Request for Proposal (RFP) for Selection of Implementing Agency for Providing External Attack Surface Management (EASM), Incident Response (IR) Services and End Point Management Solution for Gujarat Security Operations Center Department of Science & Technology, Government of Gujarat

(RFP # GIL/e-Gov/EASM/2025)

GeM Bid No:- GEM/2025/B/7052518

Issued By: -

Gujarat Informatics Ltd

Block No. 2, 2nd Floor, C & D Wing, Karmayogi Bhavan

Sector - 10 A, Gandhianagar-382010, Gujarat

Ph. No. 23259237, 23259240, Fax: 23238925.

www.gil.gujarat.gov.in

Definitions

Authorized Signatory	The bidder's representative (explicitly, implicitly, or through conduct) with the powers to commit the authorizing organization to a binding agreement.
Bid	"Bid" means the response to this document presented in Single Packet, Technical Cum Commercial Bid and Financial Bid, which are supplied with necessary documents and forms as given in Annexure, complete in all respect adhering to the instructions and spirit of this document.
Bidder	"Bidder" means any individual/proprietor/ partnership firm/ agency/ Company responding to Request for Proposal and who submits Bid.
Contract	Means the contract of service entered between the User Department and the "Service Provider" for External Attack Surface Management (EASM), Incident Response (IR) Services and End Point Management Solution for Gujarat Security Operations Center Department of Science & Technology, Government of Gujarat.
EMD	Earnest Money Deposit
DD	Demand Draft
Purchaser	User Department
TC	Tender Committee
PBG	Performance Bank Guarantee
Security Deposit (SD)	Amount of the Order Value deposited by the Bidder and retained till the successful completion of the project (as long as the bidder fulfils the contractual agreement).
RFP	"RFP" means the Request for Proposal
Work Order	"Work Order" shall mean the Purchase Order/Work order and its attachments and exhibits issued by User Department
Consignee	"Consignee" shall mean User Department.
Client	User Department/User Department's Client
EASM	External Attack Surface Management
IR	Incident Response (IR) Services
EPM	End Point Management Solution
Validity of Documents	Validity of all the documents shall be counted from the last date of submission of bids

Table of Contents

Purpose of this Document

This Request for Proposal (RFP) document has been prepared solely for the purpose of enabling GIL to select the agency for Providing External Attack Surface Management (EASM), Incident Response (IR) Services and End Point Management Solution for Gujarat Security Operations Center, Department of Science & Technology, Government of Gujarat

The GIL, for this purpose, invites proposal from Bidders who are interested in participating in this RFP who fulfil the eligibility criteria mentioned in this RFP and are also in a position to comply with the technical requirement as mentioned in this RFP. Apart from the above the bidder must also agree to all our terms & conditions mentioned under this RFP.

The RFP document is not recommendation, offer or invitation to enter in to a contract, agreement or any other arrangement, in respect of the services. The provision of the services is subject to observance of selection process and appropriate documentation being agreed between the GIL and any successful Bidder as identified by the GIL, after completion of the selection process as detailed in this document.

GIL may, at its own discretion, extend the date for submission of bids. In such case, all rights and obligations of the GIL and bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

Information Regarding RFP

Proposal in the form of BID is requested for the item(s) in complete accordance with the documents/attachments as per following guidelines.

i. Bidder shall upload their bids on https://gem.gov.in/
ii. Bids complete in all respects should be uploaded on or before the BID DUE DATE.
iii. In the event of the date specified for receipt and opening of bid being declared as a holiday for GIL office, the due date for submission of bids and opening of bids will be the next working day at the appointed time.
iv. Services offered should be strictly as per requirements mentioned in this Bid document.
v. Please spell out any unavoidable deviations, Clause/ Article-wise in your bid under the heading Deviations.
vi. Once quoted, the bidder shall not make any subsequent price changes, whether resulting or arising out of any technical / commercial clarifications sought regarding the bid, even if any deviation or exclusion may be specifically stated in the bid. Such price changes shall render the bid liable for rejection.
The bid submitted should be valid for a period of 180 days from the date of bid opening

Instruction to the bidders for online bid submission

i. 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/.

ii. 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/.

iii. Interested and eligible Bidders are required to upload the eligibility related document in eligibility bid section, Technical related document in Technical bid section & Commercial Bid in Commercial bid section. The Technical & Commercial Bid must be uploaded to https://gem.gov.in/

iv. In case of any clarifications required, please contact General Manager (Software Development) in writing 2 days before the Pre-Bid meeting date.

v. In case the bidders need any support related to bidding on https://gem.gov.in , Bidder may also send their clarifications on dgmapp-gil@gujarat.gov.in and manager-egov@gujarat.gov.in. also, bidder may contact the following office:

GM (Software Development),
e-Governance Division, Gujarat informatics ltd
Block No. 2, 2nd floor, Karmayogi bhavan,
Gandhinagar-382010

Fact Sheet: -

#	Particulars	Details
1.	Tender No:	GeM Bid No:- GEM/2025/B/7052518 dated – Date of Float bid with RFP# GIL/e-GOV/EASM/2025
2.	Contract Period	As per mentioned Contract duration for External Attack Surface Management (EASM) Solution for the period of 2 years, extendable by 1 year. For Incident Response (IR) Services for 2 years, extendable by 1 year and For End Point Management (EPM) Solution for 5 Years
3.	Earnest Money Deposit (refundable)	Rs. 16,00,000/- 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 For Bank Guarantee Format: Follow 'Form 5'

4.	Last Date and time of Submission of query in GIL	Note: Proposal must be submitted online on https://gem.gov.in/ website. If you have any query, then please send us by email on dgmapp-gil@gujarat.gov.in; manager-egov@gujarat.gov.in; exe1-egov-gil@gujarat.gov.in tse1-egov-gil@gujarat.gov.in
5.	Place, date and time for opening of Preliminary bid	DD.MM.2025 up to 1600 hrs. Gujarat Informatics Ltd. Block No. 2, 2nd Floor, C & D Wing, Karmyogi Bhavan, Gandhinagar
6.	Validity of Tender	180 days.
7.	Contact Person	GM (Software Development) Gujarat Informatics Ltd, Email ID: dgmapp-gil@gujarat.gov.in
8.	EMD Exemption	• MSME seller exempted from the EMD submission with a relevant MSME certificate having relevant NIC code as per RFP • The seller also exempted from EMD submission with respect to clause "Sellers will get exemption from furnishing Bid Security Sellers / Service Provider having annual turnover of INR 500 Crore or more, at least in one of the past three completed financial year(s)".

Note:

1) The TENDERER reserves all the rights to cancel the process and reject any or all the proposals at any time.
2) No contractual obligation whatsoever does arise from the RFP document/process unless and until a formal contract is signed and executed between the TENDERER and the successful proposers.
3) The TENDERER disclaims any factual or other errors in the RFP document (the onus is purely on the individual proposers to verify such information) and the information provided therein are intended only to help the proposers to prepare a logical proposal.

SECTION – 1 ELIGIBILITY CRITERIA

Eligibility and Evaluation Criteria

Evaluation will be based on the firm meeting the Pre- qualification criteria. It is mandatory for the firm (as an individual or in consortium) to fulfill all the pre-qualification criteria to be technically qualified. The User Department/GIL reserves the right to assess the firm's capability and capacity in the overall interest of the project.

Table 1.1: Pre-qualification Criteria

#	Basic Requirement	Specific Requirement	Documents Required
1	Legal Entity	The bidder should be a registered company (registered under Indian Companies Act, 1956 or Indian Companies Act, 2013) in India. The bidder should have been in operation for at least five financial years (FY2019-20, FY2020-21, FY2021-22, FY2022-23, FY 2023-24)	Copy of Letter of Incorporation/ Certificate of Registration attested by Authorized signatory of the company
2	Financial Turnover of bidder	The bidder should have minimum annual average turnover of Rs. 16 Crores from IT/ITES services in the last three financial years (i.e. 2021-22, 2022-23 and 2023-24) as on 31st March 2024 for which bidder's accounts have been audited.	• Audited and Certified Balance Sheet & Profit/ Loss Account of last 3 Financial Years. • CA certificate clearly certifying the turnover requirements as per the clause

3	Bidder Past Experience of work execution:	The bidder must have successfully executed/completed at least 1) One single order of Rs. 6 Crores or 2) Two Orders each of Rs. 4 Crores or 3) Three Orders each of Rs. 3 Crores for similar product / services in last 3 years to any central/ state Government / PSU/ Listed Company/BFSI. The project should cover similar activities and scope of work as defined in this RFP such as • External Attack Surface Management (EASM) services • Solution Incident Response (IR) Services • End Point Management Solution Services	The bidder shall submit Purchase Order/ Work Order and Project completion Certificate.
4	OEM Authorization (MAF)	Manufacturer Authorization: Wherever Authorized Distributors/ service providers are submitting the bid, Authorization Form /Certificate with OEM/Original Service Provider details such as name, designation, address, e-mail Id and Phone No. required to be furnished along with the bid	MAF Submitted
5	Neighboring country	Bidder and OEM does not belong to a country which shares a land border with India.	Signed and stamped as per Form-5 on company letterhead & Form -6 on OEM letter head for suppling items
6	Mandatory Undertaking	Bidder should not be blacklisted by any Ministry of Government of India or by Government of any other State in India or by Government of Gujarat or any of the Government PSUs at the time of bidding.	Self- Declaration Certificate on Non-Judicial Stamp Paper duly Notarized, Annexure 'B'
7	Consortium/ Subletting	Consortium/ Subletting shall not be allowed	Not applicable
8	Technical/Compliance Checklist	Bidder should submit Compliance Checklist for EASM, Incident Responses & End Point Management	As per format given Compliance/Checklist in RFP

Technical Criteria: -

Sr.	Requirement	Documentary Evidence Required
1	The bidder should have at least 2 years of experience in providing External Attack Surface Management (EASM) and Digital Risk Monitoring / Digital Risk Protection (DRM/DRP) services/ End Point Management (EPM) Solution/ Incident Response (IR) Services in Government / PSU / Financial Institution / Large Enterprise organizations/Listed Companies in India during the last three (3) years (as on RFP release date	Documentary Proof such as order implementation / contract execution copy / Work Order / Completion Certificate.
2	The bidder should have a minimum of 5 qualified cybersecurity professionals on permanent payroll holding certifications such as CISA / CISSP / CEH / CCSP / CISM / OSCP / CRTP / CREST issued by globally recognized bodies like ISACA / $(ISC)^2$ / EC-Council / Offensive Security / CREST.	Copy of valid certificates and an undertaking on company letterhead confirming employment status.
3	The bidder should have a direct support presence in Gujarat (Ahmedabad/Gandhinagar region). In case a direct office is not available, the bidder must provide an undertaking to ensure 24×7 onsite support within Gujarat and support availability at national level locations whenever required by GSOC without additional cost.	Letter of undertaking / confirmation on company letterhead.

Note:

i. 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.
ii. All details and the supportive documents for the above should be uploaded in the GeM bid.
iii. Any bid failing to meet any of the required above pre-qualification criteria shall be disqualified.
iv. A board resolution OR power of attorney in the name of the person executing the bid, authorizing the signatory to commit the Bidder.
v. All certificates requested in the RFP should be valid as on date of bid submission.
vi. All annexures as sought in this bid should be complete as per the information requested.
vii. No Consortium is allowed in this bid.

1.2: INSTRUCTIONS TO BIDDERS (ITB)

1.2.1 Sources of Funds

a. Gujarat Informatics Limited (GIL), on behalf of GSOC, is issuing this Request for Proposal (RFP) for the Selection of Implementing Agency for providing External Attack Surface Management (EASM), Incident Response (IR) Services, and Endpoint Management Solution for the Gujarat Security Operations Center (GSOC) under the Department of Science & Technology, Government of Gujarat, through GIL.

b. Payment for services rendered under this RFP and subsequent Work Orders shall be made by GSOC from their own sanctioned sources of funds, in accordance with the financial terms and conditions specified in the RFP and the respective Work Orders.

1.2.2 Cost of Bidding

a. The Bidder shall bear all the costs associated with the preparation and submission of its bid, and GIL will in no case be responsible or liable for these costs, regardless of conduct or outcome of bidding process.

1.2.3 Applicable Law

a. The Contract shall be interpreted in accordance with the laws of the Union of India and that of State of Gujarat.

1.2.4 Governing Language

a. The contract shall be written in English language. All correspondence and other documents pertaining to the Contract, which are exchanged by the parties, shall be written in the same language.

1.2.5 Clarification of Bidding Documents

a. A prospective bidder requiring any clarification of the bidding documents may seek clarification of his/her query on the date indicated on RFP clause of this document. GIL will respond to any request for the clarification of any bidding documents, which it receives during the meeting on the date mentioned on the RFP clause of this document GIL shall hold a pre-bid meeting with the prospective bidders on date & time given in Section 1.

b. The Bidders will have to ensure that their queries for pre-bid meeting should reach to Name, Address and email id of the officer mentioned by post or email on or before on date & time of pre-bid meeting.

c. Pre-Bid queries sent on email id :- dgmapp-gil@gujarat.gov.in ; manager-egov@gujarat.gov.in ; exe1-egov-gil@gujarat.gov.in ; tse1-egov-gil@gujarat.gov.in

Bidder's Request for Clarification			
Name of Organization submitting request		Name & position of Person submitting request:	Address of organization including phone, fax, email points of contact
#	Bidding Document Reference (Clause / page)	Content of RFP requiring clarification	Points of Clarification required
1			
2			

Gujarat Informatics Limited shall not be responsible for ensuring that the bidder's queries have been received by them. Any requests for clarifications post the indicated date and time may not be entertained by the GIL.

1.2.6 THE BIDDING DOCUMENTS

1.2.6.1 Contents of Bidding Documents

b. The Bidder is expected to examine all instructions, forms, terms, and specifications in the bidding documents. Failure to furnish all information required by the bidding documents in format or submission of a bid not substantially responsive to the biding documents in every respect will be at the Bidder's risk and may result in rejection of its bid.

1.2.6.2 Amendment of Bidding Documents

c. At any time prior to the deadline for submission of bids, GIL may, for any reason, whether on its own initiative or in response to the clarification requested by a prospective bidder, modify, change, incorporate or delete certain conditions in the bidding document.

d. Amendment will be published on GeM/ GIL website. All prospective bidders are requested to browse GeM/GIL website & any amendments/ corrigendum/ modification will be notified on the website/ portal and such modification will be binding on them.

In order to allow prospective bidders reasonable time to take into consideration the amendments while preparing their bids the tendering authority, at its discretion, may extend the deadline for the submission of bids

1.2.7 PREPARATION OF BIDS

1.2.7.1 Language of Bid

e. The bid prepared by the Bidder, as well as all correspondence and documents relating to the bid exchanged by the Bidder and GIL shall be in English language.

1.2.7.2 Bid Form

f. The Bidder shall complete the Bid as per format and Annexure respectively. The bidder shall also complete the Bid Forms and submit along with required necessary attachments.

1.2.7.3 Earnest Money Deposit

a. Earnest Money Deposit **Rs. 16,00,000/- (Sixteen Lacs Only)** in the form of **Demand Draft** an **unconditional Bank Guarantee** (**which should be valid for 9 months from the last date of bid submission**) of any Nationalized Bank/ Scheduled Commercial Bank (operating in India having branch at Ahmedabad/ Gandhinagar) in the name of "Gujarat Informatics Limited" payable at Gandhinagar **(as per prescribed format given at Form-2)** and it must be submitted along with the covering letter. Also, the bidder must submit the PoA (Power of Attorney) in physically form to the GIL before the due time of bid opening. Bidders can upload the scan copy of EMD on the portal.

b. Proposals not accompanied by EMD shall be considered as non-responsive and rejected.

c. The successful bidder's EMD will be discharged from GIL only after the signing of the contract and submission of performance security.

d. Unsuccessful/Disqualified bidder's EMD will be discharged/refunded as promptly as possible, at least 30 days before the validity period of the bid expires.

e. The EARNEST MONEY DEPOSIT shall be forfeited:

   i. If a bidder withdraws its bid during the period of bid validity specified by the bidder on the bid form.

ii. Or in case where a successful bidder fails to sign the contract.

Note: Failing to submit physical covers of EMD along with the PoA (Power of Attorney) at GIL on or before DD.MM.2025 up to 1500 hrs. may lead to the rejection of the bid.

1.2.7.4 EMD Exemption: -

- EMD exemption shall be applicable as per the GeM General Terms and Conditions (GTC).
- MSME seller exempted from the EMD submission with a relevant MSME certificate having valid NIC code as per scope of work
- The seller also exempted from EMD submission with respect to clause "Sellers will get exemption from furnishing Bid Security Sellers / Service Provider having annual turnover of INR 500 Crore or more, at least in one of the past three completed financial year(s)".

1.2.7.5 Period of Validity Bids

a. Bids shall be valid for 180 days after the date of bid opening prescribed by GIL. A Bid valid for a shorter period shall be rejected by GIL as non-responsive.
b. In exceptional circumstances, GIL may solicit the Bidder's consent to an extension of the period of validity. The request and the responses thereto shall be made in writing. A Bidder may refuse the request without forfeiting its EMD. A Bidder granting the request will not be permitted to modify its bid.

SECTION – 2 SCOPE OF WORK

2.1 Scope of work for External Attack Surface Management (EASM) Services

Introduction

The Gujarat Security Operations Center (GSOC), under the Directorate of ICT & e-Governance, Government of Gujarat, aims to enhance its proactive cyber defense capabilities through External Attack Surface Management (EASM). The objective is to strengthen the state's cyber threat intelligence, asset visibility, risk detection, and remediation mechanisms across its digital footprint.

This RFP invites proposals from experienced and qualified vendors for provisioning of a comprehensive EASM solution encompassing External Attack Surface Management (EASM), and Digital Risk Monitoring (DRM) aligned with national cyber norms and GSOC's operational needs.

The selected bidder shall be responsible for delivering an integrated EASM platform and managed service that encompasses:

2.1.1 Comprehensive Asset Discovery & Inventory

- Continuous, automated identification and monitoring of all digital assets, including:
  - External (Internet-facing): Public IPs, domains, subdomains, APIs, web apps, open ports, exposed services.
  - Internal: Servers, endpoints, databases, IoT devices, network appliances.
  - Cloud Infrastructure: SaaS, IaaS, PaaS, storage buckets, server less functions across major cloud platforms.
  - Third-Party Assets: Vendor portals, partner systems, exposed code repositories.

Asset Classification by:

  - Ownership, business function, criticality, data sensitivity.
- Relationship Mapping: Identify interdependencies and potential attack paths.
- Change Detection: Real-time detection of configuration drift, newly added services/assets.
- Monitoring of digital assets not limited to portals and applications, Web services, APIs, IP Pools etc. listed and to be listed under the asset register.

2.1.2 Vulnerability & Exposure Identification

- Conduct scheduled and on-demand vulnerability scans for:
  - Known CVEs, misconfigurations, outdated software, weak encryption.
- Detect high-risk exposures like:
  - Publicly accessible storage, unprotected admin consoles, expired SSL certs, misconfigured DNS/SPF/DMARC records.
  - Leaked credentials or secrets on GitHub, dark web, paste sites.
- Perform attacker simulation using OSINT and ethical reconnaissance techniques.

2.1.3 Threat Intelligence Integration

- Correlate vulnerabilities with real-world exploits, TTPs, malware campaigns.
- Mapping to MITRE ATT&CK techniques.
- Real-time insights into exploit trends targeting Government and CIIs.

2.1.4 Risk Prioritization & Scoring

- Risk scoring to factor in:
  - Business impact, exploitability, exposure duration, regulatory risk.
- Support for custom risk models based on GSOC's internal framework.
- Visualization of risk posture and trend analysis dashboards.

2.1.5 Remediation Management & Workflow Integration

Provide contextual, actionable remediation steps.

- Validate remediation post-fix with closed-loop verification.
- Provide all data, logs, alerts, incidents etc. for Integration with:
  - GSOC (Audit, Assets, Advisory modules)
  - EMS, NMS, SIEM/SOAR, DevSecOps CI/CD tools.
- SLA-driven remediation tracking and escalation workflows.

2.1.6 Continuous Monitoring & Alerts

- 24x7x365 monitoring of:
  - Configuration changes, asset exposure, emergent threats.

Real-time alerts via:

  - Email, SMS, GSOC Dashboard.
- Baseline Deviation Detection: Notify deviations from secure-state baselines.

2.1.7 Digital Risk Monitoring (DRM)

- Monitor:
  - Dark web, paste in, underground forums, app stores.
  - Impersonation attacks, phishing sites, rogue applications.
- Generate alerts for:
  - Credential leaks, brand abuse, data exposure.
- Support takedown of:
  - Fake domains, phishing content, rogue mobile apps (min. 20/year).
- DRM should align with **MeitY's Digital Risk Protection Guidelines**.

2.1.8 Reporting & Compliance

- Daily, weekly, and monthly reporting dashboards.
- Executive summary reports with KPIs/KRIs.
- Compliance mapping (ISO 27001, NIST, CERT-In, DPDPA, GIGW, NCRF).
- Full audit logs and policy enforcement reports.
- Visibility dashboards for Department Heads and Nodal Officers

2.1.9 Platform Features & User Access

- **Unified Dashboard** with:
  - Role-Based Access Control (RBAC)
  - Drill-down views, severity filters, keyword search.
- Authentication & Access:
  - Support MFA and secure SSO integration.
  - Minimum 10 user licenses for GSOC analysts. (10 user)
- **Deployment:** Preferably SaaS; on-prem. or private cloud option if mandated.

2.1.10 Integration Capabilities

API-based integration with:

- GSOC Portal (Assets, Audit, Ticketing modules)
- SIEM, SOAR, and EMS
- Vulnerability Management Tools
- DevOps Pipelines
- Active Directory, DNS, Firewall Management

2.1.11 Training & Documentation

- Training for GSOC cyber security team: minimum 2 sessions/year.
- SOPs, deployment run books, API documentation.
- Final handover report with implementation summary and roadmap.

2.1.12 Deliverables

1. Fully functional EASM platform with GSOC-integrated dashboard access.
2. Dynamic asset inventory and threat exposure visibility.
3. Monthly threat landscape and executive summaries.
4. Remediation status reports with SLA adherence.
5. Incident and risk trend dashboards (aligned with NCRF).
6. Takedown reports (for phishing/impersonation sites).
7. DPDPA & CERT-In aligned compliance documentation.

2.1.13 Contract Period

The engagement will be for External Attack Surface Management (EASM) Solution for the period of 2 years, extendable by 1 year based on satisfactory performance and cybersecurity risk landscape evolution at same cost and same terms & conditions.

2.1.14 Compliance & Governance

- Must comply with:
  - CERT-In Guidelines (Current & later updates)
  - MeitY Localization Norms for Cybersecurity Products
  - NCIIPC's National Critical Information Infrastructure Framework
  - DPDPA 2023, ISO 27001
- Execution of SLA and NDA before onboarding.
- Adherence to GSOC's governance and audit guidelines.

2.1.15 Support Expectations

- 24x7 access to technical support via helpdesk, web, email, and call.
- SLA-driven resolution for incidents and advisories.
- Quarterly OEM health check, tuning, patching, and threat feed validation.
- Incident support and war-room coordination during statewide cyber drills.

2.2 Scope of work for Incident Response (IR) Services

2.2.1 Technical Requirement for On-Demand Incident Response Services

The Service Provider shall provide on-demand, threat-informed incident response 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 cybersecurity 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.

2.2.2 Phased Delivery of IRR Services

Phase 1 – Incident Response Readiness Assessment (IRRA)

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

1. Review and assess existing Cyber Crisis Management Plan, SOPs, and departmental IR plans.
2. Identify gaps in readiness through workshops, assessments, and simulations with stakeholders across GoG.
3. Evaluate current technologies, logging sources, and monitoring practices.
4. Conduct tabletop exercises and readiness drills covering scenarios such as ransomware, phishing, insider threats, data breaches, and APT attacks etc.
5. Provide recommendations for enhancing log sources, detection capabilities, and backup/recovery readiness.
6. Develop/Update IR Playbooks and Runbooks aligned with MITRE ATT&CK framework and GoG environment.
7. Assist in defining team structures, roles, and escalation procedures.
8. Establish secure infrastructure for IR analysis, including agents/sensors/ scripts, to collect and analyze forensic evidence.
9. 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 24×7×365 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.

2.2.3 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.

2.2.4 Contract Period

The engagement of Incident Response (IR) Services for 2 years, extendable by 1 year based on satisfactory performance and cybersecurity risk landscape evolution at same cost and same terms & conditions.

2.3 Scope of work for End Point Management (EPM) Solution

2.3.1 Objective

To deploy a secure, scalable, and centrally managed End Point Management solution that enables patching, configuration, inventory, and security enforcement across all endpoints and appliances within GSOC's infrastructure. The solution must support full SIEM integration, supply chain risk visibility via SBOM, QBOM, advanced threat detection, and customization for compliance workflows. OEM enterprise-grade highest support is mandatory throughout the engagement.

2.3.2 Coverage & Target Assets

Asset Type	Quantity	Notes
Workstation, Servers, Endpoints	2000	OS: Windows, Ubuntu, RedHat, CentOS, Rocky Linux in virtual machine, physical, containerized
Network & Security Appliances	200	Includes firewalls, routers, switches, IDS/IPS, VPNs, HSMs, Load Balancers, Web Application Firewalls (WAFs)
Scalability	+25 % YoY	Additional endpoints/appliances (up to 25 % annually) without additional cost
		must be covered at no extra cost

2.3.3 Scope of Work

1. Design, install, configure, and commission the latest EPM solution across desktops, servers, and workstations. Installation, configuration, and commissioning shall be carried out by the OEM or OEM-authorized personnel, and Proof of Design and Configuration must be provided.
2. Required severs and other active and passive hardware's/software should be provided by bidder without additional cost to tenderer.
3. The EPM solution must provide full lifecycle management of Local site and DR sites assets, including patching, configuration, inventory, and security enforcement. DR endpoints must be manageable via multi-zone architecture, with offline policy enforcement, secure update transfer, and telemetry forwarding to central SIEM and EPM both should be mandatory.
4. Complete installation within 45 days of GSOC site hardware delivery. Declare prerequisites in proposal If any.
5. Licensing must be perpetual for minimum 10 users.
6. Quarterly OEM health check, tuning, patching, and integration validation.
7. Provide 5-year onsite comprehensive warranty starting from the date of FAT clearance and support must be of highest category whatever is the nomenclature.
8. OEM must provide version upgrades during warranty. Notify GSOC of Alpha, Beta, and Release versions. During the contract period, if OEM declares any equipment as end of support for any

reasons, Bidder has to replace that equipment with better or equivalent products without any cost to GoG.

9. Operationalize stable versions within 10 days of release. Report prerequisites/ bottlenecks immediately.
10. All updates/patches must be transferred via data diode (unidirectional) due to air- gapped network.
11. Reinstallation of agents' post reformatting must retain license status.
12. Resolve operational issues within 48 hours. Submit detailed bug analysis and resolution report.
13. Remote access to devices is prohibited. Onsite engineer required. Remote access only with prior approval and justification.
14. Provide minimum 7-day onsite training.
15. Bidder/OEM must provide hardware, software, install required OS, applications.
16. FAT must be completed within 30 days of installation. Bidder/OEM must support FAT committee and prepare documentation for approval. License start date is FAT clearance date.
17. Supply additional licenses up to 25% as per table of indent at same cost and terms year on year.
18. Bidder/OEM must not be blacklisted by any Indian organization.
19. Disputes shall be resolved mutually or via arbitration under Arbitration & Conciliation Act, 1996 (amended), arbitrator appointed by Director, Directorate of ICT e-Governance.
20. Bidder/OEM must sign NDA ensuring no GSOC-specific data or architecture is disclosed without permission.

2.3.4 Contract Period

The engagement of End Point Management (EPM) Solution will be for 5 Years

2.3.5 Technical Features

A. Agent & Architecture

1. Must operate in multi-tenant mode
2. Agent software must be deployed on all managed Endpoints. Support Windows, Ubuntu, RedHat, CentOS, Rocky Linux in physical, virtualized, containerized form. Must operate without AD/domain dependency but support AD integration.
3. Support agent deployment via AD Group Policy, login scripts, third-party tools, manual install.
4. Provide remote agent deployment utility using AD, NT domains, or local admin credentials.
5. Support agent inclusion in gold OS image.
6. End users must not be able to uninstall agents.
7. Agents must enforce last-applied policies even when offline/disconnected.
8. Agents must cache logs and sync with central console/SIEM upon reconnection.
9. Support encrypted communication natively (AES-256) without third-party certificates.

B. Patch Management

1. Centralized patching for desktops, laptops, servers, appliances via single UI.
2. Provide patching of OS, Application, Database, Middleware, Virtualization platforms, Security Tools, Packages.
3. Determine patch dependencies before deployment.
4. Provide patch severity levels and descriptions.

5. Enable patch deployment without user intervention.
6. provide custom patch policies and real-time status monitoring.
7. Allow patch deployment without reboot and staggered rollout to reduce bandwidth impact.
8. Automatically apply patches to newly added systems.
9. Auto-delete patch files post successful installation.
10. Provide patch rollback with status reporting and monitoring.
11. End-of-Life (EOL) and End-of-Sale (EOS) components patching must be provided where OEM-issued patches or documented security workarounds are available.

C. Configuration Management

1. The solution must enforce and maintain system configuration baselines across all managed endpoints, including registry settings, services, firewall rules, and OS-level parameters.
2. The agent must detect configuration drift in real time and automatically remediate deviations from approved baselines without requiring manual intervention.
3. Configuration policies must be enforced even when endpoints are disconnected from the network. Agents must cache last-applied policies and apply them autonomously.
4. All configuration changes—manual, automated, or policy-driven—must be logged locally and forwarded to the central console or SIEM upon reconnection."
5. Only authorized administrators should be able to define, modify, or approve configuration policies. RBAC must be enforced at both console and agent levels.
6. The solution must support versioning of configuration policies, allowing rollback to previously approved states and tracking of change history.
7. Configuration policies must be assignable to dynamic groups based on OS, hardware, subnet, installed applications, or AD attributes.
8. The administrator must be able to remotely edit registry entries, start/stop services, and enforce service startup types (e.g., automatic, manual, disabled).
9. The solution must support creation, deployment, and enforcement of custom Windows firewall rules across endpoints.
10. Custom Script Deployment
11. The solution must allow deployment of scripts to enforce configuration policies not available as predefined options.
12. Configuration enforcement, drift detection, rollback, and audit logging must be validated during Final Acceptance Test (FAT) with test cases covering online and offline scenarios.

D. Software Distribution

1. Support MSI, Install Shield, batch formats.
2. Distribute third-party and in-house software to targeted systems.
3. Install predefined software packages.
4. No separate agent required for software distribution.

E. Inventory & Asset Management

1. Real-time hardware/software inventory with auto-alerts on changes.
2. Dynamic grouping by AD, OS, subnet, RAM, CPU, disk space, etc.
3. Retrieve hardware details (CPU, disk, IP, peripherals, etc.).
4. List all software/services with near real-time updates with version, Build number.

5. Support registry edits via central console.
6. Create custom queries and generate asset reports.
7. Provide EOL/EOS inventory with expiry.

F. Remote Control

1. Full desktop control of Windows systems with/without user permission.
2. Role-based restrictions for control, reboot, file transfer.
3. AES-256 encryption for remote sessions.
4. End users must be able to regain control anytime.
5. Support searchable target list and group-based access control.
6. Web interface must support remote control, chat, file transfer.
7. Log session details (host, policies, events, transcripts).
8. Support collaboration, AD authentication, and full data stream encryption.

G. Security Policy Management

1. Control Windows desktop appearance, network settings, Control Panel, Task Manager, Start menu.
2. Start/stop services, reboot/shutdown endpoints.
3. Distribute certificates and manage permissions on files, folders, registry. Deploy custom scripts for security enforcement.
4. Control Windows firewall via custom rules.
5. Identify and uninstall specific applications.

H. Device & File Control

1. Control all ports and removable devices.
2. Block unauthorized data access and monitor file actions.
3. Create trusted device list.
4. Store mirror copies of transferred files in password-protected shares.
5. Monitor file actions in real time with full audit trail.

I. Disk Encryption

1. Support TPM/BitLocker status scanning.
2. Support OS drive, used space, and full disk encryption.
3. Manage recovery keys with auto-renewal and domain controller backup.

J. Vulnerability Management

1. Identify and assess Endpoint, Appliance, network-wide vulnerabilities and zero day at regular interval for all the endpoints and appliances including EOL, EOS assets.
2. Audit systems against CIS benchmarks and provide remediation insights.
3. Detect expired SSL, and unsafe software.
4. Monitor ports and processes for malware indicators.

K. Application Control

1. Control browser usage and plugins.
2. Support application whitelisting/blacklisting.
3. Grant on-demand access to unmanaged apps.

L. Reporting & Compliance

1. Track installed applications with publisher, title, version, and count.
2. Role-based access to reporting UI with filtering and custom views.
3. View raw agent data and inventory properties.
4. Include Software ID Catalog for vendor/product identification.
5. Generate license compliance reports.
6. Web-based reporting module with access control.
7. Reports must be ≤1-day old for active devices.
8. Include patch progress, vulnerability trends, asset distribution, top vulnerabilities, installed software.
9. Support built-in and custom report templates.
10. Generate hardware/software inventory reports.

M. Log, data forwarding and Integration

1. Provide all logs, data forwarding and API for integration with EDR, SIEM, SOAR, XDR
2. Behavioral analytics, IOC scanning, threat hunting
3. Endpoint telemetry forwarding to SIEM
4. Alert correlation and automated response support
5. Audit trail for all patch/config actions
6. SIEM log taxonomy must be defined for endpoint events (patch status, config changes, USB/file actions, threat alerts)

N. SBOM, QBOM Preparation & Supply Chain Risk

1. Should provide SBOM, QBOM generation natively / third-party SBOM, QBOM without additional agent
2. Exportable SBOM, QBOM formats for audit, CERT-IN, and compliance reviews
3. Visibility into software provenance and package-level risk

SECTION – 3 PENALTIES AND SERVICE LEVEL AGREEMENT (SLA)

The purpose of this Service Level Agreement (hereinafter referred to as SLA) is to clearly define the levels of service which shall be provided by SUCCESSFUL BIDDER to the CLEINT for the duration of this contract period of the Project.

All the payments related to the warranty period to the selected bidder referred to as "agency" are linked to the compliance with the SLA metrics specified in this document. Penalty levied for non-performance as per SLA requirements shall be deducted from subsequent payments due or from the Performance Bank Guarantee submitted by the bidder. The maximum ceiling of penalty shall be up to 10 percent of quarterly payment.

3.1 SLA & Other terms for EASM

The Service Provider shall ensure **24x7x365 availability** of the EASM platform, threat intelligence feeds, and associated managed services as per the agreed scope of work.

All SLAs shall be **measured monthly**, with **quarterly reporting** to GSOC management.

3.1.1 Service Level Agreement (SLA)

SLA Parameter	Target / Requirement	Measurement Criteria	Penalty / Action
Platform Availability (Uptime)	≥ 99.5% monthly uptime	System logs / monitoring reports	2% penalty on quarterly invoice for every 0.5% deviation below target
Asset Discovery Frequency	Daily incremental discovery; full scan weekly	Discovery report logs	Warning on first instance, 1% deduction thereafter
Threat Intelligence Feed Update	Real-time (within 1 hour of feed publication)	Feed update audit logs	1% penalty per delayed update instance
Remediation Advisory / Recommendations	Within 24 hours of issue identification	GSOC ticketing system	1% deduction per delayed advisory per day
Dark Web / Brand Monitoring Reports	Weekly	Submitted reports	1% penalty for each delayed or missed submission
Monthly Executive Summary Report	By 5th of following month	Acknowledged submission	2% deduction for each delayed report
Takedown Request Execution	Within 72 hours of GSOC approval	Report with evidence	2% penalty per delayed takedown
Support Response Time (Critical / High Severity)	< 1 hour (Critical); < 2 hours (High)	Ticketing / call logs	2% deduction per incident per delay

Support Resolution Time (Critical / High Severity)	< 6 hours (Critical); < 12 hours (High)	Ticket closure time	2% deduction per instance
Training & Knowledge Transfer	2 sessions annually	Attendance / completion reports	₹25,000 deduction per missed session
Compliance & Audit Support	As and when required by GSOC	Audit participation logs	₹50,000 per instance of non-participation

Note:

- Repeated SLA violations (>3 instances in a quarter) may lead to service review and performance warning.
- Three consecutive quarters of non-compliance may result in contract termination as per terms.

3.1.2 Performance Review and Reporting

- GSOC shall conduct **monthly performance review meetings**.
- SLA reports to be submitted by Service Provider within **7 working days of month-end**.
- Quarterly reports shall include summary of asset coverage, vulnerabilities discovered, risk posture improvement, and remediation trends.
- The Service Provider shall maintain all performance data for audit verification.

3.1.3 SERVICE LEVELS AND UPTIME

SLA Description	Requirement
Minimum Service Uptime	99.90%
Phishing / Rogue App Takedown	24 hours
Browser Blocking (if takedown not possible)	48 hours
Domain Take Down Time	72 hours
Social Media Abuse Removal	48–72 hours
TI Critical Alert Reporting	4–6 hours
EASM Report	3–7 days

3.1.4 Penalty

SLA penalties up to 10% of quarterly invoice
3 consecutive SLA failures → contract termination option

3.1.5 DELIVERY

Activity	Timeline
Service commencement	7 days from PO
Documentation submission	2 weeks
Integration & deployment	6 weeks
Go-live and Training	8 weeks

Note: - Delay penalty: 1% per week up to 5% max, beyond which contract may be cancelled

3.1.6 Payment Terms of EASM

3.1.6.1 Payment Milestones for EASM

Stage	Activity	Payment Percentage	Conditions / Deliverables
Phase 1 – Implementation	Installation, configuration, and integration of EASM platform with GSOC (UAT sign-off)	**30%**	Post successful deployment, training to GSOC staff, and UAT sign-off
Phase 2 – Operationalization	Go-Live and start of continuous monitoring	**30%**	Successful Go-Live after FAT signoff
Phase 3 – Quarterly Operations	Managed services, monitoring, and reporting	**40%**	Payment in 8 equal quarterly instalments upon submission of SLA-compliant performance report, invoice, and GSOC approval

3.1.6.2 General Conditions

1. Invoices shall be raised **quarterly**, post submission of performance and SLA compliance reports.
2. Deductions for SLA non-compliance (if any) shall be applied to the corresponding quarterly payment.
3. The **Service Provider must provide Performance Bank Guarantee (PBG)** equivalent to **3% of total contract value** valid for the entire contract period plus 60 days.
4. Taxes, statutory deductions, and GST will apply as per prevailing Government of India norms.
5. GSOC reserves the right to **withhold payment** for incomplete deliverables, missed SLAs, or unapproved changes.

3.1.6.3 Support and Maintenance

- 24x7 support through phone, web portal, and email.

- Designated SPOC for GSOC with escalation matrix.
- Periodic system patching, version upgrades, and bug fixes included in AMC.
- Proactive monitoring and tuning to ensure optimal performance.

3.1.6.4. Performance Evaluation and Penalties

- Monthly SLA compliance below **95%** shall trigger a **warning and penalty** (up to 5% of quarterly invoice).
- SLA compliance below **90% for two consecutive quarters** may result in **contract review or termination**.
- The decision of GSOC and the Directorate of ICT & e-Governance shall be **final and binding** in all performance-related matters.

3.2 SLA & Other terms for Incident Response

Other Terms of Contract, Project Schedule & Payment Conditions

3.2.1 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.

3.2.2 Helpdesk & Support Requirements

The selected service provider shall establish and operate a dedicated **24×7×365 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) b) Ensure trained technical experts 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.

3.2.3 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.

3.2.4 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.

3.2.5 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.

3.2.6 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

3.2.7 SLA, NDA & Legal Costs

The successful bidder shall bear all legal charges including stamp duty and documentation fees associated with SLA and NDA execution.

3.2.8 Project Execution Timelines

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

3.2.9 Incident Response Timelines (SLA)

Initial Response SLA 24*7*365 days dedicated global and	**Upper Time limit**

domestic support facility for incident response	
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	Within 12 hrs
Within India-Cities apart from above in 3.1	Within 24 hrs
Interim update report	**Every 12 hours during crisis incidents**
Final complete IR Report	**Within 10 working days post-containment**

3.2.10 Incident Response & Resolution

Severity Level	Example	Response Time	Resolution Time
Critical (P1)	Platform outage, critical data exposure	≤ **30 minutes**	≤ **4 hours**
High (P2)	Major functional degradation	≤ **1 hour**	≤ **8 hours**
Medium (P3)	Partial issue, minor alert delays	≤ **4 hours**	≤ **24 hours**
Low (P4)	Cosmetic issues, non-urgent queries	≤ **1 business day**	≤ **3 business days**

Response time = Time from issue reporting to acknowledgment.
Resolution time = Time to provide a permanent fix or acceptable workaround.

3.2.11 Penalty for SLA Non-Compliance

Metric	Penalty
Delay in onsite deployment	**1% of monthly retainer fee per hour delay**, max **15%**
Delay in final IR report	**0.5% per day**, max **10%**

Compliance Table

S. No.	GSOC Requirement	Compliance (Y/N)	Supporting Documents / Remarks
1	IR services must be delivered by a globally recognized OEM with minimum **10 years of experience** in cyber incident response engagements		

2	OEM must have proven experience managing **Advanced Persistent Threats (APTs)**		
3	OEM must have published **APT discovery and threat research** publicly; latest **five APT research reports** must be submitted		
4	OEM must have a minimum pool of **10+ cybersecurity experts stationed in India**, supported by a dedicated global incident response team Additionally 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)		
5	OEM must deploy **Incident Responders onsite within 12 hours** of incident notification by GSOC		
6	OEM must bring and utilize their **own tools, software and forensic devices** for live investigation		
7	Scope shall include but not be limited to: log analysis, configuration review, identification, containment & eradication, root cause identification, APT analysis, malware reverse engineering, endpoint/network/digital forensics, Purple & Red Team exercises, DB analysis (SQL/NoSQL)		
8	OEM must submit a **comprehensive incident investigation report** including: attack timeline, root cause, exploited vulnerabilities, payloads, lateral movement details, compromised data analysis, artifacts, IOCs, Sigma/YARA/SNORT/SIEM detection rules, MITRE mapping and remediation plan		
9	OEM must conduct investigation **onsite anywhere in India** as directed by GSOC		
10	OEM must appoint a **Single Point of Contact (SPOC)** for IR engagement		
11	Minimum **100 IR hours annually** included; scalable as needed		
12	Unutilized IR hours must be converted into **training, proactive assessments or professional certifications**		

13	**No logs, artifacts or data** shall leave GSOC premises; all analysis must be performed onsite		
14	**Remote response strictly prohibited** unless specially approved		
15	**Confidentiality to be enforced strictly**; no publication or sharing of any investigation detail externally without written approval of DST Gujarat		

3.2.12 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 **Phase-1: 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 from SOC authorized team.

3.3 SLA & Other terms for EPM

- The EPM timeline defines key deliverables and corresponding penalties for delays in submission or execution. The Vendor is required to adhere to the following timelines for deliverables:

S/n	Work type	Time Limit for Execution	Penalty for Delay	Maximum Penalty	Overall Penalty Cap
	Submission of PBG and HLD to be submitted	Within 07 working Days from date of issuance of GEM Contract	EMD will be forfeited, and contract will be terminated or part thereof	-	-
	Supply of the material Including Licenses & OEM	T1=T+90 days from the date of issuance of work order	0.5% of order value of delayed/ pending work per	10% of order value	Overall Penalty CAP is not more than 10% of the order

	Warranty Certificate.		week or part thereof		value For IMPLEMENTATION TIMELINES & PENALTIES:
	Installation, commissioning & integration	T2=T1+30	0.5% of order value of delayed/pending work per week or part thereof	10% of order value	
	Final Acceptance Testing (FAT) with SOP and Documentation	T3=T2+15 days	0.5% of order value of delayed/pending work per week or part thereof	10% of order value	

Material supplied, installed and commission as per this Bid/contract should be covered under the warranty for a period of five years from the date of FAT.
T= Date of issuance of contract over GEM

S/N	Deliverable
1	EPM Briefing Document
2	EPM Assessment Reports
3	Technical Findings Report
4	Executive Summary Report
5	Post-Exercise Debriefing Report
6	Training Session Reports

Note:

3.3.1 Service Level Agreement, Incident Classification & Penalty Matrix

Priority	Description	Response Time	Resolution Time	Penalty Clause
P1 – Critical	Complete outage of EPM console, agent failure across multiple endpoints, breach of security controls, or failure	Within 1 hour	Within 4 hours	₹5,000 per hour of delay beyond resolution time max 10% of Quarterly Order Value
P2 – High	Partial failure of patch/config enforcement, SIEM integration broken, DR	Within 4 hours	Within 12 hours	₹2,500 per hour of delay beyond resolution time max 10% of

	site sync failure, or critical policy drift			Quarterly Order Value
P3 – Medium	Single endpoint failure, report generation issues, minor config drift, or inventory mismatch	Within 8 hours	Within 24 hours	₹1,000 per hour of delay beyond resolution time max 10% of Quarterly Order Value
P4 – Low	Cosmetic UI issues, non-blocking alerts, documentation gaps, or training queries	Within 24 hours	Within 72 hours	₹500 per day of delay beyond resolution time max 10% of Quarterly Order Value

3.3.2 Performance Metrics

The Vendor is expected to meet the following performance standards:

3.1.1 Accuracy of Reports: Reports must accurately reflect the findings of the EASM, IR and EPM Exercise, including vulnerabilities, their criticality, and recommended remediation steps.

3.1.2 Completeness: All reports must include detailed technical analysis, risk ratings, and evidence of exploitation or proof-of-concept.

3.1.3 Compliance with Standards: The Vendor must ensure compliance with relevant industry standards such as MITRE ATT&CK, NIST, and other security frameworks as published by CERT-IN, NCIIPC, GOI.

3.1.4 Timely Communication: The Vendor is required to communicate any potential delays in deliverables well in advance and propose corrective actions to minimize the impact as mentioned in this RFP.

3.3.3 Resolution of Complaints

3.3.3.1 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.

3.3.3.2 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.

SECTION–4: GENERAL CONDITIONS OF CONTRACT (GCC)

❖ **Definitions**

In this Contract, unless the context otherwise requires, the following terms shall have the meanings assigned to them below:

a) "The Contract" means the agreement entered into between *Gujarat Security Operation Center (GSOC)* and the *Service Provider (SP)*, as recorded in the Contract Form signed by the parties, including all attachments, appendices, and documents incorporated therein by reference.
b) "Contract Price" means the price payable to the Service Provider under the Contract for the full and proper performance of its contractual obligations.
c) "Services" means all services specified in the Scope of Work of this document.
d) "GCC" means the General Conditions of Contract contained in this section.
e) "Gujarat Security Operation Center (GSOC)" means the Client availing the services from the Service Provider.
f) "Client's Country" means the country specified in the GCC.
g) "Service Provider (SP)" means the individual, firm, or entity supplying the goods and/or providing the Services under this Contract.
h) "Day" means a working day.
i) "Critical Deliverables" means the deliverables supplied by the Service Provider that are essential for project milestones and approvals.
j) "Time Required for Approval" means the time elapsed between the date of submission of a critical deliverable (complete in all respects for all business functions/services) and the date of its approval, excluding the intermediate time taken by the Service Provider for providing clarifications, modifications, or additional communication.
k) "Bid Document" and "Tender Document" shall be treated as the same and used interchangeably.
l) "Project Site", wherever applicable, means the place or places where the work is to be executed.
m) "Completion of Work" means the stage at which the work is certified by the competent authority, considering the design and development of the Comprehensive Website/Application as proposed in the RFP/Work Order.
n) "Go-Live" means the Comprehensive Solution, Platform is ready in all respects, including design, development, testing, and implementation of all modules listed in the Scope of Work, and is made available for first use by citizens and/or departmental users.
o) "Office Completeness" means the project site is complete in all respects, including:

- Supply, installation, and commissioning of hardware;
- Installation of requisite system software;
- Installation of requisite application software;
- Establishment of connectivity setup;

- Deployment of requisite manpower; and
- Full functionality of the entire setup as defined in the Scope of Work, enabling transactions to be carried out on computers.

p) "Maintenance" means all activities required to keep the system fully functional, including but not limited to:

- Maintenance of hardware and the Comprehensive Website/Application;
- Updating patches related to operating systems and software used for development;
- Identification and resolution of application-related issues such as runtime errors, malware, or viruses, including reloading of systems and mobile applications, wherever required;
- Ensuring continuous power supply to all machines during working hours; and
- Any other task necessary to ensure uninterrupted system operations.

q) "Performance Standards" means the maintenance and operational standards to be complied with by the Service Provider, including but not limited to:

- Maintenance of data, backups, and logs in accordance with CERT-In and GSOC guidelines (prevailing and upcoming), and providing the same as and when required; and
- Mandatory signing of a Non-Disclosure Agreement (NDA) by the Service Provider.

❖ **Application**

These General Conditions shall apply to the extent that provisions in other parts of the Contract do not supersede them.

❖ **Country of Origin**

- All Services rendered under the Contract shall have their origin in the member countries and territories eligible i.e. India
- The origin of Services is distinct from the nationality of the service provider.

❖ **Standards**

The software supplied under this Contract shall conform to the standards and when no applicable standard is mentioned; to the authoritative standard appropriate to the country of origin and such standards shall be the latest issued by the concerned institution.

❖ **Use of Contract Documents and Information**

- The service provider shall not, without Gujarat Security Operation Center(GSOC)'s prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample or information furnished by or on behalf of the in connection therewith, to any person other than a person employed by the service provider in performance of the Contract. Disclosure to any such employed person shall be made in confidence and shall extend only so far as may be necessary for purposes of such performance.

- The service provider shall not, without Gujarat Security Operation Center(GSOC)'s prior written consent, make use of any document or information except for purposes of performing the Contract.
- Any document, other than the Contract itself, enumerated in GCC shall remain the property of Gujarat Security Operation Center(GSOC) and shall be returned (in all copies) to Gujarat Security Operation Center(GSOC) on completion of the service provider's performance under the Contract if so, required by Gujarat Security Operation Center(GSOC).
- The Service Provider shall permit DIT/GSOC to inspect the service providers accounts and records relating to performance of the service provider with regards to this contract and to have them audited by auditors appointed by DIT/GSOC, if so, required by DIT/GSOC.

❖ **Patent Rights, Copy Right**

The Service Provider shall indemnify DIT/GSOC against all third-party claims of infringement of copyright, patent, trademark or industrial design rights arising from use of the Goods or any part thereof in India.

❖ **Intellectual Property Rights**

- The Department shall retain exclusive intellectual property rights over all custom-developed components, configurations, integrations, scripts, workflows, reports, and enhancements specifically created for the project, and the final solution, to that extent, shall be the sole and exclusive property of the Department.
- All pre-existing, proprietary, licensed software, platforms, tools, frameworks, and intellectual property of the OEM/Bidder shall remain the exclusive property of the respective OEM/Bidder, and no ownership rights therein shall be transferred to the Department, except for usage rights as defined under the contract**.**

Inspection/Testing

- The Department or its authorized representative shall have the right to **inspect, test, and validate** the EASM, IR, and EPM solutions and related deliverables at any stage to ensure compliance with the RFP specifications, security standards, and performance requirements, without any additional cost to the Department.

❖ **Change Request**

Any change in scope, specifications, or deliverables shall be governed through a mutually agreed Change Request (CR) mechanism, including impact assessment on cost, timeline, and resources, subject to written approval of the Department.

❖ **Earnest Money Deposited (EMD)**

- The bidder shall furnish, as part of its bid, an Earnest Money Deposit as asked in the bid.
- Proposals not accompanied by EMD shall be rejected as non-responsive.
- The successful bidder's EMD will be discharged from GIL only after the signing of the contract and submission of performance security.

- Unsuccessful bidder's EMD will be discharged / refunded as promptly as possible, but not later than 30 days of the validity period of the bid.
- The EARNEST MONEY DEPOSIT shall be forfeited:
    - If a bidder withdraws its bid during the period of bid validity specified by the bidder on the bid form;
    - Or in case of a successful Bidder, if the Bidder fails to sign the Contract; or to furnish the performance security.
    - No exemption for submitting the EMD will be given to any agency.

❖ **Performance Security/Performance Bank Guarantee (PBG)**

- The successful Bidder has to furnish a security deposit so as to guarantee his/her (Bidder) performance of the contract.
- The Successful bidder has to submit **Performance Bank Guarantee @ 5%** of total order value within 15 days from the receipt of notification of award/Contract Signing for the duration of warranty/contract period from banks (operating in India having branch at Ahmedabad/Gandhinagar) as per the G.R. no. FD/MSM/e-file/4/2023/4020/DMO dated 11th March 2024 issued by Finance Department or further instruction issued by Finance department time to time. (The draft of Performance Bank Guarantee is as per Section 10).
- The Performance Security shall be in the form of Bank Guarantee valid till 6 months from the date of contract expiry.
- The proceeds of the performance security shall be payable to the Gujarat Security Operation Center(GSOC) as compensation for any loss resulting from the Service provider's failure to complete its obligations under the Contract.
- The Performance Security will be discharged by Gujarat Security Operation Center(GSOC) and returned to the Bidder on completion of the bidder's performance obligations under the contract.
- No interest shall be payable on the Performance Bank Guarantee amount. Gujarat Security Operation Center(GSOC) may invoke the above bank guarantee for any kind of recoveries, in case; the recoveries from the bidder exceed the amount payable to the bidder.

❖ **Delivery and Documents**

- Delivery of the Goods shall be made by the Service Provider in accordance with the terms specified by Gujarat Security Operation Center(GSOC) in the Notification of Award.

❖ **Incidental Services**

- The Service Provider is required to provide the following services, including additional services, if any.
- Performance or supervision of the on-site assembly of the supplied Goods;
- furnishing of tools required for assembly and/or maintenance of the supplied Goods;
- furnishing of detailed operations and maintenance manual for each appropriate unit of supplied Goods;
- Performance or supervision or maintenance and/or repair of the supplied Goods, for the period of time mentioned in the tender notification.

❖ **Prices**

- Prices payable to the service provider as state in the contract shall be fixed during the performance of the contract.

❖ **Assignment**

- The service provider shall not assign, in whole or in part, its obligations to perform under the Contract, except with prior written consent of Gujarat Security Operation Center(GSOC).

❖ **Delays in the Service Provider's Performance**

1) Delivery of the Goods and performance of the Services shall be made by the Service Provider in accordance with the time schedule specified by DIT/GSOC.
2) If at any time during performance of the Contract, the Service Provider or his sub-contractor(s) should encounter conditions impeding timely delivery of the Goods and performance of Services, the Service Provider shall promptly notify DIT/GSOC in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the Service Provider's notice, DIT/GSOC shall evaluate the situation and may, at its discretion, extend the Service Provider's time for performance with or without a penalty, in which case the extension shall be ratified by the parties by amendment of the Contract.
3) The bidders shall read & understand the requirements thoroughly & shall adhere to the schedule strictly.

❖ **Termination for Default or otherwise**

- Gujarat Security Operation Center(GSOC) may, without prejudice to any other remedy for breach of contract, by written notice of default sent to the service provider, terminate the Contract in whole or part:
  a) if the service provider fails to deliver any or all of the services within the period(s) specified in the Contract, or within any extension thereof granted by Gujarat Security Operation Center(GSOC); or
  b) If the service provider fails to perform any other obligation(s) under the Contract.
  c) If the service provider, in the judgment of Gujarat Security Operation Center(GSOC) has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.
  For the purpose of this Clause:

  "Corrupt practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of a public official in the procurement process or in contract execution.
  "Fraudulent practice: a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the Borrower, and includes collusive practice among Bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the Borrower of the benefits of free and open competition;"
  d) If the Service Provider fails to conform to the quality requirement laid down/third party inspection/consultants opinion.

- If Bidder has violated / infringement of any Indian or foreign trademark, patent, registered design or other intellectual property rights. Certificate/affidavit regarding non-violation / infringement of any Indian or foreign trademark, patent, registered design or other intellectual property rights.

❖ **Exit and Transition**

- Upon contract termination or completion, the vendor shall:
    - Provide all data, reports, and configurations in usable format.
    - Support smooth transition to new service provider (minimum 30 days' support).
    - Ensure no data loss or service disruption during handover.
    - Return or delete all GSOC data as per approved retention policy.

❖ **Force Majeure**

1) Force Majeure shall mean any event beyond the control of Authority or of the Agency, as the case may be, and which is unavoidable notwithstanding the reasonable care of the party affected, and which could not have been prevented by the exercise of reasonable skill and care and good industry practices and shall include, without limitation, the following:
    a. War, hostilities, invasion, acts of a foreign enemy and civil war.
    b. Rebellion, revolution, insurrection, mutiny, conspiracy, riot, civil commotion, and terrorist acts.
    c. Strike, sabotage, unlawful lockout, epidemics, quarantine, and plague.
    d. Earthquake, fire, flood or cyclone, or other natural disaster
    e. Any other event as decided by the Authority

2) As soon as reasonably practicable but not more than 48 (forty-eight) hours following the date of commencement of any event of Force Majeure, an Affected Party shall notify the other Party of the event of Force Majeure setting out, inter alia, the following in reasonable detail:
    a. The date of commencement of the event of Force Majeure.
    b. The nature and extent of the event of Force Majeure.
    c. The estimated Force Majeure Period,
    d. Reasonable proof of the nature of such delay or failure and its anticipated effect upon the time for performance and the nature of and the extent to which, the performance of any of its obligations under the Agreement is affected by the Force Majeure.
    e. The measures which the Affected Party has taken or proposes to take to alleviate/mitigate the impact of the Force Majeure and to resume the performance of such of its obligations affected thereby.
    f. Any other relevant information concerning the Force Majeure and/or the rights and obligations of the Parties under the Agreement.

❖ **Termination for Insolvency**

- Gujarat Security Operation Center(GSOC) may at any time terminate the Contract by giving written notice to the Supplier / service provider, if the Supplier / service provider becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the Supplier / service provider, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to Gujarat Security Operation Center(GSOC).

❖ **Termination for Convenience**

- Gujarat Security Operation Center(GSOC) by written notice sent to the service provider, may terminate the Contract, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for Gujarat Security Operation Center(GSOC)'s convenience, the extent to which performance of the service provider under the Contract is terminated, and the date upon which such termination becomes effective.
- The services / software that is complete and ready for rendering / deployment within 30 days after the service provider's receipt of notice of termination shall be accepted by Gujarat Security Operation Center(GSOC) at the Contract terms and prices. For the remaining services, Gujarat Security Operation Center(GSOC) may elect:
    a) To have any portion completed and delivered at the Contract terms and prices; and/or
    b) To cancel the remainder and pay to the service provider an agreed amount for partially completed services / software and for services / software previously procured by the service provider.

❖ **Resolution of Disputes**

- In this regard Gujarat Security Operation Center(GSOC) doesn't go for any arbitration on dispute and Gujarat Security Operation Center(GSOC)'s decision will be final and binding on the service provider.

❖ **Governing Language**

- The contract shall be written in English language. All correspondence and other documents pertaining to the Contract, which are exchanged by the parties, shall be written in the same language.

❖ **Applicable Law**

- The Contract shall be interpreted in accordance with the laws of the Union of India and that of the State of Gujarat.

❖ **Taxes and Duties**

- Service providers shall be entirely responsible for all taxes, duties, license fees, octroi, road permits, etc., incurred until delivery of the contracted software/ services to Gujarat Security Operation Center(GSOC). However, GST in respect of the transaction between Gujarat Security Operation Center(GSOC) and the service provider shall be payable extra as on actual at the time of invoicing.

❖ **Binding Clause**

- All decisions taken by GIL regarding the processing of this tender and award of contract shall be final and binding on all parties concerned.

❖ **Confidential Information, Security and Data: -**

The selected bidder will promptly on the commencement of the exit management period supply to GSOC, Gujarat or its nominated agencies the following:

1. Documentation relating to Intellectual Property Rights;
2. Project related data and confidential information;
3. All current and updated data as is reasonably required for purposes of GSOC, Gujarat or its nominated agencies transitioning the services to its replacement selected bidder in a readily available format nominated by GSOC, Gujarat or its nominated agencies; and
4. All other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable GSOC, Gujarat or its nominated agencies, or its replacement operator to carry out due diligence in order to transition the provision of the services to GSOC, Gujarat or its nominated agencies, or its replacement operator (as the case may be).
5. Before the expiry of the exit management period, the selected bidder shall deliver to GSOC, Gujarat or its nominated agencies all new or up-dated materials from the categories set out above and shall not retain any copies thereof, except that the selected bidder shall be permitted to retain one copy of such materials for archival purposes only.

❖ **GIL/ Gujarat Security Operation Center(GSOC), Gandhinagar, reserves the right:** -

- To vary, modify, revise, amend or change any of the terms and conditions mentioned above; or
- To reject any or all the tender/s without assigning any reason whatsoever thereof or may terminate the tender process midway without assigning any reason.
- The decision regarding acceptance of tender by DIT/GSOC will be full and final.
- Conditional tenders shall be summarily rejected.
- Gujarat Security Operation Center(GSOC) is free to phase out the work if it feels it necessary.

Section: -5 Technical Bid Evaluation

The Technical Proposal will be evaluated for technical suitability and the criteria for evaluation of technical bids are as under:

5.1 Technical evaluation matrix of bids**:**

Criteria	Evaluation Parameters	Max Marks	Documents to be submitted
Technical POC – EASM and DRM Solution	Evaluation based on bidder's technical proof of-concept demonstrating completeness, functionality alignment with RFP requirements, scalability, automation, reporting, and integration capability, For DRM threat intelligence coverage, brand monitoring capability, alerting mechanism, remediation workflows, automation and dashboard maturity.	**30**	POC score sheet, demonstration adherence report, supporting documentation
Technical POC – EPM Solution	Evaluation based on bidder's technical proof-of-concept demonstrating endpoint security readiness, vulnerability reporting, device posture monitoring, remediation capability, compliance enforcement and integration support.	**30**	POC score sheet, demonstration adherence report, supporting documentation
IR (Incident Response) Services – Approach & Methodology	Evaluation of bidder's proposed Incident Response (IR) services approach, including IR framework, detection and response process, incident classification and severity handling, containment and recovery methodology, forensic readiness, communication and escalation matrix, SLA commitments, post-incident reporting, and alignment with industry best practices (CERT-In / NIST / ISO 27035).	**20**	IR methodology document, process flow diagrams, SLA & escalation matrix, sample IR report
Coverage of Complete Proposed Solution (EASM, DRM, IR, Endpoint Security)	Mandatory evaluation of bidder's submission, documentation, and demo covering all proposed modules. Bidder must demonstrate complete end-to-end solution. Partial demo or missing modules may result in deduction of marks or technical disqualification at tenderer's discretion.	**No separate marks — Mandatory Compliance Factor**	Solution overview, technical documents, supporting evidence
Technical Presentation by Bidder	Technical presentation covering the proposed approach and methodology for EASM, IR & EPM solutions, along with relevant client portfolio and implementation experience	**20**	-

Notes: -

- Only one experience will be counted for technical scoring in case of renewal or repeat orders from the same client organization.
- The vendor must achieve a **minimum cut-off score of 70 marks (70%)** in the technical evaluation stage to qualify for the financial bid opening.
- **100% compliance with all mandatory technical requirements** specified in the RFP is required to remain eligible in the evaluation process.
- All experience records, supporting documents, certificates, and evidence required for evaluation must be submitted as part of the eligibility-cum-technical bid.
- The bidder must demonstrate the proposed **EASM, DRM, EPM solutions through POC** and explain the **IR services approach and methodology** as per RFP requirements.
- SOC officials may conduct reference checks or physical site visits to validate claims made in the bid.
  If only one vendor scores 70 marks or above, the tendering authority may also consider the vendor with the next highest score to ensure competitive financial bidding.
- If none of the vendors meet the 70% cut-off, the tendering authority may shortlist the top two highest-scoring vendors at its discretion, subject to satisfactory demonstrations and reference checks.

5.2 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.

5.3 Award of Contract

i. Bid evaluation committee will evaluate and compare the bids determined to be substantially responsive. It is bid evaluation committee's intent to select the proposal that is most responsive to the project needs and each proposal will be evaluated using the criteria and process outlined in this section.

ii. Technical demonstration shall be examined by the bid evaluation committee and GSDC/GSOC/GIL with respect to compliance, completeness and suitability of the solution to

the project and only the bids which are complying to the requirements shall be considered as technically qualified.

iii. Only the bidders, who qualifies in Technical evaluation process successfully, will qualify for the financial bid evaluation.

iv. Shortlisted bidder quoting lowest bid value (L1) will be considered for final selection.

v. If the L1 Bidder is not agreed to execute the project for any reason, Tenderer may call L2 Bidder to match the price of L1. If L2 bidder agree to match the price of L1, tenderer may award the contract to L2 bidder to execute the Project.

Section: - 6 Financial Bid

6.1 Financial Bid for Comprehensive Scope of Work for RFP

Sr No.	Item Description	Quantity	Total Price (INR) (with tax)
1	Cost of External Attack Surface Management (EASM) Solution for the period of 2 years, extendable by 1 year. (As per Price Bid for EASM)	1	
2	Cost of Incident Response (IR) Services for period of 2 years, extendable by 1 year (Price Bid for IR -Indicative Pricing Format (Man-Hour Model)	1	
3	Cost of End Point Management Solution for 5 Years (As per Price Bid for End Point Management Solution)	1	
	Total (with taxes)		

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

6.2 Price Bid for EASM

Sr.	Description	One Time Cost (OTC)	Year 1 Cost (Rs.)	Year 2 Cost (Rs.)*	Year 3 Cost (Rs.)*	Total Cost (Rs.)	GST Amount (Rs.)	Total Amount (including GST) in Rs.
1	External Attack Surface Management – Annual Subscription Cost	X						
2	Digital Risk Monitoring – Annual Subscription Cost	X						
3	Additional Cost per Takedown beyond Minimum Included Takedowns (Unit Rate – Rs./Takedown)	X						
Total Cost of Ownership (TCO) (in Rs.)						0	0	0

Note: -

- Commercial Bid should be **strictly as per the Commercial Bid format**. Any commercial bid not in conformity or submitted along with the Eligibility-cum-Technical Bid shall be **rejected outright**.
- Commercial Bid must be submitted **without any deviations or alterations**.

- **Year 2 and Year 3 costs shall be quoted by the bidder** and will be considered for **TCO calculation**. However, it is **optional for the Tenderer** to avail the services beyond Years 2, extendable by up to **1 additional year**.
- Annual Subscription Cost shall include **all costs**, including but not limited to:
  - License/subscription charges
  - Support & maintenance
  - Operational services
  - Infrastructure/components required to meet RFP requirements
- **No value shall be entered** in fields marked as **"X"**.
- The cost quoted under Sr. No. 3 shall be a **unit rate per additional takedown**, applicable beyond the minimum number of takedowns included in the base DRM/EASM subscription.
- The Bidder shall provide **additional takedown services**, beyond the minimum number of takedowns included in the base EASM/DRM subscription, **as and when required by the Authority** during the contract period.
- Such additional takedowns shall be charged strictly **as per the unit rate quoted under Sr. No. 3 of Clause 6.2**, without any escalation or change in terms and conditions.

6.3 Price Bid for IR -Indicative Pricing Format (Man-Hour Model)

Sr.	Type of Service	Man-Hours (B)	Rate (₹ per Man-Hour)	Total Amount (₹)
1	Incident Response Retainer Services	100	₹ _____ / hr	₹ _____
2	Phase-1 IRRA incl. sensors / tools deployment	Max 40 hours	₹ _____ / hr	₹ _____
3	IRR Services – Remaining Hours (100 – IRRA Hours)	Balance Hours	₹ _____ / hr	₹ _____
	Total Contract Value (TCO)	100 Hours Total		₹ _____

Notes: -

- 8 (Eight) Man-Hours shall be considered as 1 (One) Man-Day.
- GST shall be applicable extra, as per prevailing Government norms.
- Prices quoted shall remain valid for a period of **6 months** from the bid closing date.
- No pricing information shall appear outside this Annexure.
- Travel, boarding, lodging, and logistics costs shall be included in the quoted rates.
- The Bidder must attach their **standard Terms & Conditions** along with the Price Bid.
- **In case services are required beyond the total contracted 100 man-hours, the Bidder shall quote the applicable per-man-hour rate for additional hours separately, which shall remain fixed for the contract period.**

6.4 Price Bid for Endpoint Management Solution

Sr.	Description	One Time Cost (OTC)	Year 5 Cost (Rs.)	Total Cost (Rs.)	GST Amount (Rs.)	Total Amount (including GST) (Rs.)
1	Endpoint Management Solution – Subscription / License / Support Cost	X				
2	Additional License Cost per Endpoint / Appliance (Unit Rate – Rs./Endpoint or Appliance)	X				
	Total Cost of Ownership (TCO) (in Rs.)	0	0	0	0	0

Notes:

- The quoted **EPM cost must include per-endpoint and/or per-appliance licensing**, subscription, support, and all components required to comply with the RFP.
- The **base cost (Sr. No. 1)** shall cover the minimum number of endpoints/appliances as specified in the RFP.
- If the number of managed endpoints or appliances **exceeds the specified threshold** during the contract period, the **incremental license cost** shall be applicable as per **Sr. No. 2 (unit rate)**.
- Prices shall be filled **only in the yellow-highlighted cells** of the Commercial Excel Sheet.
- **No values shall be entered** in fields marked as **"X"**.
- Year 5 cost represents the **entire warranty/support period** as defined in the Scope of Work and shall be considered for **TCO evaluation**.
- In case the number of managed endpoints and/or appliances exceeds the minimum quantity specified in the RFP during the contract period, the Bidder shall provide **additional endpoint/appliance licenses** on demand.
- The cost for such additional licenses shall be charged strictly **as per the unit rate quoted under Sr. No. 2 of Clause 6.4**, and shall remain valid for the entire contract duration.

SECTION 4: Payment Terms

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

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.
- 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.

SECTION – 5: Financial Bid

Sr No.	Item Description	Quantity	Total Price (INR) (with tax)
1	Cost of External Attack Surface Management (EASM) Solution for the period of **2 years**, extendable by 1 **year**.	1	
2	Cost of Incident Response (IR) Services for **2 year**, extendable by 1 **year.**	1	
3	Cost of End Point Management Solution for **5 Years**	1	
	Total (with taxes)		

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

5.3 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.

Forms & Annexures

Form-1: Proposal Covering Letter

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

Tender Ref No:

To
Deputy General Manager (Technical)
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:

Form-2: Bank Guarantee format for Earnest Money Deposit

To **Dated:**
General Manager (Software Development)
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: xxxxxxxxxxxxxxxxxx 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.

Form-3: PERFORMANCE BANK GUARANTEE

(To be stamped in accordance with Stamp Act)

Ref: **Bank Guarantee No.**
Date:

To,
General Manager (Software Development)
Gujarat Informatics Ltd.
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 it 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.

Form- 4: Format for Financial Summary of the Bidder

(Same should be furnished by the Chartered Accountant / Statutory Auditor on their letter head)

Average Annual Turnover of the Bidder

S. No	Financial Year	Annual Turnover (INR)
1.	Year 2021-22	
2.	Year 2022-23	
3.	Year 2023-24	
	[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.

Form-5: Certificate / Undertaking for Land border from Supplier

<Bidder Company Letterhead>

To
General Manager (Software Development)
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>>

Form-6: Certificate / Undertaking for Land border from OEM

To
General Manager (Software Development)
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>>

Compliance & Check list

Technical Requirement and Compliance Checklist for EASM

Technical Requirement	Compliance (Yes/No)	Bidder Remarks
General Requirements		
The bidder shall provide services including but not limited to External Attack Surface monitoring and management, Deep and Dark Web monitoring, Credential Leak monitoring, Data Leak monitoring, Cyber Threat Intelligence, Monitoring of hacker forums, Social Media Monitoring, Anti-Phishing protection, Brand monitoring and protection to detect threats for Government of Gujarat entities.		
The bidder shall provide a single unified console for GSOC officials to view threats, alerts, dashboards and reports across Surface, Deep and Dark Web, EASM, Brand Protection and Digital Risk Monitoring.		
The proposed platform shall support Multi-Factor Authentication.		
Continuity of services shall be ensured via DR setup.		
All user activity shall be logged and made available for audit.		
The platform shall support minimum 10 GSOC user logins.		
GUI must be intuitive and user-friendly.		
Cybersecurity news, alerts & threat reports shall be shared daily / weekly / monthly with summarized insights and recommendations.		
Visual dashboards, analytics & reporting required.		
24×7 support availability via portal, email & phone.		
Services must comply with CERT-In / GoI cybersecurity regulations & DPDPA requirements.		

External Attack Surface Management (EASM)

Requirement	Compliance	Remarks
Discovery of known & unknown assets of Govt. of Gujarat ecosystem including departments, PSUs, boards, agencies, third-parties		
Frequent (daily/weekly) updated data collection automated into console		
Vulnerability, risk & attack vector identification with mitigation recommendations		
Historical attack surface insight availability		
Passive scanning & continuous exposure monitoring		
Vulnerability & misconfiguration exposure of infrastructure, applications, ports, certificates		
Application security exposure analysis		
Detection of sensitive data leakage such as code/API exposure		
Change summary reporting of attack surface changes		
Ability to add/remove assets from console		
Asset tagging & classification		
Metadata & discovery attributes		
Identification and evidence path of asset discovery		

Continuous scanning without performance impact		
Remediation recommendations		
Identify anomaly or risky asset behaviour		
Notify changes in ports, certificates, infrastructure		
Detect website/app defacement attempts		
Third-party/vendor exposure analysis		
Detect cloud misconfigurations		
Web/mobile app OWASP analysis		
Shadow IT Asset Discovery		

Digital Risk Monitoring (DRM)

Requirement	Compliance	Remarks
Monitoring of brand abuse & impersonation (domains/social media/apps)		
Unlimited takedown support		
Browser blocking support		
Fake/typosquat domain discovery		
Credential leak detection		
Rogue app monitoring		
Fake news / misinformation monitoring		
Monitoring of attack sources, botnets, malware infrastructure		
Daily / weekly / monthly dashboards		
24×7 detection & response		
Capability to shut down malicious content globally		

Technical Requirement & Compliance Checklist for Incident Responses

Compliance Table

S. No.	GSOC Requirement	Compliance (Y/N)	Supporting Documents / Remarks
1	IR services must be delivered by a globally recognized OEM with minimum **10 years of experience** in cyber incident response engagements		
2	OEM must have proven experience managing **Advanced Persistent Threats (APTs)**		
3	OEM must have published **APT discovery and threat research** publicly; latest **five APT research reports** must be submitted		
4	OEM must have a minimum pool of **10+ cybersecurity experts stationed in India**, supported by a dedicated global incident response team Additionally		

	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)		
5	OEM must deploy **Incident Responders onsite within 12 hours** of incident notification by GSOC		
6	OEM must bring and utilize their **own tools, software and forensic devices** for live investigation		
7	Scope shall include but not be limited to: log analysis, configuration review, identification, containment & eradication, root cause identification, APT analysis, malware reverse engineering, endpoint/network/digital forensics, Purple & Red Team exercises, DB analysis (SQL/NoSQL)		
8	OEM must submit a **comprehensive incident investigation report** including: attack timeline, root cause, exploited vulnerabilities, payloads, lateral movement details, compromised data analysis, artifacts, IOCs, Sigma/YARA/SNORT/SIEM detection rules, MITRE mapping and remediation plan		
9	OEM must conduct investigation **onsite anywhere in India** as directed by GSOC		
10	OEM must appoint a **Single Point of Contact (SPOC)** for IR engagement		
11	Minimum **100 IR hours annually** included; scalable as needed		
12	Unutilized IR hours must be converted into **training, proactive assessments or professional certifications**		
13	**No logs, artifacts or data** shall leave GSOC premises; all analysis must be performed onsite		
14	**Remote response strictly prohibited** unless specially approved		
15	**Confidentiality to be enforced strictly**; no publication or sharing of any investigation detail externally without written approval of DST Gujarat		

Sr. No.	Requirement	Complied (Yes/No)	Remarks / Evidence Reference
1	Design, install, configure & commission latest EPM by OEM/OEM-authorized personnel with Proof of Design & Configuration		
2	All required servers, active & passive hardware/software provided without additional cost		
3	Full lifecycle management for Local & DR sites with multi-zone architecture, offline policy enforcement, secure updates & SIEM/EPM telemetry		
4	Complete installation within 45 days of GSOC hardware delivery		
5	Perpetual licensing for minimum 10 users		
6	Quarterly OEM health check, tuning, patching & integration validation		
7	5-year onsite comprehensive warranty from FAT clearance		
8	OEM version upgrades during warranty & replacement of EOS equipment at no cost		
9	Stable version operationalization within 10 days of release		
10	Updates/patches transferred via data diode (unidirectional)		
11	Agent reinstallation retains license post reformatting		
12	Operational issues resolved within 48 hours with RCA report		
13	No remote access; onsite engineer mandatory		
14	Minimum 7 days onsite training		
15	OEM/Bidder to provide hardware, OS & applications		
16	FAT within 30 days of installation; license start from FAT		
17	Additional licenses up to 25% at same cost & terms		
18	Bidder/OEM not blacklisted by any Indian organization		
19	Arbitration under Arbitration & Conciliation Act, 1996		
20	NDA signed ensuring GSOC data confidentiality		

Technical Features – Compliance Checklist for EPM

A. Agent & Architecture

Sr.	Requirement	Yes	Partial	No	Remarks
A1	Multi-tenant architecture				
A2	Agent supports Windows, Ubuntu, RHEL, CentOS, Rocky Linux				
A3	Works without AD dependency; supports AD integration				
A4	Agent deployment via GPO, scripts, tools, manual				
A5	Agent inclusion in gold image				
A6	End users cannot uninstall agent				
A7	Offline policy enforcement				
A8	Log caching & sync with SIEM				
A9	Native AES-256 encrypted communication				

B. Patch Management

Sr.	Requirement	Yes	Partial	No	Remarks
B1	Centralized patching via single UI				
B2	OS, App, DB, Middleware				
B3	Patch dependency analysis				
B4	Patch severity classification				
B5	Silent patch deployment				
B6	Custom patch policies & real-time status				
B7	Staggered & no-reboot patching				
B8	Auto patching of new systems				
B9	Patch rollback with monitoring				
B10	EOL/EOS patching where available				

C. Configuration Management

Sr.	Requirement	Yes	Partial	No	Remarks
C1	Enforce configuration baselines				
C2	Real-time drift detection & auto-remediation				
C3	Offline configuration enforcement				
C4	RBAC for configuration control				
C5	Versioning & rollback of configurations				
C6	Dynamic group-based policy				

	assignment				
C7	Registry & service control				
C8	Custom script deployment				
C9	FAT validation for config. management				

D–N (Software Distribution, Inventory, Remote Control, Security Policy, Device & File Control, Disk Encryption, Vulnerability Management, Application Control, Reporting, Integration, SBOM, QBOM)

Bidder to confirm compliance for each sub-feature as per RFP clause with documentary evidence, screenshots, OEM datasheets, or certifications.

Note: This checklist shall be used for technical compliance evaluation. Any deviation must be clearly highlighted with justification and supporting documents.