



Directorate of ICT & e-Governance

Department of Science & Technology
Government of Gujarat

Directorate of ICT & e-Governance

Block No. 2, 2nd Floor, C & D Wing, Karmayogi Bhavan,
Sector - 10 A, Gandhinagar - 382010

Request for Proposal (RFP)

for

External Attack Surface Management (EASM),

Digital Risk Monitoring (DRM),

Incident Response (IR) Services for 2 Years

for

Gujarat Security Operations Center, Directorate of ICT & e-Governance, Department of Science & Technology, Gujarat

GeM Bid# GEM/2026/B/7942125

1. DISCLAIMER:

Directorate of ICT & e-Governance (DIT)/GIL, through this RFP, invites proposals from reputed firms (hereafter referred to as 'Bidders') that meet the evaluation criteria and can be onboarded to offer an External Attack Surface Management (EASM), Digital Risk Monitoring (DRM), Incident Response (IR) Services for the Gujarat Security Operations Centre (GSOC), Gandhinagar.

The information contained in this Request for Proposal (RFP) document or subsequently provided to Bidder(s), whether verbally or in documentary or any other form by or on behalf of the DIT/GIL/DST, Government of Gujarat or any of their employees or consultants, is provided to Bidder(s) on the terms and conditions set out in this RFP and such other terms and conditions subject to which such information is provided.

The purpose of this RFP is to provide interested parties with information that may be useful to them in eliciting their financial offers (the "Proposal") pursuant to this RFP. This RFP includes statements, which reflect various assumptions and assessments arrived at by the TENDERER, in relation to the RFP. Such assumptions, assessments and statements do not purport to contain all the information that each Bidder may require. This RFP may not be appropriate for all persons, and it is not possible for the TENDERER, its employees, or Consultants to consider the investment objectives, financial situation and particular need of each party who reads or uses this RFP. The assumptions, assessments, statements, and information contained in this RFP may not be complete, accurate, adequate, or correct. Each Bidder should, therefore, conduct its own surveys and analysis and should check the accuracy, adequacy, correctness, reliability, and completeness of the assumptions, assessments, statements, and information contained in this RFP and obtain independent advice from appropriate sources before filling out the RFP. Any deviation in the specification or proposed solutions will be deemed as incapability of the respective Agency and shall not be considered for the final evaluation process.

Information provided in this document to the Bidder(s) is on a wide range of matters, some of which depend upon interpretation of law. The information given is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. The TENDERER accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein.

TENDERER- its employees and advisors make no representation or warranty and shall have no liability to any person, including any Applicant or Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness, delay or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way during the Bidding process.

2. ABBREVIATIONS:

Abbreviation	Description
Authorized Signatory	The bidder's representative/ officer vested (explicitly, implicitly, or through conduct) with the powers to commit the authorizing organization to a binding agreement. Also called signing officer/ authority having the Power of Attorney (PoA) from the competent authority of the respective Bidding firm.
Bid	"Bid" means the response to this document presented in Technical Bid and Financial Bid, which are submitted online with necessary documents and forms as given in Annexure, complete in all respects, adhering to the instructions and spirit of this document.
Bidder	"Bidder" means any company/firm/agency responding to this Request for Proposal and who submits their Bid.
BOM	Bill of Material
BOQ	Bill of Quantity
Client	User Department/User Department's Client
Contract/ Procurement Contract	Means the contract of service entered between the procuring entity and the "Service Provider" for SITC of SAN Storage Solution with Comprehensive Onsite Warranty Support for Gujarat Security Operations Centre (GSOC), Gandhinagar with the entire documentation specified in the RFP.
Consignee	User Department - Gujarat Security Operations Centre (GSOC)
Day	"Day" means a working day as per the rules of the User Department.
DIT	Directorate of ICT & e-Governance
DST	Department of Science & Technology
GIL	Gujarat Informatics Limited
GSOC	Gujarat Security Operations Centre
GoG	Government of Gujarat
EMD	Earnest Money Deposit
PBG	Performance Bank Guarantee
Purchaser	User Department
TC	Tender Committee
GST	Goods & Service Tax
Incident	"Incident" refers to any event/issue that affects the normal functioning of the services/infrastructure, reported by the Client to the Supplier.
Response Time	"Response time" is the time interval between Client-initiated event (e.g., logging of the request/mail) and the bidder-initiated event in response to that stimulus.
RPO	Recovery Point Objective is the maximum acceptable amount of data loss measured in time that an organization can tolerate following a disruption.
RTO	Recovery Time Objective is the maximum acceptable downtime for a system, application, or process after a disaster or failure.
OEM	Original Equipment Manufacturer
TPA	Third Party Auditor
SLA	Service Level Agreement
POA	Power of Attorney
UAT	User Acceptance Testing
PROD	Production (Environment)

DR	Disaster Recovery
BCP	Business Continuity Plan (or Business Continuity Planning)
TPS / RPS	Transactions Per Second / Requests Per Second
EASM	External Attack Surface Management
IR	Incident Response (IR) Services
DRM	Digital Risk Monitoring

3. DEFINITIONS:

In this document, the following terms shall have the following respective meanings:

1. **"Acceptance Test (AT)"** means the acceptance testing of the ordered product & services on completion of installation and commissioning under the project.
2. **"Acceptance Test Document"** means a document, which defines procedures for testing the Gujarat Security Operations Centre against requirements laid down in the Agreement.
3. **"Agreement"** means the Service Level Agreement to be signed between the successful bidder and DIT/GIL/SOC/DST/GoG including all attachments, appendices, all documents incorporated by reference thereto together with any subsequent modifications, the RFP, the bid offer, the acceptance and all related correspondences, clarifications, presentations.
4. **"Authorized Representative/Agency"** shall mean any person/agency authorized by either of the parties.
5. **"Bidder"** means any agency providing similar solutions as per the scope of work of RFP. The word Bidder when used in the pre-award period shall be synonymous with Bidder, and when used after award of the Contract shall mean the successful Bidder with whom GoG signs the Service Level Agreement.
6. **"Contract"** is used synonymously with Agreement.
7. **"Corrupt Practice"** means the offering, giving, receiving or soliciting of anything of value or influence the action of a public official in the process of Contract execution.
8. **"Default Notice"** means the written notice of Default of the Agreement issued by one Party to the other in terms hereof.
9. **"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 Bidders (before or after Bid submission) designed to establish Bid prices at artificial non- competitive levels and to deprive GoG of the benefits of free and open competition.
10. **"Good Industry Practice"** means the exercise of that degree of skill, diligence and prudence which would reasonably and ordinarily be expected from a reasonably skilled and experienced Operator engaged in the same type of undertaking under the same or similar circumstances.
11. **"Law"** shall mean any act, notification, by-law, rules and regulations, directive, ordinance, order or instruction having the force of law enacted or issued by the Central Government and/ or the Government of Gujarat or any other Government or regulatory authority or political subdivision of government agency.
12. **"LoI"** means Letter of Intent, which constitutes the intention of the GoG to place the Purchase Order with the successful bidder.
13. **"LOA"** shall mean Letter of Award of work issued by GoG to the successful bidder. LOA will be issued after the successful bidder gives his acceptance to the LoI.
14. **"Request for Proposal"** means the detailed notification seeking a set of solution(s), service(s), materials and/or any combination of them.
15. **"Requirements"** shall mean and include schedules, details, description, statement of technical data, performance characteristics, standards (Indian as well as International) as applicable and specified in the Agreement.
16. **"Service"** means provision of Contracted Services for purchaser, GoG.
17. **"Termination Notice"** means the written notice of termination of the Agreement issued by one Party to the other in terms hereof.
18. **"Uptime"** means the time period when specified services are available to GoG and its user organizations. The uptime will be calculated as follows:
 - Total time in a quarter (in minutes) less total Service Downtime (in minutes) in the quarter.
19. **"% Uptime"** means the ratio of 'uptime' (in minutes) in a quarter to total time in the quarter (in minutes) multiplied by 100.

20. **“Downtime”** means accumulated time during which the System is totally inoperable within the Scheduled Operation Time but outside the Scheduled Maintenance Time.
21. **“Incident”** refers to any event/abnormalities in the functioning of the GoG components & operations which may lead to disruption in normal operations of the GoG.
22. **“Support”** shall mean the 24x7x365 support which shall handle patch updates, Fault Reporting, Trouble Ticketing, and resolution of related enquiries during the contract period.
23. **“Scheduled Maintenance Time / Scheduled downtime”** shall mean the time that the System is not in service due to scheduled work. Scheduled maintenance time is planned downtime with the prior permission (Minimum 48 Hour prior Notice) of the GSOC Team.
24. **“Scheduled Operation Time”** means the scheduled operating hours of the System for the month. All scheduled maintenance time on the system would be deducted from the total operation time for the month to give the scheduled operation time. The total operation time for the solution will be 24x7x365.
25. **“GSWAN – Gujarat State Wide Area Network”** is the IT Backbone of the state of Gujarat.
26. **“GSDC- Gujarat State Data Centre”** is the central location where all the IT infrastructure of the State of Gujarat is hosted.

4. INTRODUCTION AND GENERAL INFORMATION:

This Request for Proposal (RFP) has been published for and on behalf of the Gujarat Security Operations Center (GSOC), Directorate of ICT & e-Governance, Department of Science & Technology (DST), GoG, to select an Agency for Providing External Attack Surface Management (EASM), Digital Risk Monitoring (DRM), Incident Response (IR) Services for Gujarat Security Operations Center, Department of Science & Technology, Government of Gujarat. The Successful Bidder will be liable for the entire scope of work mentioned/defined in this RFP document along with its corrigendum/clarifications etc.

Gujarat Informatics Limited (GIL), acting as the Bidding agency for the Government of Gujarat, hereby invites proposals from eligible bidders who meet the qualification criteria prescribed in this RFP and possess the requisite technical expertise, experience, and capabilities to deliver the required associated services in accordance with the requirements specified herein.

The selected bidder shall be responsible for providing the External Attack Surface Management (EASM), Digital Risk Monitoring (DRM), Incident Response (IR) Services, including all necessary hardware and its accessories, software, premium licenses, implementation services, integration, training, technical support, and maintenance services during the contract period, as detailed in this RFP document.

This RFP is neither an offer nor an agreement and is issued solely for inviting competitive bids from interested and eligible bidders. The selection of the successful bidder shall be carried out through the process specified in this RFP, on behalf of GSOC/DIT/DST, GoG.

GIL/DIT/DST reserves the right to amend, modify, supplement, or cancel this RFP, or to extend the bid submission deadline at any stage of the bidding process without assigning any reason. In such an event, all rights and obligations of GIL/DIT/DST and the bidders shall thereafter be subject to the revised terms and timelines as notified by GIL/DIT/DST.

5. INSTRUCTIONS TO THE BIDDERS REGARDING RFP:

A proposal in the form of a BID is requested for the item(s) in complete accordance with the documents/attachments as per the following guidelines:

1. The bidder shall upload their bids on GeM - <https://gem.gov.in>.
2. Bids complete in all respects should be uploaded on or before the bid due date.
3. Products & Services offered should be strictly as per requirements mentioned in this Bid document.
4. Once quoted, the bidder is not allowed to make any price changes, whether resulting or arising out of any technical/commercial clarifications sought regarding the bid. Such price changes shall render the bid liable for rejection.
5. No Consortium will be allowed. The Bidder must submit the bid and execute the contract as a single legal entity. Bids submitted by a consortium of companies, joint ventures, or partnerships will not be considered and will be deemed nonresponsive. The Bidder will be solely responsible for the execution of the contract and the delivery of all deliverables specified. Any attempt to subcontract or form a consortium will result in the immediate disqualification of the bid or termination of the contract.
6. Bidders shall submit EMD (Rs. 9,00,000/-) in the form of Demand Draft OR in the form of an unconditional Bank Guarantee (which should be valid for 12 months from the last date of bid submission) of any Nationalized Bank including the public sector bank or Private Sector Banks or Commercial Banks or Co-Operative Banks and Rural Banks (operating in India having branch at Ahmedabad/Gandhinagar) as per the G.R. no. FD/MSM/e-file/4/2025/2712/DMO dated 01.04.2026 issued by the Finance Department or further instructions issued by the Finance Department from time to time; in the name of "Director, Directorate of ICT and e-Governance" payable at Gandhinagar (as per prescribed format given) and must be submitted along with the covering letter in a sealed cover at GIL. The sealed cover should be superscribed as "EMD for the Request for Proposal for Supply, Installation, Testing and Commissioning (SITC) of Enterprise Backup Solution with Comprehensive Onsite Warranty Support for Gujarat Security Operations Centre (GSOC), Gandhinagar."

OR

Bidders can also submit the EMD with Payment Online through RTGS/Internet Banking in the beneficiary's name Gujarat Informatics Ltd., Account No. 50200010918090, IFSC Code HDFC0000190, Bank Name HDFC Bank Ltd., Sector-16, Gandhinagar Branch.

7. For interpretation of any clause in the RFP or Contract Agreement, the interpretation of the Purchaser shall be final and binding on the agency.
8. If the Bidder fails to complete the due performance of the contract in accordance with the specifications and conditions of the offer document, the Purchaser reserves the right either to cancel the order or to recover a suitable amount as deemed reasonable as Penalty/Liquidated damage for non-performance.
9. GIL/DIT/DST reserves the right to accept or reject any tender offer without giving any reason.
10. Financial bids of only those bidders who qualify based on evaluation of eligibility & technical bids will be opened.
11. The Successful bidder will have to submit Performance Bank Guarantee of an amount equal to 10% of the total order value (including 2 years' comprehensive warranty and OEM Support) within 15 calendar days (including holidays) from the issuance of the Work Order/Contract, for the duration of the contract period + 6 months from banks (operating in India having a branch at Ahmedabad/Gandhinagar) as per the G.R. no. FD/MSM/e-file/4/2024/2859/D.M.O. dated 01.05.2025 issued by the Finance Department or further instructions issued by the Finance Department from time to time.
12. GIL/DIT/DST/GoG is not liable for any cost incurred by a Bidder in the preparation and production of any Proposal, the preparation or execution of any benchmark demonstrations, simulation or laboratory service or for any work performed before the execution of a formal contract. All materials submitted become the property of the DIT/GIL & may be returned at its sole discretion. The content

of each Bidder's Proposal will be held in strict confidence during the evaluation process, and details of any Proposals will not be discussed outside the evaluation process.

13. The Bid will be valid for a period of 180 days from the last date of bid submission.

14. Important Information:

1	GeM Bid Number	GEM/2026/B/7942125 dated:- 14/10/2026
2	Contract Period	2 (two) years
3	Date & Time of Pre-Bid Meeting	As per GeM bid
4	Venue of Pre-Bid Meeting	Gujarat Informatics Limited Conference Room, Gujarat Informatics Ltd, Block No. 2, 2 nd Floor, Karmayogi Bhavan, Sector-10A, Gandhinagar 382 010
5	Last Date & Time for submission of written pre-bid queries for clarification (Only by e-mail as per predefined format)	Up to the date preceding the pre-bid meeting date E-mail: gm-sp-gil@gujarat.gov.in ; ; manager-egov@gujarat.gov.in ; exe1-egov-gil@gujarat.gov.in ; tse1-egov-gil@gujarat.gov.in
6	Last Date & Time for Submission of Bids electronically on https://gem.gov.in	As per GeM portal
7	Last Date and time for submission of EMD in person/physically along with original Affidavit of Self Declaration	Within 7 days from the last Date of bid submission.
8	Date & Time of Opening of Bids (Un-priced Bids)	As per GeM portal
9	Date & Time of Opening of Commercial Stage	Will be intimated to the qualified bidders at a later date.
10	Earnest Money Deposit (E.M.D.)	Rs. 9,00,000/- (Nine lacs only) in the name of Gujarat Informatics Limited payable at Gandhinagar (in case of DD) For RTGS; Beneficiary name: Gujarat Informatics Limited, Account No:50200010918090 IFSC Code: HDFC0000190 Bank Name: HDFC Bank Branch address: Sector 16 Gandhinagar
11	GIL Contact Person	GM (Software Procurement) Gujarat Informatics Ltd, Email ID: gm-sp-gil@gujarat.gov.in
12	Validity of Tender	180 days

6. GENERAL TERMS AND CONDITIONS:

1. Instructions to the Bidders for Online Bid Submission:
 - 1) Tender documents are available only in electronic format, which Bidders can download free of cost from the website <https://gil.gujarat.gov.in> and <https://gem.gov.in>.
 - 2) The bids have been invited through GeM portal, i.e., the eligibility criteria, technical and financial stages shall be submitted online on the GeM portal <https://gem.gov.in>.
 - 3) Interested and eligible Bidders are required to upload the eligibility-related document in the eligibility bid section, Technical-related document in the Technical bid section & Commercial Bid in the Commercial bid section. The Technical & Commercial Bid must be uploaded to <https://gem.gov.in>.
2. In the technical bid section of GeM, the bidder is required to upload the following documents.
 - 1) OEM MAF, Brochure, and OEM Compliance on the Offered product (with remarks of Yes/no only) on both OEM and Bidder Letterhead. Any partial remarks are not allowed.
 - 2) Compliance of the SOW, SLA, and Payment terms, etc., to be uploaded as part of the GeM Bid on bidder's letterhead.
 - 3) Supporting documents for the Eligibility & Technical Criteria as specified in the RFP.
 - 4) Undertaking as per guidelines published by the Ministry of Finance, Dept. of Expenditure, Public Procurement Division dated 23.07.2020 in the given format by Bidder as well as OEM.
 - 5) Other documents asked in the RFP.

7. ELIGIBILITY CRITERIA

Sr. No	Eligibility Criteria	Attachments
1.	The bidder should be a Registered Company (registered under the Indian Companies Act, 1956 or Indian Companies Act, 2013)/LLP Act,2008 in India. The bidder should have been in operation for at least five financial years. AND Bidder should be an established IT/Cybersecurity System Integrator or Cybersecurity Service Provider and should have been engaged in similar IT projects/solutions business for a period of at least five years as on the bid issuance date.	Copy of valid Certificate of Incorporation, PAN and GST registration Certificate. AND Work Orders / Client Certificates confirming year and area of activity should be enclosed.
2.	The Bidder shall have a minimum Average Annual Turnover of ₹6 Crore during the last three (03) financial years, i.e. FY 2023-24, FY 2024-25 and FY 2025-26.	Audited and Certified Balance Sheet & Profit/Loss Account of last 3 Financial Years. CA certificate clearly certifying the turnover requirements as per the clause along with UDIN NUMBER.
3.	The OEM of the proposed product should have an Average Turnover of Rs. 15 Crore (Minimum) in the last three financial years (i.e., 2023-24, 2024-25 and 2025-26) as on the last date of bid submission. for each proposed EASM/DRM/Managed SOC OEMs	Audited and Certified Balance Sheet & Profit/Loss Account of last 3 Financial Years. CA certificate clearly certifying the turnover requirements as per the clause along with UDIN NUMBER.
4.	The Bidder shall have been engaged in providing Cybersecurity Services for at least five (05) years as on the date of bid submission. Further, during the last five (05) years, the Bidder shall have successfully executed/completed contracts for any Central/State Government Organization, PSU or Public Listed Company meeting at least one of the following criteria: (i) one order of minimum value ₹3 Crore; or (ii) two orders, each of minimum value ₹2 Crore; or (iii) three orders, each of minimum value ₹1.5 Crore. In addition, for Similar Services, the Bidder shall have successfully executed at least three (03) similar projects during the last five (05) years wherein EASM and DRM were substantive components of the scope, along with Cyber Security, SOC, MSS, Threat Intelligence and/or Digital Risk Protection services, as applicable. All qualifying Work Orders/Contracts shall be in the name of the Bidder.	The bidder shall submit Purchase Order/ Work Order and Project completion Certificate or Client Certificate or Ongoing Contract with satisfactory performance certificate or CA certificate clearly specifies details like project value, tenure and scope of work, project status.
5.	OEM for each External Attack Surface Management (EASM) services and Digital Risk Monitoring Services (DRM), Managed SOC should have provided service(s) either as a standalone service or as part of an integrated cybersecurity project having a value of minimum Rs. 5 Crore in the last three financial years in any Central / State Government Organization / PSU/ Public Listed Company as on last date of bid	The bidder shall submit Purchase Order/ Work Order and Project completion Certificate or Client Certificate or Ongoing Contract with satisfactory performance certificate or CA certificate clearly specifies details like project value, tenure and scope of work, project status.

	submission. The qualifying project may have been executed directly by the OEM or through its authorized partner.	
6.	OEM/IR Service Provider have Incident Response (IR) Services should have provided service(s) having a value of minimum Rs. 1 Crore in the last three financial years in any Central / State Government Organization / PSU/ Public Listed Company as on last date of bid submission.	submit Purchase Order/ Work Order and Project completion Certificate or Client Certificate or Ongoing Contract with satisfactory performance certificate or CA certificate clearly specifies details like project value, tenure and scope of work, project status certifying the requirements as per the clause
7.	The bidder must be an authorized partner of the OEM. In cases where the proposed Services comprises EASM and DRM from two distinct OEMs, the bidder must submit a Joint Manufacturer Authorization Form (Joint MAF) signed by authorized signatories of both OEMs. The Bidder shall submit a separate OEM Authorization/Service Support Letter from the proposed OEM/IR Service Provider, authorizing the Bidder to provide the proposed Incident Response (IR) services and confirming OEM technical support and assistance for the solution throughout the contract period.	The Bidder should submit the tender-specific MAF from OEM(s).
8.	Bidder and OEM should not be blacklisted by any Ministry of the Government of India or by any State Government of India or any of the Government PSUs at the time of bidding.	Self-Declaration / Certificate / Affidavit mentioning that the Bidder and OEM are not blacklisted as per the clause.
9.	No Consortium or Subletting will be allowed.	Bidder's Self Declaration.
10.	The Bidder should have at least one office in Gujarat. If the Bidder does not have any office in Gujarat, then the Bidder should submit a letter of undertaking to open the office in Gujarat within 45 calendar days (including holidays) from the date of award.	The copy of Registration of Incorporation/ Lease agreement/ Property Tax Bill/ Electricity Bill/ Telephone Bill/ GST/ CST should be submitted, or an Undertaking Letter should be submitted.

Note:

- Bidder must match the eligibility criteria, experience, bidder’s turnover criteria, etc. as mentioned in the RFP document and time to time published corrigendum, and will be considered for evaluation.
- All the details and the supportive documents for the above-mentioned items should be uploaded in the bid.
- EMD and PBG should be submitted by the bidder as mentioned in the RFP.
- The Bidder must attach valid documents in support to their Technical and Financial capabilities/strength, as mentioned above. Without proper supporting documents, the Bid proposals are liable to be rejected.
- SLA, NDA & Legal Costs The successful bidder shall bear all legal charges including stamp duty and documentation fees associated with SLA and NDA execution.
- No Consortium is allowed in this bid.

8. PRE-BID MEETING

- 1. The Pre-bid meeting will be held at the GIL Office.
- 2. A prospective Bidder requiring any clarification of the bidding documents may seek clarifications by submitting their queries to the email ID: If you have any query, then please send us by email on gm-sp-gil@gujarat.gov.in ; manager-egov@gujarat.gov.in; exe1-egov-gil@gujarat.gov.in; tse1-egov-gil@gujarat.gov.in prior to the date of the Pre-Bid Meeting. No bid queries would be entertained post completion of the Pre-Bid Meeting.
- 3. The interested vendors submitted their queries in writing at least 3 days before the date of pre-bid meeting date.
- 4. The interested bidder should send the queries as per the following format:

Bidder’s Request for Clarification			
Name of Organization submitting the request		Name & position of the person submitting the request	Address of the Organization including phone, email & contact person details
Sr. No.	Bidding Document Reference (Clause/Page)	The content of the RFP requiring	Points of Clarification Required
1			
2			
.			

- 5. Tenderer will discuss the queries received from the interested bidders/vendors in the Pre-Bid Meeting and respond to the clarifications by publishing/uploading on the website <https://gil.gujarat.gov.in> and <https://gem.gov.in>.
- 6. No further or new clarification whatsoever shall be entertained after the Pre-Bid Meeting.

9. SCOPE OF WORK

Scope of work For EASM & DRM Managed Services

9.1 Overview

The Directorate of ICT & e-Governance, Government of Gujarat, intends to procure a comprehensive **External Attack Surface Management (EASM), Digital Risk Monitoring (DRM), Incident Response Services** on a fully managed subscription basis. These services cover continuous identification, monitoring, analysis, prioritization and mitigation of cyber risks associated with Government-owned Internet-facing infrastructure, digital assets, brand identity and sensitive information exposed across the Internet, Deep Web and Dark Web.

The selected bidder shall provide the OEM-managed service, implementation, onboarding, continuous monitoring, threat intelligence, incident investigation assistance, takedown coordination, reporting, technical support, and knowledge transfer throughout the contract period.

The Platform shall operate on a fully managed service model with continuous monitoring and proactive notification of cyber risks.

9.2 Scope of Services

The scope shall broadly include:

- External Attack Surface Management (EASM)
- Digital Risk Monitoring (DRM)
- Digital Brand Protection
- Domain Protection
- Credential Exposure Monitoring
- Data Leak Monitoring
- Threat Intelligence
- Deep & Dark Web Monitoring
- Phishing Detection & Takedown
- Brand Abuse Monitoring
- Executive Monitoring
- Continuous Reporting
- Dashboard & Analytics
- API Integration

The bidder shall provide all services necessary to achieve the objectives of this RFP, whether specifically mentioned or reasonably implied. Any service required for successful implementation shall be considered within scope without additional commercial implication.

9.3 External Attack Surface Management (EASM)

The proposed EASM Service shall automatically discover Government-owned Internet-facing assets without requiring manual asset inventory and shall continuously monitor, analyze, prioritize and report cyber risks throughout the contract period.

The Managed Service shall include, but not be limited to, the following capabilities.

9.3.1 Asset Discovery

Automatically discover and maintain inventory of:

- Public IP Addresses
- Domains
- Sub-domains
- Wildcard Domains

- DNS Records
- Websites
- Web Applications
- APIs
- Cloud Assets (AWS, Azure, GCP)
- Virtual Machines
- Load Balancers
- Internet Gateways
- CDN Assets
- SSL/TLS Certificates
- Internet-facing Servers
- Email Infrastructure
- VPN Gateways
- Remote Access Portals
- Third-party exposed assets
- Shadow IT Assets
- Orphaned Assets
- Unknown Internet-facing Assets

The Managed Service shall automatically identify asset ownership relationships and continuously update the inventory.

9.3.2 Continuous Exposure Monitoring

The Managed Service shall continuously monitor:

- Newly discovered assets
- Newly exposed services
- Asset ownership changes
- DNS changes
- SSL certificate changes
- Cloud exposure
- Public exposure
- Technology stack changes
- Internet footprint changes
- Newly registered Government-related domains

9.3.3 Security Exposure Assessment

The Managed Service shall identify:

- Internet exposed services
- Open Ports
- RDP Exposure
- SSH Exposure
- VPN Exposure
- Database Exposure
- Web Server Exposure
- Mail Server Exposure
- Management Interfaces
- Remote Administration Portals
- Default Configurations
- Publicly Accessible Storage
- Directory Listing
- Weak SSL/TLS Configuration
- Missing Security Headers
- End-of-Life Technologies
- End-of-Support Software/Components
- Misconfigured Cloud Resources

- Misconfigured Web Applications

9.3.4 Vulnerability Intelligence

The Managed Service shall identify externally observable vulnerabilities including:

- Known CVEs
- Critical Vulnerabilities
- High Risk Vulnerabilities
- Publicly Exploitable Vulnerabilities
- Exploit Availability
- Exploit Prediction
- Attack Path Analysis
- Vulnerability Prioritization
- Business Risk Context

9.3.5 Asset Risk Scoring/Rating/Severity

Provide:

- Asset Criticality
- Business Context
- Internet Exposure Score
- Security Risk Score
- Exploitability Score
- Threat Score
- Prioritized Remediation Guidance

9.3.6 SSL & Certificate Monitoring

Monitor:

- Certificate Expiry
- Weak Encryption
- Unauthorized Certificates
- Certificate Transparency Logs
- Certificate Changes
- Self-Signed Certificates

9.3.7 Attack Surface Reporting

Generate dashboards showing:

- Total Internet-facing Assets
- Unknown Assets
- Shadow IT
- High Risk Assets
- Misconfigured Assets
- Internet Exposure Trend
- Vulnerability Trend
- Department-wise Inventory
- Executive Dashboard

9.4 Digital Risk Monitoring (DRM)

The bidder shall provide continuous Digital Risk Monitoring services for Government-owned digital assets, brand identity and sensitive information across Surface Web, Deep Web and Dark Web.

9.4.1 Credential Exposure Monitoring

Continuously monitor for exposure of:

- Employee Credentials
- Administrative Credentials
- Server Credentials
- Domain Credentials
- Service Account Credentials
- API Keys
- VPN Credentials
- Cloud Credentials
- VIP User Credentials

Provide:

- Leak Source
- First Seen
- Risk Level
- Associated Asset
- Recommended Remediation

9.4.2 Source Code & Repository Monitoring

Continuously monitor public repositories for exposure of:

- Source Code
- Configuration Files
- Secrets
- API Keys
- Tokens
- SSH Keys
- Certificates
- Hardcoded Passwords
- Cloud Credentials

9.4.3 Data Leak Monitoring

Monitor for unauthorized exposure of:

- Government Data
- Citizen Information
- Confidential Documents
- Intellectual Property
- Internal Reports
- Database Dumps
- Sensitive Files
- Third-party Data Exposure

9.4.4 Business Email Compromise (BEC)

Identify:

- Executive Impersonation
- Email Spoofing
- Domain Spoofing
- Look-alike Domains
- Credential Harvesting Campaigns
- Email Fraud

9.4.5 Deep & Dark Web Monitoring

Continuously monitor:

- Dark Web Forums
- Underground Communities
- Marketplaces
- Paste Sites
- Telegram Channels
- IRC Conversations
- Threat Actor Discussions
- Initial Access Brokers

Detect:

- Government Data
- Credentials
- Database Leaks
- Malware Campaigns
- Sale of Access
- Threat Actor Discussions

9.5 Digital Brand Protection

The Managed Service shall continuously monitor unauthorized usage of Government identity.

Capabilities shall include:

- Brand Protection
- Logo Misuse Detection
- Department Name Misuse
- Campaign Name Misuse
- Government Seal Misuse
- Website Impersonation

9.5.1 Fraud & Phishing Protection

Detect:

- Fake Government Websites
- Phishing Sites
- Credential Harvesting Pages
- Fake Login Pages
- Fake Customer Care Numbers
- Scam Portals
- QR Code Scams
- Payment Fraud Websites

9.5.2 Domain Monitoring

Continuously monitor:

- Look-alike Domains
- Typo squatting
- Homograph Domains
- Domain Abuse
- DNS Abuse
- Newly Registered Suspicious Domains

Provide registrar-level takedown coordination.

9.5.3 Rogue Mobile Application Monitoring

Monitor:

- Google Play
- Apple App Store
- Third-party App Stores
- APK Distribution Sites

Identify:

- Fake Applications
- Malicious Applications
- Brand Abuse Applications

Provide takedown assistance.

9.6 Takedown Services

The bidder shall coordinate with domain registrars, hosting providers, search engines, app stores and social media Managed Services for takedown of:

- Phishing Websites
- Fake Domains
- Rogue Mobile Applications
- Fake Social Media Accounts
- Brand Abuse Content
- Fraudulent Websites
- Copyright or Trademark Misuse

As part of service, Evidence preservation is required.

9.7 Alerts & Reporting

The Managed Service shall provide:

- Near Real-time Alerts
- Email Notifications
- API Integration
- Webhooks
- SIEM Integration
- Executive Dashboards
- Monthly Reports
- Quarterly Risk Trends
- Asset Inventory Reports
- Digital Risk Reports
- Threat Intelligence Reports
- Takedown Status Reports

The selected bidder shall:

- Continuously monitor the environment on a 24×7×365 basis.
- Baseline deviation detection from secure-state baseline.
- Validate findings to minimize false positives.
- Notify GSOC immediately for Critical and High severity observations.
- Assist in investigation and remediation.
- Provide monthly review meetings and quarterly executive presentations.
- Provide OEM-backed technical support throughout the contract period.
- Deliver administrator training, documentation and knowledge transfer.

Scope of work for Incident Response Retainer (IRR) Services

The Service Provider shall provide proactive and on-demand, threat-informed incident response retainer services within defined timelines to address alerts, mitigate security risks, and support SOC in effective incident handling of GOG assets.

This includes, but is not limited to:

- On-demand activation of IR services in line with SLA timelines.
- Deployment of expert-level cyber security professionals to validate and respond to incidents.
- Real-time monitoring and corrective actions for threats such as malicious network indicators, command-and-control traffic, and data exfiltration attempts.
- Malware analysis to determine the nature, origin, and scope of intrusion or infection.
- Log review and analysis from diverse sources (network, system, devices, applications).
- Threat briefing and advisory to senior stakeholders/officials of GoG.
- Collaboration with GoG stakeholders and, if required, external agencies including law enforcement, PR, and statutory authorities.
- Ensuring auditability and electronic record-keeping of all evidence and forensic steps performed.
- Maintaining strict chain-of-custody for all digital evidence.
- Support in restoring IT systems, applications, and services back to normal operational state.
- Recommendations for system hardening, policy changes, and backup/recovery improvements.
- Scalable investigation capabilities across multiple technologies, systems, and geographic locations.
- Archival of forensic data/logs as per contract period requirements for audit or compliance purposes.
- Execution of SLA and NDA before onboarding.
- Phased Delivery of IRR Services

Incident Response Readiness Assessment (IRRA)

Phase 1. Incident Response Readiness Assessment

This phase aims to improve GoG's CII posture, incident response plans, procedures, and readiness. The Vendor shall:

- Review and assess existing Cyber Crisis Management Plan, SOPs, and departmental IR plans.
- Identify gaps in readiness through workshops, assessments, and simulations with stakeholders across GoG.
- Evaluate current technologies, logging sources, and monitoring practices.
- Conduct tabletop exercises and readiness drills covering scenarios such as ransomware, phishing, insider threats, data breaches, and APT attacks etc. Tabletop exercise is to be conducted for DST Technical staff and Officers and conducted biannually.
- Provide recommendations for enhancing log sources, detection capabilities, and backup/recovery readiness.
- Develop/Update IR Playbooks and Runbooks aligned with MITRE ATT&CK framework and GoG environment.
- Assist in defining team structures, roles, and escalation procedures.
- Establish secure infrastructure for IR analysis, including agents/sensors/ scripts, to collect and analyze forensic evidence.
- Deliver IRRA Report and IRRA Guide with recommended improvements.

Phase 2. Incident Identification

- Collect and analyze data from SIEM, IDS/IPS, logs, and threat intelligence feeds to identify potential incidents.
- Provide 24x7x365 dedicated hotline/email response facility for GoG.
- Ensure incident triage within SLA timelines upon receipt of alerts.
- Begin preliminary analysis based on provided information and escalate for containment.

Phase 3. Containment

- Isolate compromised systems, networks, or applications to prevent lateral movement or data loss.
- Implement temporary workarounds while ensuring continuity of essential services.
- Support SOC in immediate mitigation actions against threat actors.

Phase 4. Analysis

- Perform forensic and malware analysis to identify root cause, attacker TTPs, and IOCs.
- Correlate logs across multiple sources (network, endpoint, applications, cloud, VPN, etc.).
- Ensure export of logs in standard formats for compliance.
- Provide evidence-based recommendations to remediate exploited vulnerabilities.

Phase 5. Eradication

- Assist in removal of malicious artifacts (malware, backdoors, rogue accounts).
- Guide patching, configuration changes, and vulnerability closure.
- Ensure eradication is done without unnecessary disruption to business operations.

Phase 6. Recovery & Monitoring

- Support system restoration to pre-incident state.
- Monitor affected systems/networks post-recovery to ensure no reinfection or persistence.
- Recommend security hardening measures and update IR readiness based on learnings.

Phase 7. Reporting & Lessons Learned

- Provide comprehensive Incident Response Reports including root cause analysis, IOCs, evidence, and corrective recommendations.
- Assist GoG in notifications to statutory bodies, CERT-In, and law enforcement agencies as required.
- Conduct post-incident review workshops to identify strengths and gaps in IR process.
- Provide strategic recommendations to improve GoG cyber resilience and SOC capability.

The minimum phase-wise requirements mentioned above are based on our current understanding of the scope and operational needs. However, the bidder may propose additional activities, or methodologies aligned with industry best practices to further strengthen the overall Incident Response capability.

All required tools, hardware, software, licenses etc. to be bring by bidder.

Deliverables

The Vendor shall provide the following deliverables:

- Incident activation acknowledgement reports.
- Periodic (daily/weekly) status reports during incidents.
- Forensic analysis reports, evidence inventories, and chain-of-custody records.
- Executive summary reports for senior decision-makers.
- Quarterly IR readiness health-check reports.
- Annual IR Maturity Assessment and updated Playbooks.

10. IMPLEMENTATION TIMELINES & PENALTIES:

The Successful Bidder will have to complete the Supply, Installation, Configuration, Commissioning, and Integration with Acceptance of the ordered work within the time period(s) specified in the table below. However, in case of any delay solely on the part of the successful bidder, DST/DIT/GIL reserves the right to levy the appropriate penalties as per the table below:

Incident Response Service

Activity	Timeline from PO Date
Signing of SLA & NDA	Within 30 days
Completion of onboarding staff & technical training	Within 45 days
Phase-1 Incident Response Readiness Assessment (IRRA)	Within 60 days
Activation of Incident Response Services	As per SLA timelines defined in Section – IR Response Timeline

External Attack Surface Management (EASM), Digital Risk Monitoring (DRM)

Sr. No.	Work Type	Time Limit for Execution	Penalty for Delay	Penalty
1	Submission of PBG	Within 15 calendar days (including holidays) from the date of issuance of Work Order/ Contract	If the successful bidder fails to submit the PBG as specified, the EMD will be forfeited, and the contract will be terminated beyond 15 (including holidays) days without any further communication.	-
2	Kick-off meeting	1 week from issuance of work order/contract	Rs. 50,000/week or part thereof. In case of delay beyond 4 weeks, DST/DIT/GIL may terminate the contract and forfeit the PBG.	-
3	Integration & deployment	T1 = T + 45 days from the date of issuance of work order	0.5% of order value of delayed/pending work per week or part thereof proportionately	10% of total contract value
4	Go live and Training	T2 = T1 + 15	0.5% of order value of delayed/pending work per week or part thereof proportionately	

Note:

- T= Date of issuance of work order/contract.
- Days will be considered as calendar days including holidays.
- Aforesaid penalty cap will not be applicable for any severe impact/incident/outage at GSOC, resulting in loss to Government of Gujarat.

11. SERVICE LEVEL AGREEMENT (SLA) & PENALTIES:

The Successful Bidder will have to ensure adherence to SLA and time schedules given in this RFP.
Service Level Agreement (SLA) – External Attack Surface Management (EASM), Digital Risk Monitoring (DRM)

The successful bidder shall comply with the following Service Levels throughout the contract period. SLA shall be measured on a **monthly basis**, and applicable penalties shall be deducted from the subsequent quarterly payment. The overall SLA penalty for quarter shall be capped at **10% of the Quarterly Invoice**.

Platform/Service Availability for EASM, DRM

SLA Parameter	Target	Penalty
EASM & DRM Platform/ Services Availability or any part of the services	Minimum 99.90% monthly uptime (24x7x365)	1% of the quarterly payment of Managed EASM & DRM Services for each 0.10 percentage point below 99.90%, subject to the overall quarterly SLA penalty cap of 10% of the Quarterly Invoice

Planned maintenance, where notified and approved in advance by the Tenderer, shall not be treated as service downtime.

Failure to achieve the availability SLA for **three consecutive months** may result in a formal performance review and may lead to termination in accordance with the termination provisions of the contract.

The successful vendor should adhere to the following timelines:

Sr.	Service Activity	Description	Timeline *
1	Digital Risk Monitoring	Evidence of Takedown Request Initiation	Within 3 hours
2		Phishing Website / Rogue Application – Takedown	Within 24 hours
3		Phishing Website blocking in major web browsers and/or search engines, in case takedown is not feasible	Within 48 hours
4		Brand Abuse on social media - Takedown	Within 72 hours
5		Reporting of threats as and when observed on Deep web / Dark web.	Within 6 hours
6	External Attack Surface Management	External attack surface scanning and reporting	Within 7 days
7			

***Subject to timely response from Domain Registrars, Hosting Providers, App Stores, Search Engines, Social Media Platforms, CERT-In, Government of India, Government of Gujarat or other external agencies. The bidder shall initiate the takedown request within 3 hours of validation. bidder must provide evidence of takedown initiation within 4 hours.**

Note: Time line may vary as per CERT-In, Government of India, Government of Gujarat or other external agencies mandate and guideline.

The calculations for delay in achieving defined timeline / SLA would be done on monthly average basis. In case of delays in completion of activities beyond the defined timeline / SLA, the SP will have to justify such delays to the Tenderer. In case tenderer is not satisfied with justification given by the SP, Tenderer will have the discretion to impose penalty equivalent to 2% of the monthly subscription cost (of EASM/DRM service, as applicable) for delay in each activity per month.

Penalty: Any failure to achieve the specified Service Level Agreement (SLA) shall attract a penalty of **1% of the Monthly Subscription Cost** for each instance of non-compliance, subject to a maximum cumulative penalty of **10% of the Quarterly Invoice**.

Incident Response Retainership Timelines (SLA)

Initial Response SLA	Time limit
24*7*365 days dedicated global and domestic support facility for incident response and onsite resource	
Initial Acknowledgement	<=30 minutes
Initial Response/Scoping of incident response once alerted from tenderer through Call/Email/Hotline/Other communication media for any location.	<=4 hrs
Upon confirmed Incident, the IR analyst should immediately start working on preliminary information submitted by the tenderer Incident Response-Remote support	<=6 Hrs
Onsite Location - If required, the IR analyst shall be deployed onsite at the location where the incident occurs	
Within India-Tier1 Cities, metropolitan city, State capitals	<=12 hrs
Within India-Cities apart from above	<=24 hrs
Interim update report	Every 12 hours
Final complete IR Report	<=10 days post-containment

Incident Response & Resolution

Severity Level	Example	Response Time	Resolution Time	Onsite
Critical (P1)	Data breach / ransomware, Platform outage, critical data exposure	≤ 30 minutes	≤ 24 hours	<=12 Hours
High (P2)	Malware outbreak, Major functional degradation	≤ 1 hour	≤ 24 hours	<=12 Hours
Medium (P3)	Suspicious activity, Partial issue, minor alert delays	≤ 4 hours	≤ 24 hours	NA
Low (P4)	Advisory, Cosmetic issues, non-urgent queries	≤ 1 business day	≤ 3 business days	NA

Response time = Time from issue reporting to acknowledgment.

Resolution time = Time to provide a permanent fix or acceptable workaround.

Penalty for SLA & Non-Compliance

Metric	Penalty
Delay in onsite deployment	0.1% of total annual cost of IR service per day delay, max 15%
Delay in final IR report	0.5% of total annual cost of IR service per day, max 10%

Other terms for Incident Response Contract, Project Schedule & Payment Conditions

Start Date & Contract Duration Start Date (T): Effective from the date of issuance of Purchase Order (PO) or date of execution of Service Level Agreement (SLA) and Non-Disclosure Agreement (NDA), whichever is later.

Helpdesk & Support Requirements The selected service provider shall establish and operate a dedicated 24x7x365 hotline and remote support facility for Incident Response services. The bidder is required to:

- a. Provide a fully functional global and domestic emergency response hotline for incident reporting and escalation.
- b. Ensure trained onsite technical experts at least L3 level capable of addressing IR-related issues raised by SOC / Government of Gujarat users.
- c. Deliver investigation support for cyber threats including surface web / deep web / dark web intelligence, and submit detailed reports within mutually agreed timelines.
- d. Provide customized IR reporting formats, dashboards, summaries and analytics in standard formats and as requested by SOC DIT/DST.

Incident Response Activation the IR team must commence incident response activities within the SLA timelines defined in the Incident Response Timelines Section of this RFP upon receipt of notification via phone, email, hotline or official communication from SOC/DIT/DST.

Training The bidder shall conduct onboarding workshops, IR operational training and simulations / tabletop exercises for SOC stakeholders and issue certification to participants as part of project scope.

Applicability of Rates Across GoG Agencies The same awarded commercial rates shall be made available to all Government of Gujarat Departments, Boards, Corporations and Field Offices as and when requested, during the contract period, on the same pricing terms and man-hour model.

Confidentiality, Integrity & Comprehensive Security Review The bidder shall ensure: All deployed tools, software, agents, log collectors and analytical systems are verified and secure. Strict confidentiality of data, logs, evidence and information obtained during IR engagements. Compliance with security validation and review processes mandated by SOC/DIT/DST, which at minimum include:

- Secure configuration testing
- Internal Vulnerability Assessment (VA)
- Internal Penetration Testing (PT)
- External Penetration Testing
- Application Security Assessment
- Infrastructure & Physical Security Review
- Closure of vulnerabilities and confirmatory testing

12.COMPLIANCE MATRIX & ELIGIBILITY REQUIREMENTS:

External Attack Surface Management (EASM) and Digital Risk Monitoring (DRM) - Technical Compliance Matrix

(M = Mandatory, G = Good to Have)

A. External Attack Surface Management (EASM)

Sr	Technical Requirement	Category	OEM Response / Remarks
1	Managed Service shall automatically discover all Internet-facing assets without manual input.	M	
2	Automatic discovery of unknown/shadow IT assets.	M	
3	Discovery of domains, sub-domains and wildcard domains.	M	
4	Discovery of public IPv4/IPv6 assets.	M	
5	Discovery of cloud assets across AWS, Azure and Google Cloud.	M	
6	Continuous asset discovery and inventory updates.	M	
7	Automatic asset ownership correlation.	M	
8	Technology fingerprinting of Internet-facing assets.	M	
9	Asset criticality classification.	M	
10	Business context mapping of assets.	G	
11	Asset relationship visualization.	G	
12	Attack path visualization.	G	
13	Historical asset exposure timeline.	G	
14	Third-party asset visibility.	G	
15	API discovery.	G	

B. Exposure & Vulnerability Detection

Sr.	Requirement	Category	OEM Response / Remarks
16	Open Port Detection.	M	
17	Internet exposed service detection.	M	
18	RDP Exposure Detection.	M	
19	SSH Exposure Detection.	M	
20	VPN Exposure Detection.	M	
21	Database Exposure Detection.	M	
22	SSL/TLS Security Assessment.	M	
23	Certificate Expiry Monitoring.	M	
24	Weak Cipher Detection.	M	
25	Misconfigured Web Application Detection.	M	
26	Cloud Misconfiguration Detection.	M	
27	Public Storage Bucket Detection.	M	
28	Missing Security Header Detection.	G	
29	Directory Listing Detection.	G	
30	Default Credentials Detection.	G	
31	Exposed Administrative Interface Detection.	M	
32	EOL/EOS Software Detection.	M	
33	Known CVE Detection.	M	
34	Exploit Availability Intelligence.	G	
35	Risk-based Vulnerability Prioritization.	M	

C. Digital Risk Monitoring

Sr.	Requirement	Category	OEM Response / Remarks
36	Employee Credential Leak Monitoring.	M	
37	Server Credential Leak Monitoring.	M	
38	Administrator Credential Monitoring.	M	
39	VIP/Executive Credential Monitoring.	M	
40	Business Email Compromise Monitoring.	M	
41	Third-party Data Leak Monitoring.	M	
42	Source Code Leak Detection.	M	
43	Git Repository Monitoring.	M	
44	API Key Exposure Detection.	M	
45	Cloud Secret Monitoring.	G	
46	SSH Key Exposure Detection.	G	
47	Certificate Leak Monitoring.	G	
48	Configuration File Leak Detection.	G	
49	Sensitive Document Leak Detection.	M	
50	Database Leak Monitoring.	M	

D. Deep & Dark Web Monitoring

Sr.	Requirement	Category	OEM Response / Remarks
51	Deep Web Monitoring.	M	
52	Dark Web Monitoring.	M	
53	Marketplace Monitoring.	M	
54	Forum Monitoring.	M	
55	Paste Site Monitoring.	M	
56	Telegram Monitoring.	M	
57	IRC Monitoring.	G	
58	Threat Actor Monitoring.	G	
59	Malware Discussion Monitoring.	G	
60	Threat Campaign Tracking.	G	
61	Credential Sale Monitoring.	M	
62	Government Data Sale Monitoring.	M	

E. Brand Protection

Sr.	Requirement	Category	OEM Response / Remarks
63	Fake Domain Detection.	M	
64	Typosquatting Detection.	M	
65	Homograph Domain Detection.	M	
66	Brand Impersonation Detection.	M	
67	Trademark Monitoring.	G	
68	Logo Misuse Detection.	G	
69	Fake Government Website Detection.	M	
70	Phishing Website Detection.	M	
71	Fraud Website Detection.	M	
72	Fake Customer Care Number Detection.	M	
73	Rogue Mobile Application Detection.	M	
74	Fake Social Media Account Detection.	M	
75	Brand Abuse Detection on Marketplaces.	G	

F. Threat Intelligence

Sr.	Requirement	Category	OEM Response / Remarks
76	Threat Intelligence Feed.	M	
77	Threat Actor Profiles.	M	
78	Indicators of Compromise (IOC).	M	
79	Indicators of Attack (IOA).	M	
80	MITRE ATT&CK Mapping.	M	

81	Threat Campaign Tracking.	G	
82	Attack Trend Dashboard.	G	
83	Sector-specific Threat Intelligence.	M	
84	Government-focused Threat Intelligence.	M	
85	Emerging Threat Alerts.	M	

G. Takedown Services

Sr.	Requirement	Category	OEM Response / Remarks
86	Phishing Website Takedown.	M	
87	Fake Domain Takedown.	M	
88	Fake Mobile Application Takedown.	M	
89	Social Media Takedown Coordination.	M	
90	Registrar Coordination.	M	
91	Hosting Provider Coordination.	M	
92	Search Engine De-indexing Assistance.	G	
93	Brand Abuse Takedown Tracking Dashboard.	G	

H. Dashboard & Reporting

Sr.	Requirement	Category	OEM Response / Remarks
94	Executive Dashboard.	M	
95	SOC Analyst Dashboard.	M	
96	Department-wise Dashboard.	G	
97	Asset Inventory Dashboard.	M	
98	Risk Trending Dashboard.	M	
99	Monthly Executive Reports.	M	
100	Quarterly Risk Reports.	M	
101	CSV/PDF Report Export.	M	
102	Role-Based Access Control (RBAC).	M	
103	REST API Support.	G	
104	SIEM Integration.	M	
105	Email Alerts.	M	
106	Webhook/API Alerts.	G	

I. Managed Service & Support

Sr.	Requirement	Category	OEM Response / Remarks
107	24x7 Managed Monitoring Service.	M	
108	Dedicated Technical Support.	M	
109	Named Technical Account Manager.	G	
110	Health Check Reports.	M	
111	Knowledge Transfer & Administrator Training.	M	
112	OEM Product Updates during Contract.	M	
113	Secure Multi-Tenant or Dedicated Deployment Option.	G	
114	High Availability Managed Service.	M	
115	Audit Logs & Activity Logs.	M	
116	SSO/SAML Integration.	G	
117	MFA Support.	M	
118	Comprehensive Documentation.	M	
119	Customizable Alert Rules.	M	
120	Asset Tagging & Classification.	G	

IRR Compliance Matrix & Eligibility Requirements

Incident Response Retainership – Compliance Matrix

Sr.	Description	Bidders Response	Compliance [Yes/No]
A.	Mandatory requirements for Service Provider/OEM		
i.	Service provider must have at least 7 years of experience in incident response and forensic investigations related to Cyber Security incidents in Information Technology Infrastructure, across India and globally.		
ii.	Service provider must have deep knowledge of attack methodologies, background, objectives, target countries/verticals categorized by specific APT groups, especially Threat event occurrences in Asia-India Region and in financial sector around the globe.		
iii.	Service provider must use combination of their own tools, scripts, inbuilt tools in available in Operating system wherever applicable to perform the incident investigation in order to collect telemetry data across Perimeter, Network & Endpoint.		
iv.	The tools used by Service provider must include custom built tools as well as commercially available products such as Network sensors and log collector.		
v.	The tools used by Service provider must support telemetry data collections from IT Networks / Systems / Endpoints.		
vi.	If required, the service provider must have the ability to perform malware analysis and reverse engineering of malware samples using both automated and manual techniques and provide host-based and network-based indicators that are used to find the malware variants in the wild.		
vii.	As part of the engagement, the service provider shall support in all subsequent phases of incident management lifecycle – triage / analysis, containment, eradication and recovery, and post-incident review.		
viii.	The service provider shall be equipped with tools and processes to ensure chain of custody is maintained throughout the engagement, secure handling (during incident response) and secure disposal of information (upon completion off incident response).		
ix.	Extensive library of Indicators of Compromise (IOC) and Threat Intelligence should be utilized during assessment to analyze network traffic, servers, PCs, network devices, and critical log data during assessment.		
x.	Service provider must have in-house capabilities or past experience to engage with law enforcement agencies and CERT-In to aid in investigations. Public reference on case studies of your engagement with law enforcement agencies shall be provided.		
xi.	The Service provider must have responded to more than 50 cyber security incidents in last 10 years India, out of which at least 5 belongs to incident response in BFSI sector.		
xii.	The Service provider must have cumulative experience of 5000 hours in last five year in cyber security investigations.		

xiii.	The Service provider must have more than 25 MITRE Attack references.		
xiv.	The Service provider must be able to provide profiles of at least 5 Advanced Persistent Threat (APT) / Threat Actor groups with comprehensive insights built based on tracking-of and responding to threats/breaches originating from these APT groups.		
xv.	The Service provider must have dedicated team of more than 50 Security Researchers, Analysts, and Incident Responders.		
xvi.	At least five (5) relevant client references for incident response shall be provided, for each reference include (client name may be redacted to comply with NDA); Nature of the engagement, dates of the engagement, Name (or description) of the client firm, and a summary of the activities Bidder performed. If necessary, references can be interviewed via blind conference calls to protect Bidder's previous clients' confidentiality.		
xvii.	Provide incident response engagements have Bidder had in the past three (3) years involving APT group intrusions. Provide examples of the nature of the intrusion and major activities that Bidder performed, or consulted with the customer organization to perform, in the past three (3) to remediate the intrusion.		
xviii.	Provide redacted incident response engagements have Bidder had in the past three (3) years involving ransomware attacks. Provide examples of the nature of the intrusion and major activities that Bidder has performed.		
xix.	Provide the experience Bidder's analysts have with malware analysis along with the tools used for incident response.		
xx.	Bidder should have an experience presenting information about incidents to a Board of Director level body. Provide details of Bidder's staff have this type of experience.		
xxi.	Provide at least three (3) sample (redacted) final report for an incident response engagement.		
xxii.	Provide five (5) sample resumes that represent a typical team. Names of the individuals are not necessary.		
xxiii.	Bidder will be responsible to provide all the hardware required for solution implementation, i.e. server/Virtual Machines and will provide RHEL OS and Mysql, if required as part of the solution. Any other software (database, application etc.) required for this project should be provided by bidder, included in BoQ and prices quoted for in the Commercial Bid Document.		
xxiv.	The bidder must supply a thorough inventory of the hardware components required for the planned implementation. This bill of Quantity (BoQ) should be itemized separately for all the environments, including DC and Disaster Recovery (DR). The BoQ should include, but is not limited to, the following details: In Scope solutions Components Site/Environment		

	Type (VM/Physical) OS name database license Database details, CPU/vCPU VLAN requirement (VLAN or Internet) RAM Hard Disk Size Software pre-requisites (.NET framework, IIS, IE, any other OS services, etc.) If any missing requirements are discovered at any stage, the bidder will be obliged to provide them free of cost as a part of solution.		
B.	SKILL and Experience of resources deployed for Incident Response		
i.	The resources /consultants engaged in the activity must have at least 5 years hands on experience in identifying compromises and responding to security breaches.		
ii.	The incident responders should be holding at least any two of the following professional certifications: GIAC Cyber Threat Intelligence (GCTI), or GIAC Certified Forensic Analyst (GCFA), or GIAC Certified Incident Handler Certification (GCIH) or EC-Council Certified Incident Handler v2 (E CIH), or Certified Information Systems Security Professional (CISSP) or GIAC Cloud Forensics Responder (GCFR) or GIAC Network Forensic Analyst (GNFA) or GIAC Reverse Engineering Malware Certification (GREM) or Computer Hacking Forensic Investigator (CHFI) or Offensive Security Certified Professional (OSCP)		
iii.	The consultants engaged in the activity must have at least 3 years of hands on experience in threat hunting / malware/ IOC analysis.		
iv.	The consultants engaged in this activity must have experience of dealing with Incident response projects of multinational financial institutions.		
v.	The consultants engaged in this activity must have at least 3 years hands on experience with SOC, either in advisory or operational capacity.		
vi.	The consultant shall engage resources for implementation of various job activities required to complete this assessment by giving a detailed item wise plan of action.		
C.	Methodologies for handling of Cyber Incident and response		
i.	The Bidder must be able to Conduct host-based sweeping activities.		
ii.	The Bidder must be able to search for malware and tools linked to specific attack groups that are collectively known as Advanced Persistent Threat (APT) groups.		

iii.	The Bidder must be able to utilize a mix of automated and manual techniques to identify indicators of compromise.		
iv.	The Bidder must be able to search for various artifacts not limited to: staging paths, persistence mechanisms, lateral movement mechanisms, registry keys, etc.		
v.	The Bidder must have to capability to sweep the Endpoint with IOC's related to Custom Malware looking for Persistence Mechanism and Lateral Movement techniques.		
vii.	The Bidder must have an ability to scan different flavors of Windows, Linux, Unix etc. environments for evidence of compromise.		
viii.	The Bidder must be able to also search for malware and tools associated with non-APT groups.		
ix.	The Bidder must inspect IT systems for IOCs Identifying file names and hashes of known malware and utilities.		
x.	The Bidder must inspect IT systems for IOCs Analyzing file import tables of each executable file for specific IOCs.		
xi.	The Bidder must inspect IT systems for IOCs Reviewing all running processes and network connections for references to known "hostile" domains.		
xii.	The Bidder must inspect IT systems for IOCs Inspecting registry keys and values associated with known malware, and for persistence mechanisms that could lead to the detection of unknown malware.		
xiii.	The Bidder must inspect IT systems for IOCs Identifying specific global mutexes used by processes.		
xiv.	The Bidder must inspect IT systems for IOCs Detecting rootkits, hidden files, hidden processes etc.		
xv.	The Bidder must be able to analyses Web Shells for evidence collection.		
xvi.	The Bidder must be able to analyze event logs generated from different IT systems for evidence collection.		
xvii.	The Bidder must be able to automate collection and analysis of evidence and minimize manual activities.		
xviii.	The Bidder must be able to analyse a majority of assets (at least 85% or higher) and not limit to dipstick analysis on a limited set of assets.		
xix.	The Bidder must be able to Conduct network monitoring activities.		
xx.	The Bidder must have the capability to sweep the Network with IOC's related to Custom Malware looking for Lateral Movement techniques.		
xxi.	The Bidder must be able to monitor the Network traffic for Backdoor command and control protocols.		
xxii.	The Bidder must be able to monitor the Network traffic for Communication to IP addresses that are associated with targeted attacker activity.		
xxiii.	The Bidder must be able to monitor the Network traffic for Resolution of domain names that associates with targeted attacker activity.		

xxiv.	The Bidder must be able to monitor the Network traffic for Certificates that are used by attackers to encrypt malicious traffic.		
xxv.	The Bidder must be able to Conduct log data analysis activities.		
xxvi.	If required, the Bidder must have the ability to perform malware analysis and reverse engineering of malware samples using both automated and manual techniques and provide host-based and network-based indicators that are used to find the malware variants in the wild.		
xxvii.	If required the Bidder should be able to assist for an incident response, from the initial detection to the final resolution of the incident.		
xxviii.	The bidder must able to provide Signatures, YARA rules, detection rules, block rules for the solution deployed in GoG environment such AV, SIEM, EDR, IDS/IPS, WAF, Load balancer, NBAD, Active Directory, etc. in order to detect the presence of IOC or revert the back the changes made by the attacker.		
xxix.	Bidder must be able to perform non-intrusive IRR activities such as log collection, scanning activity, IOC scans using inbuilt tools in cases if agent installation or vendor proposed tool installation is not possible.		
xxx.	The bidder shall identify and document all potential entry points through which cyber attackers may gain access to the network.		
xxxi.	The bidder shall review and update the existing "Cyber Crisis Management Plan" to ensure it includes clearly defined roles and responsibilities.		
D.	WORKSHOPS		
i.	The successful vendor should conduct two in-person workshop/ hands-on trainings for GoG's official, during the contract period. The content of the training/workshop will be such that it should facilitate GoG's team members in responding to Cyber Security incident. Three days of Incident Response training and certification for GoG's Security team aligned with IRR Activities should be provided by the vendor. The successful vendor shall arrange to provide Hands-on simulation-based training on well-known Cyber Security Incidents.		
E.	ANALYSIS AND REPORTING OF INCIDENTS		
i.	The various Incident Response handling process, analysis, reporting should follow the standard frameworks such as NIST, Lockheed Martin cyber kill chain process, MITRE ATT&CK, diamond model etc.		
ii.	The Security Vendor must be able to provide comprehensive detail of compromise(s) and attack flow(s) if GoG is found compromised.		
iii.	The Security Vendor must be able to Provide Executive reports for Senior Management and non-technical stakeholders with the details of the scanning results and evidence.		
iv.	The Security Vendor must be able to analyze and provide context and intel related to any evidence(s) of		

	compromise found instead of purely enumerating list of the same.		
v.	At the end of the any particular IRR activity, Bidder should provide written confirmation that the infrastructure is free of threat/infection, or the presence of threat actor is seen after agreed monitoring time from both parties.		
vi.	Draft report of the incidents to be vetted by GoG officials. Reports should not be shared to unauthorized entities without written consent.		
vii.	Draft detailed report for law enforcement agencies, regulators, communication with internal and external stakeholders.		
F.	DELIVERY OF IRR SERVICES AND SCOPE		
i.	Phase 1: Incident Response Readiness Assessment (IRRA). This phase will Improve GoG's Incident Response Plan and Procedures. In this phase vendor will help to establish an incident response capability so that it is ready to respond to it. Under this preparation phase, this involves preparing for potential cyber incidents by establishing incident response plans, identifying the procedural and technical gaps in existing IT Setup w.r.t. incident response readiness, creating an incident response team representative from GoG and IRR vendor personals, defining roles and responsibilities, and implementing monitoring and detection systems. Workshops/assessment to be conducted with various stakeholders in GoG in order to understand GoG environment to enable to Bidders Incident response team to respond, mitigate, recover from attacks as soon as possible. This phase is to review GoGs existing Incident response plans, technologies deployed, log sources in place to detect/analyses to be checked and reediness in order to respond to attacks/breaches within stipulated timelines.		
ii.	The vendor should perform the gap assessment on existing SOP of Cyber Security incident handling/ Cyber crisis management plan and various other procedure documents.		
iii.	The IRRA should not be only limited to meetings/workshops/trainings, but Infrastructure manipulation capabilities also to be assessed based on various real time use cases, but not limited to; 1. Centralized deployment/execution of IOC scanners or other tools designed to obtain digital evidence. 2. Credentials management (e.g. password change policies) 3. System backup architecture and backup recovery. 4. Logging security event sources 5. Log sources / security controls check. 6. Assessment of readiness to respond, mitigate, recover from various attack scenarios, but not limited to; i. Espionage by threat actors (including state-sponsored groups) ii. Watering hole attacks		

	iii. Trusted relationship attacks iv. Supply chain attacks v. ATM jackpotting vi. Ransomware attacks vii. Unauthorized access to servers viii. Unauthorized access to databases ix. Unauthorized access to web applications or security bypass attacks x. Unauthorized access to network equipment xi. Insider attacks (leaks) xii. Insider attacks (disruption, sabotage) xiii. Insider attacks (unauthorized access) xiv. Insider attacks (unauthorized crypto-currency mining) xv. Infection using botnets. xvi. Phishing campaigns (links) xvii. Phishing campaigns (attachments) - xviii. Crypto-currency mining malware attacks xix. Cyber-physical attacks 7. The log sources / security controls should include, but not limited to i. Active directory logs ii. Network traffic logs iii. Event logs from endpoints and servers (at the OS, database and application level) iv. EDR v. SIEM vi. VPN connection logs vii. Web access logs viii. Antivirus software logs ix. Authentication logs x. Logs of user authorization and activities on business systems xi. Audit logs of user actions on virtual machine servers - Checking sources and performance of SIEM systems xii. Email etc.		
iv.	The vendor will help GoG to prepare incident response team's specific technical methods, strategies, checklists, and forms based on gap assessment.		
v.	The vendor will provide recommendations on how to improve incident response readiness.		
vi.	The vendor will provide recommendations on how to reconfigure or upgrade existing security event monitoring.		
vii.	The vendor will setup the dedicated IT infrastructure for GoG , either physical or in onsite private cloud instance, which will be utilized and accessed by IRR analysts, during incident response for log analysis and correlation. No logs or metadata should be transferred outside premises. The cloud instance should be preserved at least for 3 years of end of contract or based on agreed retention period as per CERT-In / GoG guideline.		

viii.	MITRE ATT&CK coverage for the most valuable tactics, techniques, and sub-techniques.		
ix.	During Incident response readiness review exercise the vendor should clearly define below modalities in detail. Incident Response Retainership team structure and responsibilities Communication between different teams (Stakeholders from GoG) will take place in case of Cyber Incident Procedure of sharing evidence / access to the required logs. The selected vendor will help to prepare and regularly update IRR Playbooks.		
x.	Establishing required Infrastructure to handle Cyber Incident/ sharing evidence: The successful vendor should establish a process, and deploy/install necessary hardware, software, sensors, scripts, agents for collection of evidence for incident analysis, and Assist in clearing/signoff of Comprehensive security review (CSR) of such tools, devices, and technologies before completion of Phase 1 (IRR)		
xi.	Recommendations on how to reconfigure or upgrade existing security event monitoring systems, backup solutions, security devices, etc.		
xii.	Incident Response Readiness Assessment Report.		
xiii.	Incident Response Readiness Assessment Guide.		
xiv.	Phase 2: Incident Identification – The remaining man hours will be utilized in onwards phases, on actual utilization and deployment of IRR services.		
xv.	This phase will involve identifying a potential incident by collecting and analyzing data from various sources, such as intrusion detection systems, log files, applications, devices and network traffic.		
xvi.	24 * 7* 365 days dedicated India and domestic support facility for incident response shall be made available by the vendor. The vendor IRR staff should be well trained to effectively handle queries raised by GoG, whenever a phone call/ email /alert received from GoG's dedicated Officials for probable incident.		
xvii.	The Service provider should start the Incident Response within 4 Hours of reporting of alert from GoG. Upon confirmed breach, the IR analyst should immediately start working on preliminary information submitted by LIC. The IR analyst should be at onsite location of breach, if required, as per timelines mentioned in this RFP.		
xviii.	Phase 3 – Containment: In this phase, the IR (incident response) team will work to contain the incident to prevent the further damage to IT assets. This may involve, and not limited to, isolating affected systems, disconnecting them from the network, or shutting them down.		
xix.	The vendor should help GoG to contain the Cyber Security Incident and to eliminate components (Malware, Threat actor) of the Cyber Security Incident.		

xx.	The vendor should assist GoG in identifying and mitigating all vulnerabilities that were exploited by the Threat Actor.		
xxi.	Phase 4 - Analysis: This phase will involve analyzing the incident to determine the scope, cause, and extent of the damage. The IR team may further gather and examine evidence, interview witnesses, and use forensic tools to identify the attacker and their methods.		
xxii.	Log retention and the logs collected/processed should be available for export in supported formats and not associated without any proprietary formats for audit/compliance purposes.		
xxiii.	The vendor should restore the attacked system/operations to normal state and should ensure that the systems are functioning normally and remediate vulnerabilities to prevent similar incidents.		
xxiv.	The vendor should be able to perform investigation on different technologies, assets inclusive of all technologies, applications, devices residing in GoG's IT-Ecosystem and the various resources required during the investigation should be scalable.		
xxv.	Phase 5 Eradication: This phase involves removing the threat and restoring affected systems to their original state. For example, this may involve deleting malware, applying software patches, recommendation of closing vulnerability, exploit used by the threat actor to gain access to the network or restoring from backups. It should be made sure that eradication of threat is to be carried out without disruption to the business.		
xxvi.	Phase 6 Recovery/Monitoring: In this phase, the incident response team works to restore normal business operations and ensure that all systems are functioning properly. This shall also involve conducting user awareness training, updating policies and procedures, and reviewing incident response plans. The bidder should perform continuous monitoring of the network/in for the agreed period of time based on the severity of incident in order to make sure that there is no remanence of the threat actor left in the network.		
xxvii.	Phase 7: Reporting & Lesson learned: The successful vendor should provide.		
xxviii.	Threat Briefing with Executive Board Members. Assist in reporting and notification to Regulatory and statutory authorities, Law Enforcement Agencies, communication to external and internal customers, GoG's Corporate communication handling Public Relations &. Social Media Department, Human Resource Department, News publication etc. Root cause analysis of the incident for corrective actions to be submitted to GoG for improvements in robustness and resilience in Cyber Security posture of GoG's IT infrastructure.		
xxix.	In the final phase, i.e. lesson learned, for improvement in Incident Response capabilities of GoG. The incident response team should conduct a post-incident review to identify what worked well and what could be improved for future incidents. The IR team must give inputs to update		

	GoG's incident response plan and suggest action plan for implementing necessary changes.		
xxx.	Upon submission of final report, the successful bidder shall not retain any data, and all hard drives consumed will be completely wiped out and reused by the successful bidder in future.		

Note:

- Bidder must comply with the above-mentioned criteria. Non-compliance to any of the criteria leads to rejection of the bid. GoG reserves the right to verify/evaluate the claims made by the bidder independently. Any misrepresentation will entail rejection of the offer.
- Evidence to be submitted for each criteria should be part of the same response document. Proper naming and indexing should be done to avoid any ambiguity.
- The bidder who successfully qualifies in the eligibility criteria, only their technical bids will be subsequently opened for further evaluation.

13. TECHNICAL EVALUATION (TQ):

External Attack Surface Management (EASM) and Digital Risk Monitoring (DRM)			
Criteria	Evaluation Parameters	Max Marks	Documents to be submitted
The number of External Attack Surface Management (EASM) and Digital Risk Monitoring (DRM) services proposed to the tenderer and rendered by OEM / OSD directly or through their channel partners to the BFSI/ Financial Institutions/ PSU / Govt. Organizations in India in last 3 years (as on RFP date)#.	For each client experience	2	Copies of Work Order / Client Reference letter
	Maximum Marks	10	
The number of External Attack Surface Management (EASM) and Digital Risk Monitoring (DRM) services proposed and rendered by the bidder to the BFSI / Financial Institutions/ PSU / Govt. Organizations in India in last 3 years (as on RFP date)#.	For each client experience	5	Copies of Work Order / Client Reference letter
	Maximum Marks	15	
Number of employees on the permanent payroll of the bidder with CISA / CISSP / CEH / CCSP / CISM certifications from ISACA / (ISC) ² / EC-Council.	For 5-10 employees	5	1. Copy of relevant certificate. 2. Undertaking on letter head of the bidder.
	For 11-20 employees	7	
	For more than 20 employees	10	
	Maximum Marks	10	
The OEM/OSD has own Security Operations Centre (SOC) / Security Monitoring Setup and the same is ISO 27001 / SOC 2 / SOC 3 certified.	For Own SOC	4	Letter of undertaking from the OEM/OSD and copy of certification, if applicable.
	Own Research Team	3	
	ISO 27001 / SOC 2 / SOC 3 certification	3	
	Maximum Marks	10	
Compliance to Technical Requirements	100% Compliance with mandatory technical requirements as mentioned in Annexure 12.	20	Point-wise compliance for technical requirements as per Annexure 12 along with details.
Technical Presentation	Demonstration of in-depth understanding of the tenderer's requirements as per RFP, features and functionalities of the proposed services, methodology and approach by the Bidder.	20	Copy of technical presentation, approach and methodology.
Value Added Services to the government for cyber-threat/risk identification, detection and/or protection without any additional cost / commercials	For each value-added service	5	Details of value-added services to be provided by the bidder.
	Maximum Marks	15	
TOTAL MARKS		100	

Evaluation Criteria for Incident Response Retainer (IRR) Services

Only those bidders who qualify in the Technical Evaluation (minimum 70% score) will be considered for Commercial Evaluation.

Technical Evaluation (100 marks)

Criteria	Maximum Marks	Evaluation Method
Experience of Bidder in IRR / Cybersecurity Incident Handling	20	Number of similar engagements with Government / BFSI / PSU clients (≥5 years experience)
Certifications & Competence of Proposed IR Team	20	GCIH, GCFA, CISSP, OSCP, EnCE, CEH; >70% team certified in relevant IR/forensics
Methodology & Approach for Incident Response (Phases 1–7)	20	Detailed methodology, tools, playbook development, MITRE ATT&CK coverage
Tools, Technology & Infrastructure Offered	15	Licensed forensic tools, SIEM/EDR integration, evidence handling capability
Incident Response Readiness Assessment Plan (Phase 1)	5	Quality of proposed IRR exercise and deliverables
Past Performance / Client References	10	At least 3 references from large Govt/BFSI/PSU engagements
Training & Awareness Programs	5	Number and quality of workshops, tabletop drills, certifications
Understanding of GoG Environment & Value-Added Services	5	Tailored approach, support for SOC, threat hunting, cloud/OT IR readiness

Minimum qualifying score: 70/100 (70%).

14. PAYMENT SCHEDULE:

PAYMENT TERMS

The payment for services rendered under the EASM, IR and DRM RFP will be released in a phased manner after Completion of Quarterly EASM, IR and DRM Assessment with all necessary Report Submissions which are asked in this RFP.

Payment Schedule EASM & DRM

Milestone	Payment
Successful Deployment, Configuration, Integration, Asset Discovery, Training and Go-Live (FAT Sign-off)	20%
Managed EASM & DRM Services	80%, payable in equal quarterly instalment, subject to SLA compliance

For subsequent contract years, payment shall be released in equal quarterly installment after acceptance of deliverables and SLA compliance.

No advance payment shall be made. The department shall release all payments only after verification of deliverables and certification in quarterly/half annually/yearly basis.

Statutory Deductions Applicable deductions such as TDS, GST-TDS, penalties, and liquidated damages shall be made as per Government rules.

Payment Terms for Incident Response

Payments will be processed based on actual man-hours consumed and verified deliverables. Invoicing will be permitted under the following milestones:

Deliverable	Payment Eligibility
Completion of Incident Response Readiness Assessment (IRRA)	Invoice may be raised for actual man-hours utilized subject to deployment of human resources / sensors / agents / tools / software / hardware
Completion of each Incident Response engagement from Detection to Reporting	Invoice may be raised for actual man-hours utilized upon submission & acceptance of final IR report
Training / Workshop completion	Payment upon approval of training delivery, materials and attendance certification

All invoices shall be supported with work logs, resource utilization sheets and approval certificates.

Conditions for Quarterly Payment

Quarterly payment shall be released upon submission and acceptance of:

- Invoice.
- SLA Compliance Report.
- Platform Availability Report.
- Monthly Monitoring Reports.
- Quarterly Executive Report.
- Asset Discovery & Risk Assessment Report.
- Takedown Activity Report.
- Support Ticket Summary.

Any applicable SLA penalties shall be deducted from the corresponding quarterly payment.

Common Provisions (Applicable to Both EASM/DRM and IRR)

Contract Period

The engagement of EASM, DRM and Incident Response (IR) Services for 2 years.

General Conditions

- The cumulative SLA penalty shall not exceed 10% of the Quarterly Invoice.
- Repeated SLA violations (more than three instances within 6 months) may result in issuance of a warning and performance review.
- Failure to meet critical SLA requirements for three consecutive months or repeated unsatisfactory performance may lead to termination of the contract.
- The Directorate of ICT & e-Governance, Government of Gujarat reserves the right to withhold payment for incomplete deliverables, non-compliance with contractual obligations, or failure to achieve the prescribed Service Level.

Notes:

- No advance payment will be made.
- Invoice should be generating in name of Security Operations Center, Directorate of ICT & e-Governance.
- Invoice should be submitted with all reports and necessary artifacts. payment will be processed after submission of all necessary documents.
- All payments will be subject to penalties for delays, as specified in the Service Level Agreement (SLA).
- In case of any penalties applied due to delays or non-compliance with SLAs, the corresponding deductions will be made before processing payments.
- For all above mentioned activities for EASM, IR and DRM Necessary Manpower compulsorily need to be deployed at GSOC.
- Quarterly Payment will be made after submission of aforementioned all deliverables within 30 days of completion of quarterly exercise.
- Successful Bidder shall be paid **Quarterly Payment (QP)** as per the services provided to TENDERER. The overall penalty would be calculated cumulatively & it will be generally capped at 10% of QP amount. If the cap of overall penalty is reached in two consecutive Quarter, the penalty cap for the third Quarter onwards, for each Quarter will increase by 5% over the penalty cap for the preceding quarterly till it reaches 25% of the QP. In addition to the applicable penalty and the provisions pertaining to closure/termination of contract, the TENDERER shall be within its rights to undertake termination of contract if or anytime the penalty increases by 15% of the QP. Once the penalty cap has increased beyond 10%, if the bidder through better performance delivery for any Quarter, brings the leviable penalty below 10% then the computation of the 1st of the 2 consecutive Quarter as referred above will reset and will begin afresh.
- During contract period, if tenderer asked any report bidder has to submit those reports within timeline as mentioned in this RFP.
- The Selected bidder has to provide necessary Hardware, Software, Licenses and other required accessories to complete this solution.

Payment Procedures:

- a) The Successful Bidder will have to raise the Invoice in the name of the "Directorate of ICT & e-Governance". The same has to be submitted at the DIT Office.
- b) The Successful Bidder will have to raise the component-wise invoice upon achieving the respective milestone as per the detailed payment schedule and submit the invoice to DIT.
- c) The Selected Bidder's request(s) for payment shall be made to DIT along with the 2 original copies of invoices and necessary supporting documents and artifacts. The invoice should be in English. The payment to the selected bidder shall be processed by GSOC/DIT on submission of reports and fulfilment of other contractual obligations as per the Terms and Conditions of Service Level Agreement (SLA).
- d) On receipt of such invoice, the invoice would be processed within 45 working days after due verification of the invoice and other supporting documents by GSOC/DIT/DST or its designated agency/TPA.
- e) GSOC/DIT/DST or its designated agency/TPA shall verify the invoice(s) raised against the milestone achieved along with the supporting documents as prescribed and acceptable to GSOC/DIT/DST.
- f) Payment shall be made in Indian Rupees. While making the payment, the necessary deduction for penalties (if any) and applicable tax/TDS will be made.
- g) The bidder shall have to furnish the payment receipt of tax collected and paid/deposited to the appropriate tax authorities.

- h) If there is any deficiency in the performance of contractual obligations on the part of the successful bidder, the successful bidder shall be liable for the imposition of appropriate penalties as specified in this RFP, and GSOC/DIT/DST shall be entitled to deduct such Penalties at source while making payment to the bidder for the services provided.

15. PRICE BID SCHEDULE:

IR - Indicative Price Bid

Sr. No.	Type of services / Items(A)	No. of Man hours ^ (B)	# Total amount in Rs.(C)
1	Per man-hour cost for Incident Response Retainer Services	Rs. ----- /manhour	Amount _____ For 100 Manhours (i.e. 1B x 100)
2	Phase 1 Incident Response Readiness Assessment (IRRA) (including any cost of deployment of sensors, agents, Hardware, software, licenses etc. required for IRRA) (Maximum of 40 Manhours)	Number of Man Hours required	Amount _____ for Phase 1 IRRA (i.e., 1B x 2B)
3	IRR services	Manhours left for IRR Services (i.e. 100- 2B)	Total Amount for IRR services (i.e. 1B x 3B)
4	Total Man Hours (2+3) - Annually	100 Man Hours	Amount _____ {i.e. (2C + 3C) = 1C} *

* This will be the Total Cost of Ownership (TCO)/Total Project Cost and should be quoted in the reverse auction.

Amount quoted in INR exclusive of GST/CGST)

^ Eight man hours = One man day

Note:

- Bidders are requested to submit their financial proposal only in this annexure.
- Pricing information should not appear in any other section of the proposal and must be submitted as per procurement process.
- Pricing is to be valid for six (6) months from the date designated as the bid closing date for receipt of proposals under this RFP.
- Travel and logistics to be included in the quoted rate.
- The Payment Schedule must provide a detailed cost breakdown including separate figures for each item, components or category or functional grouping as per Annexure.
- All prices / rates quoted must be quoted in Indian Rupees. Only GST will be provided extra. GST percentage for services to be mentioned.

For EASM and DRM

Sr.	Description	Total Cost (Rs.)	GST Amount (Rs.)	Total Amount (including GST) in Rs.
1	External Attack Surface Management – Annual Subscription Cost			
2	Digital Risk Monitoring – Annual Subscription Cost			
Total (with taxes)				

Commercial Bid

Sr No.	Item Description	Quantity	Total Amount (₹) (including taxes)
1	Cost of External Attack Surface Management (EASM) and Digital Risk Monitoring (DRM) for the period of 2 years.	1	
2	Cost of Incident Response (IR) Services for 2 Years	1	
Total (with taxes)			

Note: Subscription cost should include but not be limited to the cost of services, license cost, support cost and cost of all the components and services required to comply the requirements of the tenderer as mentioned in the RFP. The Bidder shall quote the Prices in the format mentioned above.

Note: All prices quoted by the Bidder should be in INR.

Bid Evaluation Process

- The TENDERER will form a committee which will evaluate the proposals submitted by the bidders for a detailed scrutiny. During evaluation of proposals, the TENDERER, may, at its discretion, ask the bidders for clarification of their Proposals.
- The bidders are expected to provide all the required supporting documents & compliances as mentioned in this RFP.
- During the evaluation, committee may seek the clarification in writing from the bidder, if required. If bidder fails to submit the required clarifications in due time, the evaluation will be done based on the information submitted in the bid.
- The financial bid will be evaluated based on the lowest financial cost quoted (L1) for the bid.
- Tenderer may negotiate the prices with L1 Bidder, under each item/head offered by Bidder.
- Based on bidder performance, Department may extend the contract for next 1 year.

Award of Contract

In case, the L1 bidder does not accept the award of contract or found to be involved in corrupt and/or fraudulent practices, then in that case, the L2 bidder will be awarded the contract. Further, if the L2 bidder also declines, the tenderer may award the contract to the L3 bidder.

Resolution of Complaints

Any complaints (other than the SLA parameters) notified by the Authority to the Agency shall have to be replied to in written along with the suggested course of action to be taken in order to resolve the complaint by the Agency within 10 (ten) working days of the complaint being notified.

The suggested course of action by the Agency shall then be reviewed by the Authority and the final modifications (if any) shall have to be implemented in a manner and time frame suggested by the Authority.

Performance Bank Guarantee (PBG)

- PBG: 10% of total contract value, valid for contract period + 6 months
- PBG to be submitted within 15 days of issuance of Purchase Order
- Unconditional, irrevocable PBG from a scheduled commercial bank (other than successful bidder's bank)
- The Performance Guarantee shall be valid for a period of 180 days beyond Warrantee period and shall be denominated in Indian Rupees and shall be in the form of an unconditional Bank Guarantee issued by All Nationalized Bank including the public sector bank or Private Sector Banks or Commercial Banks or Co-Operative and Rural Banks (operating in India having branch at Ahmedabad/ Gandhinagar) as per the G.R. no. FD/MSM/e-file/4/2023/0057/DMO dated 21.04.2023 along with its earlier referenced GRs

issued by Finance Department or further instruction issued by Finance department time to time in the format provided by GoG to be submitted within 15 days from the date of

issue of work order/Letter of Intent. The Performance Guarantee shall be discharged by GoG and returned to the bidder within 30 days from the date of expiry of the Performance Bank Guarantee.

Format 1: Proposal Covering Letter

(To be on the Bidder's letterhead duly Signed by Authorized Signatory)

Tender Ref No:

To
General Manager (Software Procurement)
Gujarat Informatics Ltd.
Block no. 2, 2nd floor, Karmayogi Bhavan,
Sector 10-A, Gandhinagar.

Ref: Request for Proposal (RFP) for <<>>>

Dear Sir,

We (Name of the bidder) hereby submit our proposal in response to notice inviting tender date And GEM bid no. xxxxxxxxxx Dated: dd/mm/yyyy and confirm that:

1. All information provided in this proposal and in the attachments, is true and correct to the best of our knowledge and belief.
2. We shall make available any additional information if required to verify the correctness of the above statement.
3. Certified that the period of validity of bids is 180 days from the last date of submission of proposal, and
4. We are quoting for all the items (including services) as per the price bid format Section-VII as mentioned in the RFP.
5. We the Bidder are not under a declaration of Ineligibility for corrupt or fraudulent practices or blacklisted by any of the Government agencies.
6. We have an office in the state and relevant documents for the same are attached. We undertake that if the local presence is not there in the state, that we shall establish an office at Gandhinagar/ Ahmedabad, within 30 days from the date of the award of contract.
7. Gujarat Informatics Limited may contact the following person for further Information regarding this tender: -
 - a. Name & Designation:
 - b. Full address of office
 - c. Email ID & Contact No.
8. We are uploading our Response to the RFP (Eligibility, technical and financial bid documents) as per the instructions set out in this RFP.

Yours Sincerely,

(Signature)

Name of Authorized Signatory:

Designation:

Date:

Name of the bidder:

Format 2: Bank Guarantee format for Earnest Money Deposit

Dated:

To
General Manager (Software Procurement)
Gujarat Informatics Ltd
Block no. 2, 2nd floor,
Karmayogi Bhavan, Sector-10A,
Gandhinagar.

Whereas ----- (here in after called "the Bidder") has submitted its bid dated ----- in response to the GeM bid no: xxxxxxxxxxxxxxxxxxxx for ----- KNOW ALL MEN by these presents that WE ----- having ----- our registered office at ----- (hereinafter called "the Bank") are bound unto the -----, Gujarat Informatics Limited in the sum of ----- for which payment well and truly to be made to Gujarat Informatics Limited, the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this ----- day of -----2025.

THE CONDITIONS of this obligation are:

The EMD may be forfeited, In case of a Bidder if:

- 1) The bidder withdraws its bid during the period of bid validity.
 - a. The Bidder does not respond to requests for clarification of their Bid.
 - b. The Bidder fails to co-operate in the Bid evaluation process.
 - c. The bidder, fails to furnish Performance Bank Guarantee in time.
- 2) The bidder fails to Sign the contract in accordance with this RFP
- 3) The bidder is found to be involved in fraudulent and corrupt practices

We undertake to pay to the GIL up to the above amount upon receipt of its first written demand, without GIL having to substantiate its demand, provided that in its demand GIL will specify that the amount claimed by it is due to it owing to the occurrence of any of the above-mentioned conditions, specifying the occurred condition or conditions.

This guarantee will remain valid up to 9 months from the last date of bid submission. The Bank undertakes not to revoke this guarantee during its currency without previous consent of the GIL and further agrees that the guarantee herein contained shall continue to be enforceable till the GIL discharges this guarantee The Bank shall not be released of its obligations under these presents by any exercise by the GIL of its liability with reference to the matters aforesaid or any of them or by reason or any other acts of omission or commission on the part of the GIL or any other indulgence shown by the GIL or by any other matter or things.

The Bank also agree that the GIL 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 SELLER and not withstanding any security or other guarantee that the TENDERER may have in relation to the SELLER's liabilities.

Dated at _____ on this _____ day of _____ 2025.

Signed and delivered by

For & on Behalf of
Name of the Bank & Branch & Its
official Address with seal

Approved Bank: All Nationalized Bank including the public sector bank or Private Sector Banks or Commercial Banks or Co-Operative & Rural Banks (operating in India having branch at Ahmedabad/ Gandhinagar) as per the G.R. no. FD/MSM/e-file/4/2024/2859/DMO dated 01st May 2025 issued by Finance Department or further instruction issued by Finance department time to time.

Format3: PERFORMANCE BANK GUARANTEE
(To be stamped in accordance with Stamp Act)

Ref: Bank Guarantee No.

Date:

To,
Director (IT)
Directorate of ICT & e-governance
Block no. 2, 2nd floor, Karmayogi Bhavan,
Sector-10A, Gandhinagar.

Dear Sir,

WHEREAS..... (Name of Bidder) hereinafter called "the Bidder" has undertaken, in pursuance of Agreement dated, (hereinafter referred to as "the Agreement for "RFP regarding empanelment of agencies for Request for Proposal (RFP) for Procurement of Routers and switches for various locations of Commissionerate of State Tax, Ahmedabad, (GEM Bid No. xxxxxxxxxxxxxxxx Dated: xx.xx.xxxx) for the Department of Science & Technology, Government of Gujarat.

AND WHEREAS it has been stipulated in the said Agreement that the Bidder shall furnish a Bank Guarantee ("the Guarantee") from a scheduled bank for the sum specified therein as security for implementing PROJECT.

1. WHEREAS we _____ ("the Bank", which expression shall be deemed to include its successors and permitted as Signs) have agreed to give the Gujarat Informatics Limited ("GIL") 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 Bidder to GIL under the terms of their Agreement dated . Provided, however, that the maximum liability of the Bank towards GIL under this Guarantee shall not, under any circumstances, exceed _____ in aggregate.

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

Attention Mr. _____.

3. 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 be mutually decided by the bidder and GIL.

The liability of the Bank under the terms 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 Bidder with any of the terms and conditions of any Agreements/credit arrangement, present or Future, between Bidder and the Bank.

4. The BANK also agrees that GIL 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 BIDDER and not withstanding any security or other guarantee that GIL may have in relation to the Bidder’s liabilities.

5. 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 GIL or any other indulgence shown by GIL or by any other matter or thing whatsoever which under law would, but for this provision, have the effect of relieving the BANK.

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

Dated this Day of ,2025

Witness

(Signature)
(Name)

(Official Address)

(Signature)
Bank Rubber Stamp
(Name)
Designation with Bank Stamp Plus,
Attorney as per Power of Attorney
No.

Dated:

Approved Bank: All Nationalized Bank including the public sector bank or Private Sector Banks or Commercial Banks or Co-Operative & Rural Banks (operating in India having branch at Ahmedabad/ Gandhinagar) as per the G.R. no. FD/MSM/e-file/4/2024/2859/DMO dated 01st May 2025 issued by Finance Department or further instruction issued by Finance department time to time.

Format 4: Format for Financial Summary of the Bidder

(Same should be furnished by theCharteredAccountant /StatutoryAuditor on their letter head)

Average Annual Turnover of the Bidder

S. No	Financial Year	AnnualTurnover (INR)
1.	Year 2023-24	
2.	Year 2024-25	
3.	Year 2025-26	
	[Average Annual Turnover]	[indicate sum of above divided by 3]

Note: Bidders are required to provide data for last three years ending 31st March 2024. Audited Balance Sheets are also required to be submitted for the same.

UDIN No:_____

Certificate from the Statutory Auditor

Note:

1. The Bidder shall submit audited annual reports (financial statements: balance sheets, profit and loss account, notes to accounts etc.) in support of the financial data duly certified by statutory auditor/s. In case, the company does not have a statutory auditor/s, it shall be certified by the chartered accountant that ordinarily audits the annual financials of the company.
2. Certificate(s) from the statutory auditors specifying the Turnover of the Bidder, as on FY 2021-22, OR FY 2022-23 OR FY 2023-24 (as the case may be). For the purpose of this RFP, net worth shall mean the sum of subscribed and paid-up equity share capital and reserves from which shall be deducted the sum of revaluation reserve, miscellaneous expenditure not written off and reserves not available for distribution to equity shareholders.

Format 5: Certificate / Undertaking for Land border from Supplier

<Bidder Company Letterhead>

To
General Manager (Software Procurement)
Gujarat Informatics Ltd.
Block no. 2, 2nd floor, Karmayogi Bhavan,
Sector-10A, Gandhinagar.

Sub: Undertaking as per Office Memorandum No.: F. No.6/18/2019-PPD dated 23.07.2020 published by Ministry of Finance, Dept. of Expenditure, Public Procurement division

Ref: Bid Number:

I have read the clause regarding restriction on procurement from a bidder of a country which shares a land border with India. I certify that we as a bidder and quoted product from following OEMs are not from such a country or, if from such a country, these quoted products OEM has been registered with competent authority. I hereby certify that these quoted product & its OEM fulfills all requirements in this regard and is eligible to be considered for procurement for Bid number

No	Item Category	Quoted Make & Model

In case I'm supplying material from a country which shares a land border with India, I will provide evidence for valid registration by the competent authority, otherwise GIL/End user Dept. reserves the right to take legal action on us.

(Signature)

Authorized Signatory of M/s <<Name of Company>>