types of technology.

- **Human resources:** To expose vulnerabilities associated to GMDC's human resources, like staff, independent contractors and business partners.
- **Infrastructure:** expose vulnerabilities related to the security of your infrastructure, including access to offices, data centers and warehouses.

The ISA needs to skilled manpower with minimum following skill set and experience

- Employees (On Board or Contractual) with Software development skills and the ability to develop custom tools to beat security systems
- Employees (On Board or Contractual) having Penetration testing experience and an understanding of how security systems work to avoid detection
- Employees (On Board or Contractual) with Social engineering skills and an understanding of how to persuade people to share sensitive information

Using this skill sets ISA needs to do Red Team audits for which they may use the below mentioned indicative tools

- Web application penetration testing to check for weaknesses in the design and configuration of your web applications.
- Network penetration testing to check weaknesses in your network or system.
- Social engineering tactics aim to persuade and manipulate human resources.

This is just a brief of the requirement defined. Based on the same the ISA needs to give an comprehensive plan for execution and scheduling part one he is onboard

Digital Forensics Readiness Assessment

GMDC intends to do Digital Forensic Readiness Assessment so that it can use maximize its potential to use digital evidence while minimizing the cost of an investigation

For the same the ISA needs to collect the below information and based on the same he need to review, access and do the gap analysis post which he needs to define a complete policy that will be enforced by the security team that will make GMDC Digital Forensic ready.

The keys points that needs to be reviewed and assessed are:

Review

- Existing network architecture, applications, process owners, Governance
- Available tools required for Digital Forensic Readiness.
- Existing log collection & retention policies of critical business applications, Firewall, IPS router, load balancer, SIEM tools etc.
- Cyber Security Incident Response policy & framework
- Legal & regulatory compliance requirements

Access

- Effectiveness of log collection & retention in tracing & tracking the security incident
- Effectiveness of log monitoring & analysis
- Effectiveness of existing controls in detection, prevention of attacks;
- Effectiveness of incident response such as handling, coordination & resolution;
- Effectiveness of evidence preservation, collection
- Awareness of SOC and IR team's skills related to forensic readiness

Using this data, the ISA needs to review access and do a gap analysis for the Digital Forensic Readiness assessment and based on the findings

- Recommend framework, policy, procedures for digital Forensic readiness
- Recommend enhancements to existing process & technology to support forensic readiness

This is just a brief of the requirement defined. Based on the same the ISA needs to give a comprehensive plan for execution and scheduling part one he is onboard

Compromise Assessment

GMDC indents to conduct a compromise assessment through its appointed ISA using non-intrusive methods to independently test certain network components and evaluate the presence of **indicators of compromise (IOCs)** and **indicators of attack (IOAs)**. The assessment focus on determining if any security breaches existed on the network.

The below mentioned Compromise Assessments needs to be carried. The details are:

- **Network compromise assessment:** This assessment will focus on evaluating the extent of a compromise within an organization's network infrastructure and identifying any vulnerabilities that may have contributed to the compromise.
- **Endpoint compromise assessment:** This assessment is will focus on evaluating the security of individual devices within an organization's network, such as laptops, tablets, and smartphones, on identifying any potential compromise or malware infections.
- **Application compromise assessment:** This assessment will evaluate the security of an individual application or system, looking for evidence of a compromise and identifying any vulnerabilities that may have been exploited.
- **Malware compromise assessment:** This assessment will focus on evaluating the presence and impact of malware on an organization's systems and identifying any vulnerabilities that may have enabled the malware to be introduced.
- **Insider threat compromise assessment:** This assessment will focus on evaluating the risk of compromise due to insider threats, such as employees or contractors who may have malicious intent or may inadvertently compromise the organization's systems.

This is just a brief of the requirement defined. Based on the same the ISA needs to give a comprehensive plan for execution and scheduling part one he is onboard

SECTION -9 ARCHITECTURE, POLICY AND FRAMEWORK FORMULATION FOR Additional SECURITY SOLUTIONS

Post Gap analysis and submission of audit which will have recommendations for improvement of configuration, identification of additional solution associated with security the ISA in principle needs to design

- Security Architecture based on the latest architectures prevailing in the market
- Design the complete Information Security Management Systems to be adapted by GMDC post the completion of all tasks that includes configuration changes, addition of hardware and architecture as recommended.
- For Monitoring and management design the architecture of Security Operations Center (SOC) for management, monitoring and dashboarding
- For Purpose of SOC support recommend analytical tools that will aid GMDC in predictively handling security threats by planning mitigation mechanisms
- Device an Incident Response, Business Continuity (BC) and Disaster Recovery (DR) plans for handling Disruptions, ranging from natural catastrophes to cybersecurity breaches, may devastate an organization's operations, sensitive information, and reputation

The brief details for each of the above points is mentioned below:

Security Architecture

The security architecture should ensure that

- Proper Attack surface management is done using tool like EASM (External Attack Surface Management) and associated. The ISA should ensure they define the positioning, specifications and configuration guideline for EASM solutions required by GMDC
- Access policy for device authentications using architectures like Zero Trusts which will be used for User authentication, device protection, data protection, Cloud services accessibility and application protection. The ISA should define the positioning, specifications and configuration guideline for Access solutions required by GMDC for the above-mentioned solutions along with the tentative cost structure for the same

Monitoring and Management

-
- The architecture and solution being offered should gather threat information from all solutions in the architecture and give a centralized view of all threats and vulnerabilities that are present in the solution matrix
- It should have a threat intelligence and detection solutions facilitating centralized threat intelligence and detection
- It should support Unified Management of all solutions that will facilitate Centralized - Policy management, Dashboarding, Altering and Investigation and Sandboxing using a single window
- All the above solutions should be AI and ML based
- The ISA should define the positioning, specifications and configuration guideline for Security Management and Monitoring solutions along with SOC design and details using tools like SIEM and SOAR as per the requirement of GMDC for the above-mentioned solutions along with the tentative cost structure for the same

- Initially GMDC may not set up the SOC as per the recommendations and till the time they might outsource the SOC services for with the ISA needs to define the complete solution modalities along with the cost tentative structure for the same.
-

Analytics for Security Operations centre

- To mitigate the threats and risk to the network predictive action is very helpful and for achieving this AI/ML based analytics should be a part of the SOC which would help GMDC to analyze the historical data and behavioural patterns in the network which would help GMDC in predictive decision making associated to security policy implementations
- The ISA should define the positioning, specifications and configuration guideline for Security Analytics solutions along with SOC design and details as per the requirement of GMDC for the above-mentioned solutions along with the tentative cost structure for the same

Incident Response, Business Continuity and Disaster Recovery Plans

The objective of Business Continuity Plan (BCP), Disaster Recovery Plan (DRP), and Incident Response Plan (IR) in place to protect an organization's operations, data, and reputation happening due to unforeseen reasons like cybersecurity breach or catastrophic failures happening due to natural disasters like flood, earthquake or manmade calamities like fire etc.

To tackle the above situations

- Post deployment of solutions and configurations as per audit recommendations the ISA needs to device an Incident Response policy framework document which will work in tandem with Business Continuity plans and Disaster recovery plans
- The complete set for frameworks for all three should be standards based and for each of the plan
- For BC plan and design the ISA should
  - Identify Critical Business Functions and IT assets associated to the same
  - Define operational methodologies for the same during times of failures
  - Define fall-back mechanism post recovery
  - Update the documents from the learnings if required
  - For DR plan and design the ISA should
  - Identify Critical Business Functions and IT assets associated to the same
  - Replication of IT assets associated to Critical Business with planning for backing data from Data center site to DR site as per the business requirement
  - Define operational methodologies for activating the DR during times of failures
  - Define fall-back mechanism post recovery
  - Update the documents from the learnings if required
  - GMDC is not having an DR site as of now. For the same ISA should define the positioning, specifications and configuration guideline for DR site solutions along with the tentative cost structure for the same

- For IR plan and design the ISA should
  - Design the plan based on the risk assessment done
  - Define clear guidelines for incident detection and action
  - Synergize IR plan with BC and DR
  - Define recovery plans for affected assets

- Update the plan if new incidents are recorded with updation of other sections like recovery plans etc. for the new incidents

These parameters are defined considering the bear minimum requirement on the operational and framework front but the ISA should not restrict the framework and the design considering this parameters only . Over and above this if additional parameters to comply to the industry best practices should be considered during the design and framework formulation for Incident response, Business continuity and Disaster Recovery plans

Project Management (during procurement and implementation of hardware / software as per architecture recommendations)

Post submission of the architecture design and gaps as mentioned in the audit report GMDC will invite bids for procurement of additional hardware/software on SITC basis during with the ISA will act as an Project Management Consultant (PMC) for the bid being floated. For the same the ISA will perform the following activities as listed below

- Review the technical specifications for the RFP being floated
- Assist GMDC in the procurement process
- Post ISA onboarding initiate the Kick off meeting with the ISA to device a complete project plan associated to installation, configuration and finetuning of the existing configuration
- On Approval of the plan the GMDC start the execution
- Monitor the complete installation and configuration processes
- Conduct regular co-ordination meetings with the ISA to review the project progress and resolve all bottlenecks impacting the installation and configuration schedules
- Define the Acceptance and Handover testing processes for GMDC
- Conduct Acceptance Testing and initiate the project closure activities
- Submit the project closure report to GMDC
- For the same the ISA should appoint certified Project Management Personals during the procurement and implementation phase

SECTION -10 USER TRAINING FOR CYBERSECURITY AWARENESS, POLICY IMPLEMENTATION

As a part of the Security enhancement to avoid security breaches Company, Contractual Employees, ISA employees dealing with GMDC and Employees/Team of Third Party carrying outsourced jobs for GMDC need to groomed for adaption of security policies finalized by the organization and for the same GMDC intends to conduct regular user training at all its locations during the ISA contract.

For the same the ISA should:

- **Design and develop** a comprehensive training module (Interactive which can be uploaded on the employee portal as well as presented to the employees physically)
- Post GMDC management consent **implement and roll out** the developed module by conducting offline and online sessions as per the agreed schedule definition
- Post completion of the session **Monitor** the progress on the adaptability front by thru appropriate feedback mechanisms and routine employee checks and based on the available data manage the gaps to ensure that security policies are stringently followed
- **Conduct refresh trainings** to share updated information associated to security threats and ensure the new practices to be followed are adapted and followed
- **Device Inspection mechanism** to check the employee security breaches happening post the training and post that work on the employee improvement associated to the adaption of security policies thru appropriate mechanisms

The following areas of concern that must be incorporated while designing the training module based on which the employees need to learn how to manage threats in the following areas:

- Phishing Attacks
- Ransomware
- Social Engineering
- Social Media Use
- Internet and Email Use
- Mobile Device Security
- Removable Media and Devices
- Passwords and Authentication
- Physical Security
- Work from Anywhere (WFA)
- Public Wi-Fi
- Cloud Security

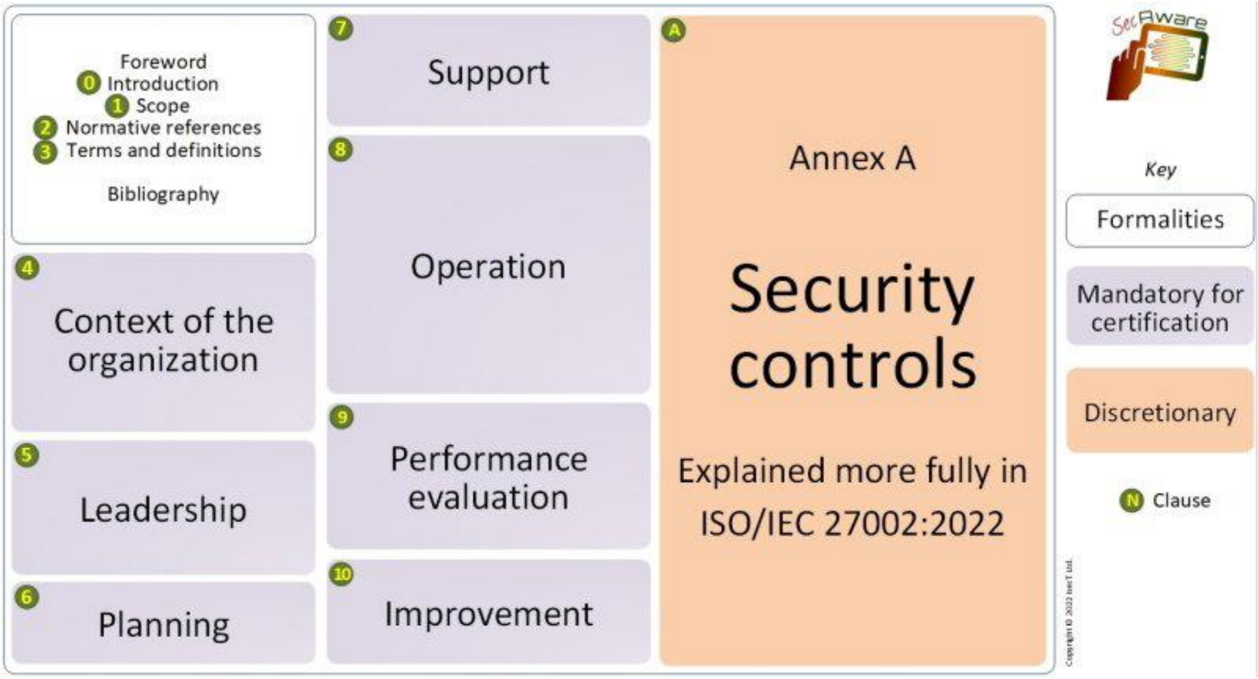
The ISA should define the complete module based on the above information as per the requirement of GMDC for the above-mentioned solutions

SECTION -11 AUDIT COMPLIANCE CERTIFICATIONS (TO BE INITIATED POST COMPLETION OF AUDITS/CORRECTIONS/DEPLOYEMENT OF ALL HARDWARE AS RECOMMENDED)

GMDC intends to go for Compliance certification process post the completion of Assessments, Audits, Configuration upgrades and architecture enhancement and conducting of training sessions. During this phases GMDC plans to adapt the ISO 27000 framework and thus ISA should conduct the activities considering the standards and regulations defined in the ISO Framework

An IT security framework is a series of documented processes that define policies and procedures around the implementation and ongoing management of information security controls. These frameworks may act as blueprint for managing risk and reducing vulnerabilities.

Structure of the standard



0 Introduction - the standard describes a process for systematically m`anaging information risks.

1 Scope - it specifies generic ISMS requirements suitable for organisations of any type, size or nature.

2 Normative references - only ISO/IEC 27000 is considered essential reading for users of '27001.

3 Terms and definitions - see ISO/IEC 27000.

4 Context of the organisation - understanding the organisational context, the needs and expectations of 'interested parties' and defining the scope of the ISMS. Section 4.4 states very plainly that "The organisation shall establish, implement, maintain and continually improve" the ISMS, meaning that it must be operational, more than merely designed and documented.

5 Leadership - top management must demonstrate leadership and commitment to the ISMS, mandate policy, and assign information security roles, responsibilities and authorities.

6 Planning - outlines the process to identify, analyse and plan to treat information risks, to clarify the *objectives* of information security, and to manage ISMS changes.

7 Support - adequate, competent resources must be assigned, awareness raised, documentation prepared and controlled.

8 Operation - more detail about assessing and treating information risks, managing changes, and documenting things (partly so that they can be audited by the certification auditors).

9 Performance evaluation - monitor, measure, analyse and evaluate/audit/review the information security controls, processes and management system, systematically improving things where necessary.

10 Improvement - address the findings of audits and reviews (*e.g.* nonconformities and corrective actions), systematically refining the ISMS.

Annex A Information security control reference - names the controls documented in ISO/IEC 27002:2022. The annex is 'normative' meaning that certified organisations are expected to use it to check their ISMS for completeness (according to clause 6.2), but that does *not* mean they are required to implement the controls: given their particular information risks, they may prefer other controls or risk treatments. Refer to ISO/IEC 27002 for lots more detail on the security controls, including useful implementation guidance, and ISO/IEC 27005 to understand information risk management.
Bibliography - points readers to related standards, plus part 1 of the ISO/IEC directives, for more information. In addition, ISO/IEC 27000 is identified in the body of the standard as a normative (*i.e.* essential) standard and there are several references to ISO 31000 on risk management.

Mandatory requirements for certification

ISO/IEC 27001 is a formalised specification for an ISMS with two distinct purposes:

1. It lays out the design for an ISMS, describing the important parts at a fairly high level;
2. It can (optionally) be used as the basis for formal conformity assessment by accredited certification auditors to certify an organisation conformant.

The following 14 items are explicitly required for certification:

1. ISMS scope (as per clause 4.3)
2. Information security policy (clause 5.2)
3. Information risk assessment *process* (clause 6.1.2)
4. Information risk treatment *process* (clause 6.1.3)
5. Information security objectives (clause 6.2)
6. Evidence of the competence of the people working in information security (clause 7.2)
7. Other ISMS-related documents deemed necessary by the organisation (clause 7.5.1b)
8. Operational planning and control documents (clause 8.1)
9. The *results* of the [information] risk assessments (clause 8.2)
10. The *decisions* regarding [information] risk treatment (clause 8.3)
11. Evidence of the monitoring and measurement of information security (clause 9.1)
12. The ISMS internal audit program and the results of audits conducted (clause 9.2).
13. Evidence of top management reviews of the ISMS (clause 9.3)
14. Evidence of nonconformities identified and corrective actions arising (clause 10.1)

The ISA should prepare this mandatory documentation is both present and fit for purpose, and may also check documentation relating to [an audit sample of] the discretionary controls.

The standard does not specify precisely what form the documentation should take, but clause 7.5.2 talks about aspects such as the titles, authors, formats, media, review and approval, while 7.5.3 concerns document control, implying a formal ISO 9001-style approach. Electronic documentation (such as intranet pages) are just as good as paper documents, in fact better in the sense that they are easier to control and maintain. Diagrams are fine too, supplementing or replacing written words - an ISMS documented *entirely* as a set of diagrams or videos would be novel, perhaps brilliant!

Considering the above requirement of GMDC and the definition of ISO 27001 and 27002 as above the ISA should come up with a complete program methodology for certification and during the course of design the ISA should adapt all applicable standards from the set of 60 standards in the 27000 series and ensure that the policy formulation, assessment and the audit process and other scheduled activities listed in the documents comply with the standards as defined in the ISO 27002

SECTION -12 UNPRICED BOQ FOR TECHNICAL DETAILS OF TOOLS, MANPOWER DETAILS

The ISA needs to provide all the details as mentioned below. For all tools technical data of the tools and sample reports generated should be provided and if Licensing is to be done it should be done on the name of GMDC and for that GMDC will not pay any extra cost to the ISA

For Surveys if required the ISA needs to make all boarding lodging arrangement on his own and GMDC will ensure that at site the necessary officer is present to assist the ISA team members. The ISA should consider all these it its costing and if possible give the brief details of the travel days and costs considered in the bid

UNPRICED BOQ FORMAT

Sr._no	**Description of Task and Sub Tasks**	**Compl-etion period (weeks)**	**Details of Tools that will be used**			**Manpower Details**	
			Freeware	**Licensed**	**Proprietary**	**Total years of experience**	**Certification Details**
	PHASE I						
01	Security Hardening (Policy review and Assessment) post review of GMDC Asset discovery process as defined in the SOW						
	PHASE II						
02	**Vulnerability Assessments and Penetration Testing**						
2.1	Vulnerability assessment and Penetration Testing for Network and Security Infrastructure						
2.2	Vulnerability assessment and Testing for Application Testing (Web based/ ERP/ Website/ Database /APIs)						
2.3	Vulnerability assessment and Testing for Cloud based services (SAAS/PASS/IAAS))						
2.4	Vulnerability assessment and Testing of End Points						

UNPRICED BOQ FORMAT							
Sr. _ no	**Description of Task and Sub Tasks**	**Compl-etion period (weeks)**	**Details of Tools that will be used**			**Manpower Details**	
			Freeware	**Licensed**	**Proprietary**	**Total years of experience**	**Certification Details**
	(Desktops/Laptops/Tablets/BYOD devices getting connected to the network)						
2.5	Vulnerability assessment and Testing of IOT Endpoints (CCTV NVRs/CCTV Servers Access and Biometric, IP Phones, IP SCADA systems in mines and all IOT devices getting connected to the network)						
2.6	Vulnerability Assessment and PET if required for indoor wireless solutions at Head Office and RF Links installed in mines						
2.7	Assessment for Security gaps and enhancement recommendation for Microsoft 365 Email solutions being used by GMDC						
03	Architecture, policy and framework formulation for additional different solutions as defined in the SoW section 4 and details in Section 9						
	PHASE III						
04	Project Management Consultancy support during the course Change management phase (Configuration						

UNPRICED BOQ FORMAT							
Sr._no	**Description of Task and Sub Tasks**	**Completion period (weeks)**	**Details of Tools that will be used**			**Manpower Details**	
			Freeware	**Licensed**	**Proprietary**	**Total years of experience**	**Certification Details**
	updation and procurement of additional hardware software) As per the details mentioned in Section 9						
05	Primary User training as per the module designed by the ISA (scheduled offline session to be conducted at all locations)						
	PHASE IV						
06	Second round of VAPT audits post readiness of infrastructure as per the audit recommendation and security architecture						
07	Compromise Assessment Audit						
08	Digital Forensic Readiness Assessment						
09	Red Team testing to check resilience of the complete infrastructure to cyber attacks						
10	Mock Drill for Incident management and Business continuity using DR site						
11	Publishing of complete ISMS policy post management approval and user training for creating awareness						
	PHASE V						
12	Initiation of Compliance certification process						

UNPRICED BOQ FORMAT							
Sr._ no	**Description of Task and Sub Tasks**	**Compl-etion period (weeks)**	**Details of Tools that will be used**			**Manpower Details**	
			Freeware	**Licensed**	**Proprietary**	**Total years of experience**	**Certification Details**
	for ISO 27001 certificate						

Considering the tentative timelines defined in the Scope of work section the ISA should

- Define the timelines for each task in each phase in the unpriced BOQ section to be submitted with the technical bid and based on that timelines offer the cost in the priced BOQ
- The total time of the contract would be 1 year in which all of the above activities needs to be complete
- If by any means the procurement process as defined in phase III is taking time and the contract period is getting over there will be two options
- One by mutual consent of the ISA and GMDC the contract period will be extended
- Two if the ISA is willing to close the project with doing activities as defined in Phase IV and V the project will be closed

SECTION -13 PRICED BOQ FOR TECHNICAL DETAILS OF TOOLS, MANPOWER DETAILS

The ISA needs to submit the price bid online in the format as mentioned below:

Sr._ no	**Description of Task and Sub Tasks**	**UOM**	**Quantity**	**Unit Price without Tax (INR)**	**Total Price without Tax (INR)**	**Applicable GST (INR)**	**Total Price with tax (INR)**
	PHASE I						
01	Security Hardening (Policy review and Assessment) post review of GMDC Asset discovery process as defined in the SOW	Job	01				
	PHASE II						
02	**Vulnerability Assessments and Penetration Testing**						
2.1	Vulnerability assessment and Penetration Testing for Network and Security Infrastructure	Job	01				
2.2	Vulnerability assessment and Testing for Application Testing (Web based/ ERP/ Website/ Database /APIs)	Job	01				

Sr._ no	Description of Task and Sub Tasks	UOM	Quantity	Unit Price without Tax (INR)	Total Price without Tax (INR)	Applicable GST (INR)	Total Price with tax (INR)
2.3	Vulnerability assessment and Testing for Cloud based services (SAAS/PASS/IAAS))	Job	01				
2.4	Vulnerability assessment and Testing of End Points (Desktops/Laptops/Tablets/ BYOD devices getting connected to the network).	Nos	600				
2.5	Vulnerability assessment and Testing of IOT Endpoints (CCTV NVRs/CCTV Servers Access and Biometric, IP Phones, IP SCADA systems in mines and all IOT devices getting connected to the network)	Nos	300				
2.6	Vulnerability Assessment and PET if required for indoor wireless solutions at Head Office and RF Links installed in mines	Job	01				
2.7	Assessment for Security gaps and enhancement recommendation for Microsoft 365 Email solutions being used by GMDC	Job	01				
03	Architecture, policy and framework formulation for additional different solutions as defined in the SoW Section 4 and Details in Section 9	Job	01				
	PHASE III						
04	Project Management Consultancy support during the course Change management phase (Configuration updation and procurement of additional hardware software) As per the details mentioned in Section 9	Job	01				
05	Primary User training as per the module designed by the ISA (scheduled offline session to be conducted at all locations)	Job	01				
	PHASE IV						
06	Second round of VAPT audits post readiness of infrastructure as per the audit recommendation and security architecture	Job	01				
07	Compromise Assessment Audit	Job	01				
08	Digital Forensic Readiness Assessment	Job	01				
09	Red Team testing to check resilience of the complete infrastructure to cyber attacks	Job	01				

Sr._ no	Description of Task and Sub Tasks	UOM	Quantity	Unit Price without Tax (INR)	Total Price without Tax (INR)	Applicable GST (INR)	Total Price with tax (INR)
10	Mock Drill for Incident management and Business continuity using DR site	Job	01				
11	Publishing of complete ISMS policy post management approval and user training for creating awareness	Job	01				
	PHASE V						
12	Initiation of Compliance certification process for ISO 27001 certificate	Job	01				
	Total						

While offering the costs the bidder should

- Define the timelines for each task in each phase in the unpriced BOQ section to be submitted with the technical bid and based on that timelines offer the cost in the priced BOQ
- The cost of all tools
- Manpower costs
- Travel costs including boarding lodging etc
- Any cost of hardware additionally required by the bidder for testing purposes
- Documentation costs (03 sets to be provided)

GMDC will only pay to the ISA for the services they take based on the unit rates defined

SECTION-14 ANNEXURES

Annexure – I - Format of Earnest Money Deposit in the form of Bank Guarantee

(On Non-judicial Stamp paper to be submitted along with submission of bids)

…………………………………………………………………. (Name of the Bank)
Address……………………………………………………………………………….Guarantee No……………………..
A/C Messer's………………………………………………………. (Name of Bidder)
Date of Expiry………………………………. Limit to liability (currency & amount)……………………………….
Invitation For RFQ No……………. dated…………………(bidding document)
For…………………………………………………….. (Name of Facilities)

Subject: Earnest Money Deposit Bank Guarantee.
Date………………20

To,
General Manger (IT),
Gujarat Mineral Development Corporation Ltd.
132 Ft Ring Road, Near University Ground
Vastrapur, Ahmedabad.
Bank Code:

Dear Sir,

In consideration of Gujarat Mineral Development Corporation (hereinafter called "GMDC") which expression shall unless repugnant to the subject of context include his successors and assigns having agreed to exempt M/s…………………………………. (herein after called "Bidder") from demand under the terms and conditions of "Technical Bid Document" (hereinafter called the said "Bidding Document") issued by the GMDC vide RFQ No.______________for the work____ (Name of the facilities) from Earnest Money Deposit (EMD) of Bid for the due fulfillment by the Bidder of the terms and conditions contained in the said Bidding Document on production of Bank Guarantee for INR _________________(____ only) (figure in words).

1. We the _______________________ (Name of Bank) hereinafter referred to as "Bank" having our registered office at ________________________ (address of Bank) do hereby undertake and agree to indemnify and keep indemnified GMDC to extent of INR __________________(___________________ only) (figures in words) against any losses, damage cost, charges and expenses caused to or suffered by or that may be caused or suffered by GMDC by reason of any breach or breaches by the Bidder of any of the terms and conditions contained in the said Bidding Document and unconditionally pay the amount claimed by GMDC on demand and without demur to the extent aforesaid.
2. We __________________________ (Name of Bank) do hereby undertake to pay the amounts due and payable under the guarantee without any demur merely on a demand by you stating that the amount claimed is due by way of loss or damage caused to or would be caused or suffered by you by reason of any breach by the said Bidderof any of the terms or conditions contained in the said Bidding

Document by reason of the Bidder's failure to fulfill the conditions of said Bidding Document. Any such demand 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 INR________________________ _________________.

3. We ___________________________ (Name of Bank) further agree that GMDC shall be the sole judge of and as to whether the Bidderhas committed any breach or breaches of terms and conditions of the said Bidding Document and the extent of loss, damages, costs, charges and expenses caused to or suffered by or that may caused to or suffered by GMDC on account hereof to the extent of the Bid Security required to be deposited by the Bidderin respect of the said document and the decision of GMDC that the Bidder has committed such breach or breaches and as to the amount or amounts of loss, damages, costs, charges, and expenses caused to or suffered by or that may be caused to or suffered by GMDC shall be final and binding on us.

4. We ___________________________ (Name of Bank) further agree that guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance on the said Bidding Document and that it shall continue to be enforceable till you certify that terms and conditions of the said Bidding Document have been fully and properly carried out by the said Bidder and accordingly discharge the guarantee. Unless a demand or claim under this guaranteed is made on us in writing on or before the (date) __________________ we shall be discharged from all liability under this guarantee.

5. We ___________________________ (Name of Bank) further agree with you that you 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 Bidding Document or to extend time of performance by the said Bidder from time to time or to postpone for any time or from time to time any of the powers exercisable by you against the said Bidder and to forbear or enforce any of the terms and conditions relating to the said Bidding Document and we shall not be relieved from our liability by reason of any such variation or extension being granted to the said Bidderor for any forbearance act or omission on your part or any indulgence by you to the said Bidderor any such matter or thing whatsoever under the law relating to sureties would but for this provision have effect of so relieving us.

6. It shall not be necessary for GMDC to proceed against the Bidder before proceeding against the Bank and the Guarantee herein contained shall be enforceable against the Bank, notwithstanding any security which GMDC may have obtained from the Bidder at this time when proceeding are taken against Bank hereunder be outstanding or unrealized.

7. We ________________________ (Name of Bank) further undertake to unconditionally pay the amount claimed by GMDC merely on demand and without demur to the extent aforesaid.

8. We, the said Bank lastly undertake not to revoke this guarantee during its currency except with the previous consent of GMDC in writing and agree that any change in the constitution of GMDC or the Bidder or the said Bank shall not discharged our liability hereunder dated _________________day of ____________ 20 . _____________ for ________________________________ (Name of Bank)

Yours faithfully

For......................................(Name of the Bank)

Please note the following details for Compulsory e-confirmation for Bank Guarantee through ICICI Bank through SFMS under our:

Gujarat Mineral Development Corporation Limited (GMDC)
132 Ft Ring Road, Near University Ground Vastrapur, Ahmedabad. Bank Name: ICICI Bank Ltd
IFS Code: ICIC0000024

UIC GMDC530265584 for Field 7037 MT760

Annexure – II: Performance Bank Guarantee Format

(To be stamped in accordance with Stamp Act)

Ref: Bank Guarantee No.

Date:

To,
The General Manager- IT
Gujarat Mineral Development Corporation
Khanij Bhavan
132 ft Ring Road, Ahmedabad

Dear Sir,

1.WHEREAS............................ (Name of ISA) hereinafter called "the ISA" has undertaken, in pursuance of Agreement dated, (here in after referred to as "the Agreement SERVICE DELIVERY FOR VARIOUS CYBERSERCURITY REALTED AT GMDC HO AND ITS OFFICES. AND WHEREAS it has been stipulated in the said Agreement that the ISA shall furnish a Bank Guarantee ("the Guarantee") from a scheduled bank for the sum specified therein as security for implementing PROJECT.

2. WHEREAS we __________ ("the Bank", which expression shall be deemed to include it successors and permitted assigns) have agreed to give the GMDC the Guarantee:
THEREFORE, the Bank hereby agrees and affirms as follows:

The Bank hereby irrevocably and unconditionally guarantees the payment of all sums due and payable by the ISA to GMDC under the terms of their Agreement dated _______________. Provided, however, that the maximum liability of the Bank towards GMDC under this Guarantee shall not, under any circumstances, exceed ___________________________________ in aggregate.

3. In pursuance of this Guarantee, the Bank shall, immediately upon the receipt of a written notice from GMDC in that behalf and without delay/demur or set off, pay to GMDC a[1]ny and all sums demanded by GMDC under the said demand notice, subject to the maximum limits specified in Clause 1 above. A notice from GMDC to the Bank shall be sent by Registered Post (Acknowledgement Due) at the following address:

____

____

____

Attention Mr. _____________.

4. This Guarantee shall come into effect immediately upon execution and shall remain in force for a period of _____ months from the date of its execution. The Bank shall extend the Guarantee for a further period which may mutually decide by the ISA & GMDC. The liability of the Bank under the terms

[1]

of this Guarantee shall not, in any manner whatsoever, be modified, discharged, or otherwise affected by:

- Any change or amendment to the terms and conditions of the Contract or the execution of any further Agreements.

- Any breach or non-compliance by the ISA with any of the terms and conditions of any Agreements/credit arrangement, present or future, between ISA and the Bank.

5. The BANK also agrees that GMDC at its option shall be entitled to enforce this Guarantee against the Bank as a Principal Debtor, in the first instance without proceeding against the ISA and not withstanding any security or other guarantee that GMDC may have in relation to the ISA's liabilities.

6. The BANK shall not be released of its obligations under these presents by reason of any act of omission or commission on the part of GMDC or any other indulgence shown by GMDC or by any other matter or thing whatsoever which under law would, but for this provision, have the effect of relieving the BANK.

7. This Guarantee shall be governed by the laws of India and the courts of Ahmedabad shall have jurisdiction in the adjudication of any dispute which may arise hereunder.

Dated this the ………………. Day of ……………………..

Witness

(Signature) (Signature)

(Name) Bank Rubber Stamp

(Name)

(Official Address) Designation with Bank Stamp

Plus, Attorney as per Power of Attorney No. Dated:

Annexure – III: Earnest Money Deposit & RFP Processing Fee Details

Sr. No.	Item	Amount (In Rs.)	Name of the Bank & Branch	Demand Draft No.
2	RFP Processing Fee			
1	Earnest Money Deposit (E.M.D.)			

Annexure IV - RFP LETTER FORM

From
(Registered name and address of the ISA.)

Date:

To,
The General Manager- IT
Gujarat Mineral Development Corporation
Khanij Bhavan
132 ft Ring Road, Ahmedabad

Sir,

Having examined the RFP documents, we the undersigned, offer the Services as detailed in the bidding document (as enclosed) in response to T/E number ....dated **..................**

we undertake to:

1) maintain validity of the RFP for a period of 6 months from the last date of RFP submission as specified in the bidding document or extended. The same shall remain binding upon us and may be accepted at any time before the expiration of that period.

2) Offer services during the bid period in conformity with the bidding documents (and as amended from time to time).

3) Complete the Service delivery execution within the time frame as defined in the RFP documents (and as amended from time to time)

4) execute all contractual documents and provide all securities & guarantees as required in the RFP document (and as amended from time to time).

5) until a formal Contract is prepared and executed, this RFP, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract on us.

Dated this _______ day of ____________.
Signature
(in the capacity of)

Duly authorized to sign RFP for and on behalf of

Witness:
(Signatures with name and designation), Address:

Annexure V – DECLARATION FOR NON BLACKLISTING

On letter head of the Bidder)

DATE:

To,
The General Manager (IT),
Gujarat Mineral Development GMDC Ltd.,
"Khanij Bhavan", 132 ft. Ring Road,
University Ground, Vastrapur,
Ahmedabad-380015

Dear Sir,

I/we here by solemnly declare that

1. The Bidder or its directors have not been blacklisted by any Government Organization, in last 5 years from the date of uploading of RFQ.
2. We have not put any condition in our offer with respect to RFQ No.______,
3. We have accepted all the terms and conditions, including Annexure, Corrigendum if any, as specified in the RFQ Document No. ____________ unconditionally.

I/we here by further declare that, if the declaration is found untrue, the GMDC shall be entitled to take any action against us severally and/or individually or our Bidder/GMDC in this regard in any manner that may be deemed fit by GMDC.

Yours faithfully,

____
Signature and Stamp of the Bidder

Annexure VI Work Experience details -as mentioned in the Pre- qualification criteria

Experience in supply, installation commissioning and maintenance for TELEPHONY Solutions							
Sr. no	Name of the Organization	Address of execution	Start Date of the Project	Completion Date of the Project	Scope of Work Description in Brief as per the definition in PQ and QCBS tables	Value of The Project in Rs.	Supporting PO and Completion Certificate attached or not
1							
2							
3							
4							
5							
6							

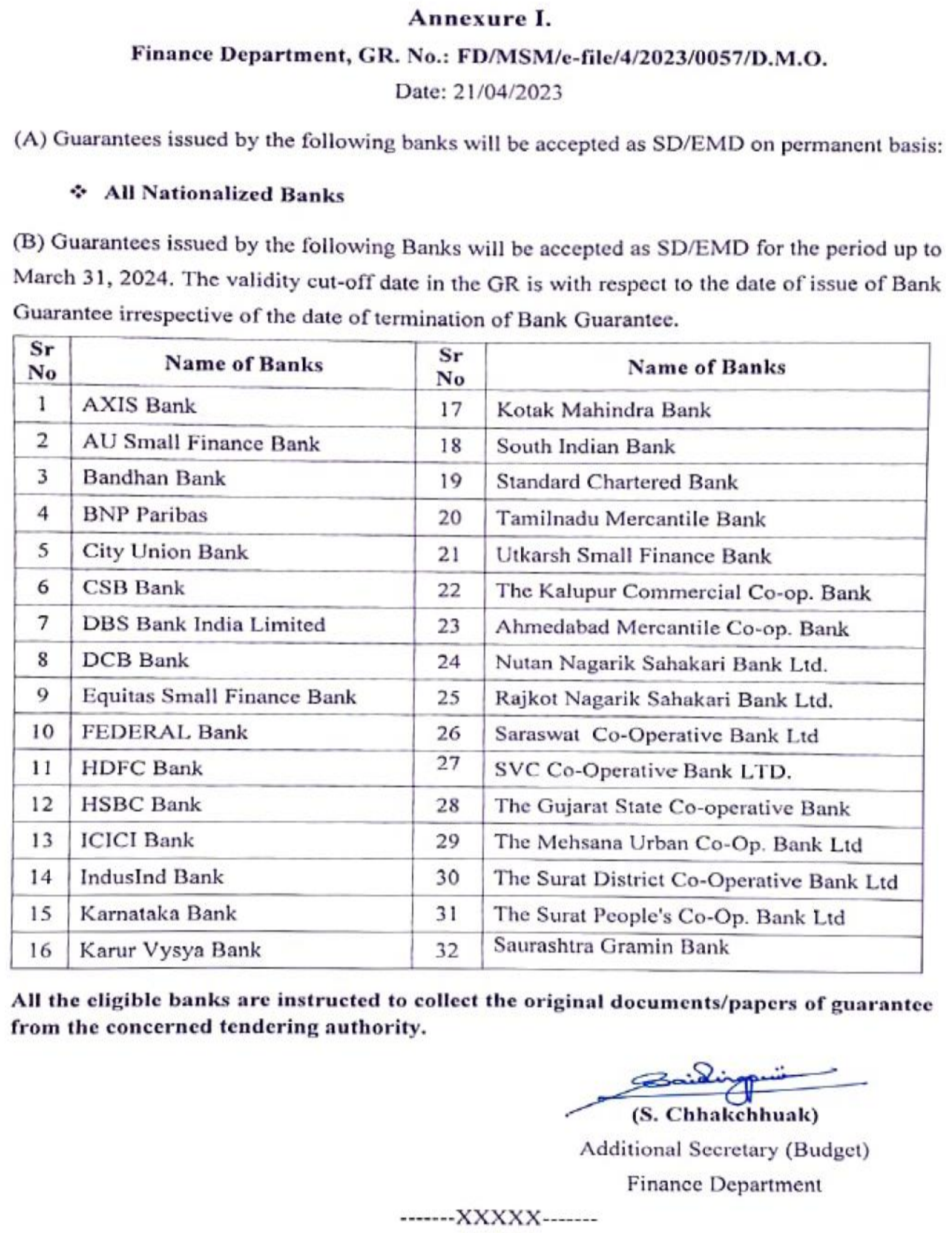
Annexure VII Financial Strength of the ISA

Financial Year	Turn Over in Lakhs of Rupees	System Integration Turnover in LACS	Audited Accounts submitted? (Yes/No) and Supporting Auditor Certificate for Security Services Turnover submitted (YES/NO)
2020-2021			
2021-2022			
2022-2023			
Note: Please fill this form and attach the audited Annual Accounts for the last three financial years along with the Auditor Certificate confirming the System Integration Turnover			

Annexure VIII Manpower Details on ISA Roll

Sr. No.	Name of Certified Professional	Date of Joining the Organization	PF No. Details of the Employee	Designation	Experience Details in years	Contact Details	CERTIFICATION DETAILS	Details of Projects handled with Brief Scope of work for each project
1								
2								
3								
4								
5								

Annexure IX – Bank List



Annexure I.

Finance Department, GR. No.: FD/MSM/e-file/4/2023/0057/D.M.O.

Date: 21/04/2023

(A) Guarantees issued by the following banks will be accepted as SD/EMD on permanent basis:

- **All Nationalized Banks**

(B) Guarantees issued by the following Banks will be accepted as SD/EMD for the period up to March 31, 2024. The validity cut-off date in the GR is with respect to the date of issue of Bank Guarantee irrespective of the date of termination of Bank Guarantee.

Sr No	Name of Banks	Sr No	Name of Banks
1	AXIS Bank	17	Kotak Mahindra Bank
2	AU Small Finance Bank	18	South Indian Bank
3	Bandhan Bank	19	Standard Chartered Bank
4	BNP Paribas	20	Tamilnadu Mercantile Bank
5	City Union Bank	21	Utkarsh Small Finance Bank
6	CSB Bank	22	The Kalupur Commercial Co-op. Bank
7	DBS Bank India Limited	23	Ahmedabad Mercantile Co-op. Bank
8	DCB Bank	24	Nutan Nagarik Sahakari Bank Ltd.
9	Equitas Small Finance Bank	25	Rajkot Nagarik Sahakari Bank Ltd.
10	FEDERAL Bank	26	Saraswat Co-Operative Bank Ltd
11	HDFC Bank	27	SVC Co-Operative Bank LTD.
12	HSBC Bank	28	The Gujarat State Co-operative Bank
13	ICICI Bank	29	The Mehsana Urban Co-Op. Bank Ltd
14	IndusInd Bank	30	The Surat District Co-Operative Bank Ltd
15	Karnataka Bank	31	The Surat People's Co-Op. Bank Ltd
16	Karur Vysya Bank	32	Saurashtra Gramin Bank

All the eligible banks are instructed to collect the original documents/papers of guarantee from the concerned tendering authority.

(S. Chhakchhuak)
Additional Secretary (Budget)
Finance Department

-------XXXXX-------