BPCL's Managed Security Services (MSS)

Document Type	BPCL Managed Security Service (MSS) Tender
Bid Type	Three part bid (Bid-Qualification, Technical & commercial)
CRFQ No	1000255452
Date of RFQ	17th May 2016
Pre-Bid Meeting	**27th May 2016, 15:00 Hrs.** at ERPCC Conference Room, BPCL, Sewree Installation, Sewree (E), Mumbai 400015.
Last Date for Submission of Bid	**07th June 2016, 15:00 Hrs.**

Subject : Managed Security Services

Dear Sir / Madam,

BPCL invites bids for **Managed Security Services**

1. You are invited to submit your offer in a three-part bid for the subject tender (CRFQ) as per the scope and deliverables outlined in the technical specifications and the terms & conditions contained in the tender document.

2. It is an e-tender. Please visit the website https://bpcleproc.in for participating in the tender and submitting your bid online.

3. Bidders are required to submit their bids in three part bids consisting as per the following, through E-Tender.

   a) Bid -Qualification Criteria (BQC) document (Part – I)
   This should contain required Bid Qualification Criteria documents /details/relevant proofs/evidences against each of the given Criteria.
   b) Techno-Commercial Bid (Part – II)
   This should contain detailed response to the scope, technical details, deliverables, Literature, Leaflets etc. including confirmation of Commercial terms and conditions of the tender.
   c) Price Bids (Part – III)
   This should contain Prices /Taxes against the bill of material as per the given format

4. The evaluation of the 3-Part bid will be as per the following process:

   a. First, BQC bid document of bidders (Part-I) will be evaluated and qualified bidders will be shortlisted.
   b. Techno-commercial bids (Part-II) of only those bidders, who qualify the BQC criteria, will be evaluated further. The bidders are then shortlisted as per the evaluation.
   c. Commercial bids (Part-III) of only those bidders, who qualify the techno-commercial criteria, will be opened and evaluated further.

5. "The tenderers shall submit an interest free Earnest Money Deposit of Rs.1.00 lakh (Rupees one lakh only) by crossed account payee Demand draft drawn on any nationalized/scheduled bank in favor of "Bharat Petroleum Corporation Ltd." payable at Mumbai. (Applicable only to unregistered vendors with BPCL.). EMD is exempted for MSME vendors and NSIC vendors subject to submission of the details of MSME Registration with Directorate of Industries or any other competent authorities and NSIC registration as applicable along with the technical bid.

   EMD of the unsuccessful bidder will be returned within due course after the evaluation of the price bid. EMD of the successful bidder will be returned only after successful execution of job against the Outline agreement/Purchase Order and submission of PBG (if applicable)"

6. You should submit your bid for Bid-Qualification document, Techno-commercial bid & Price bid through online. However, the instrument i.e. EMD in the form of Demand Draft and the Integrity Pact duly signed & stamped by authorized personnel of your company to be submitted in physical form on or before the due date and time of the tender.

7. BPCL does not take any responsibility for any delay in submission of online bid due to connectivity problem or non-availability of site and/or receipt of instrument i.e. DD and Integrity Pact in physical form due to postal delay or any other reason. No claims on this account shall be entertained.

8. Incomplete tenders shall be liable for rejection without seeking any further clarification. We also reserve the right to reject any or all tenders without assigning any reasons whatsoever.

Thanking you,

Yours faithfully,
For Bharat Petroleum Corporation Ltd.

Milind Mangalgiri
Sr. Manager IS (Procurement & Contracts)

General Instructions to Bidders on E-Tendering

1. Interested parties may download the tender from BPCL website (http://www.bharatpetroleum.in) or the CPP portal (http://eprocure.gov.in) or from the e-tendering website (https://bpcleproc.in) and participate in the tender as per the instructions given therein, on or before the due date of the tender. The tender available on the BPCL website and the CPP portal can be downloaded for reading purpose only. For participation in the tender, please fill up the tender online on the e-tender system. You can submit the bid only on https://bpcleproc.in. Prior to submission of bid, you need to register in the portal.

2. For registration on the e-tender site https://bpcleproc.in, you can be guided by the "Instructions to Vendors" available under the download section of the homepage of the website. As the first step, bidder shall have to click the "Register" link and fill in the requisite information in the "Bidder Registration Form". Kindly remember your e-mail id (which will also act as the login ID) and the password entered therein. Once you complete this process correctly, you shall get a system generated mail. Login in to the portal using your credentials. When you log in for the first time, system will ask you to add your Digital Signature. Once you have added the Digital Signature, please inform by by mail to the vendor administrator vendoradmin@bpcleproc.in with a copy to support@bpcleproc.in for approval. Once approved, bidders can login in to the system as and when required.

3. As a pre-requisite for participation in the tender, vendors are required to obtain a valid Digital Certificate of **Class IIB** and above (having both signing and encryption certificates) as per Indian IT Act from the licensed Certifying Authorities operating under the Root Certifying Authority of India (RCIA), Controller of Certifying Authorities (CCA). **The cost of obtaining the digital certificate shall be borne by the vendor**.

   In case any vendor so desires, he may contact our e-procurement service provider M/s. E-Procurement Technologies Ltd., Ahmedabad (Contact no. Tel: +91 79 4001 6868 & Tel: +91 22 2417 6419) for obtaining the digital signature certificate.

4. Corrigendum/amendment, if any, shall be notified on the site https://bpcleproc.in. In case any corrigendum/amendment is issued after the submission of the bid, then such vendors who have submitted their bids, shall be intimated about the corrigendum/amendment by a system-generated email. It shall be assumed that the information contained therein has been taken into account by the vendor. They have the choice of making changes if needed in their bid before the due date and time.

   Bidders are required to complete the following process online on or before the due date/time of closing of the tender:

   - Pre-Qualification Bid (Part-I)
   - Techno-commercial Bid (Part-II)
   - Priced Bid (Part-III)

5. Directions for submitting online offers, electronically, against e-procurement tenders directly through internet:

   - Vendors are advised to log on to the website (https://bpcleproc.in) and arrange to register themselves at the earliest, if not done earlier.

   - The system time (IST) that will be displayed on e-Procurement web page shall be the time considered for determining the expiry of due date and time of the tender and no other time shall be taken into cognizance.

   - Vendors are advised in their own interest to ensure that their bids are submitted in e-Procurement system **well before the closing date and time** of bid. If the vendor intends to change/revise the bid already submitted, they shall have to withdraw their bid already submitted, change / revise the bid and submit once again. **In case vendor is not able to complete the submission of the changed/revised bid within due date & time, the system would consider it as no bid has been received from the vendor against the tender and consequently the vendor will be out from tendering process.** The process of change / revise could be done any number of times till the due date and time of submission deadline. However, no bid can be modified after the bids submission deadline.

   - Once the entire process of submission of online bid is complete, they will get an auto mail from the system stating you have successfully submitted your bid in the following tender with tender details.

   - Bids / Offers shall not be permitted in e-procurement system after the due date / time of tender. Hence, no bid can be submitted after the due date and time of submission has elapsed.

   - No manual bids/offers along with electronic bids/offers shall be permitted.

6. For tenders whose estimated procurement value is more than Rs. 10 lakhs, vendors can see the rates quoted by all the participating bidders once the price bids are opened. For this purpose, vendors shall have to log in to the portal under their user ID and password, click on the "dash board" link against that tender and choose the "Results" tab.

7. No responsibility will be taken by BPCL and/or the e-procurement service provider for any delay due to connectivity and availability of website. They shall not have any liability to vendors for any interruption or delay in access to the site irrespective of the cause. It is advisable that vendors who are not well conversant with e-tendering procedures, start filling up the tenders much before the due date /time so that there is sufficient time available with him/her to acquaint with all the steps and seek help if they so require. Even for those who are conversant with this type of e-tendering, it is suggested to complete all the activities ahead of time. It should be noted that the individual bid becomes viewable only after the opening of the bid on/after the due date and time. Please be reassured that your bid will be viewable only to you and nobody else till the due date/ time of the tender opening. The non availability of

viewing before due date and time is true for e-tendering service provider as well as BPCL officials.

8. BPCL and/or the e-procurement service provider shall not be responsible for any direct or indirect loss or damages and or consequential damages, arising out of the bidding process including but not limited to systems problems, inability to use the system, loss of electronic information etc.

   In case of any clarification pertaining to e-procurement process, the vendor may contact the following agencies / personnel:

   For system related issues:

   M/s. E-Procurement Technologies Ltd at contact no. +91 79 4001 6868 / 022 2417 6419 followed with an e-mail to id support@bpcleproc.in & mumbai.support@abcprocure.com.

   For tender related queries:

   a. Mr. Anil Satpute of BPCL at contact no. 022-2417 6210 followed with an email to ID satputeak@bharatpetroleum.in
   b. Milind Mangalgiri of BPCL at contact no. 022-2417 6123 / 2415 2723 followed with an email to ID mangalgirim@bharatpetroleum.in

The responsible person of the tender is Milind Mangalgiri of BPCL at contact no. 022-2417 6123 / 2415 2723.

9. Integrity Pact (IP)

- Proforma of Integrity Pact as per attached **Appendix - I** shall be uploaded by the Bidder/s along with the technical bid documents, duly signed and stamped by the authorized signatory. All the pages of the Integrity Pact shall be duly signed and witnessed. Bidder's failure to upload the IP duly signed along with the bid documents shall result in the bid not being considered for further evaluation.
- If the Bidder has been disqualified from the tender process prior to the award of the contract in accordance with the provisions of the Integrity Pact, BPCL shall be entitled to demand and recover from Bidder Liquidated Damages amount by forfeiting the EMD/Bid Security as per provisions of the Integrity Pact.
- If the contract has been terminated according to the provisions of the Integrity Pact, or if BPCL is entitled to terminate the contract according to the provisions of the Integrity Pact, BPCL shall be entitled to demand and recover from Contractor Liquidated Damages amount by forfeiting the Security Deposit/ Performance Bank Guarantee as per provisions of the Integrity Pact.
- Bidders may raise disputes/complaints if any, with the nominated Independent External Monitor.
  Names/addresses/contact numbers of Independent External Monitors appointed to oversee implementation is as follows:
  Shri. Brahm Dutt
  1/8 Safdarjung Enclave, New Delhi - 110 029.
  Tel: 09871920282

Commercial Terms & Conditions

Pricing Type

i) The quoted rates (Price Validity) shall be valid for acceptance for the period of 90 days from the date of opening of price bid.
ii) Prices quoted by the bidder must be firm and final, and shall not be subject to any escalation whatsoever during the period of the contract.
iii) The contract period will be for three years from the date of signing of the contract.
iv) The Vendor should quote separately for Basic price, and taxes as applicable on the item quoted separately.
v) Variation in the rates for Statutory levies/ taxes / duties during the tenure of the contract for supplies/services within delivery schedule will be allowed only on the submission of documentary evidence from Government / Statutory Authorities and its acceptance by BPCL.

IV. Preamble:

This tender is ***Strictly Confidential***. It is being made available to your organization purely for the purposes of submitting Tender on the strict understanding that the information provided in this document will not be shown, read or passed on to any person who is not a current employee of your organization.

This tender document has been developed based on BPCL businesses and technology requirements. It remains sole property of BPCL and as such the contents of this tender shall not be shared by your organization with others. BPCL shall have the right to proceed with the project, or to decide alternate Solution Provider or execute the project by itself.

Should there be any breach of confidentiality at any time, BPCL shall have the right to disqualify the bidder and/or may initiate any disciplinary action as may deem fit.

1. Objectives

BPCL intends to procure Managed Security Services (MSS) on 24x7 basis in order to monitor, analyze security threats/Events and advise mitigation plan. We want to outsource the management of BPCL's Security Operation Center (SOC) with enhanced scope using offsite shared service model managed by a leading vendor offering the managed security services (MSS) in India. However actual configuration changes in our systems & devices will be carried out by BPCL internal teams. The contract shall be governed through defined service level agreement (SLAs).

The entire MSS shared manpower resources will operate at Security Operation Center (SOC) from Managed Security Service Provider (MSSP).

Requirement:

As part of the MSS contract the selected vendor will broadly deliver the following:

1.1. **Man power Resources:**

	Item description	Service Window (Hours)	Responsibilities	Operating Location
1	Technical Coordinator Service	8x6	Act as single point contact, coordination, SLA compliance, Reviews	Offsite/Onsite
2	Monitoring Service	24x7	Security device and event Monitoring & call logging	Offsite
3	Analyst Service	24x7	Analyzing and Advising	Offsite
4	SIEM Specialist Service	On demand (90 days over 3 years)	Consulting for SIEM configuration analysis, guidance, training, connector development and advanced configuration	Onsite
5	Tools (on subscription basis)	-	• Ticketing System • Change Management Process • Security Device Health Monitoring System	• Offsite • Offsite • Onsite
6	Anti-phishing and Anti-Rogue Services	24x7	Monitoring & takedown management	Offsite

1.2. Vendor should provide dedicated MPLS links between vendor's primary & DR SOC and BPCL's data centers at CDC, Sewree Mumbai and IDC, Greater Noida.

1.3. MSSP must have Disaster Recovery (DR) site for primary SOC to take care of any possible disaster that hits the operation at primary SOC. BPCL requires the MSSP's SOC & DR necessarily be located in different state in India.

1.4. The engagement should meet the following expectations:

- **24x7 Security Devices Monitoring:**

This ensures 24*7 monitoring of security devices covering all alerts, events, utilization status and availability and log the incidents.

- **Security Threats Monitoring:**

Vendor is required to monitor security threats / events using BPCL's existing SIEM tool and feeds from other sources like NCIIPC, CERT-In etc and Log the events.

- **Security Threats Analysis and Recommendation :**

Vendor is required to analyze all incidents logged by monitoring teams and recommend mitigation plan.

- **SIEM Specialist Service:**

Vendor is required to provide service of SIEM specialist on call basis.

- **Anti-phishing & Anti-Rogue Monitoring & Management:**

The vendor shall proactively monitor BPCL's websites for any phishing attempts and advise us about the incident with details along with action plan to take down the website.

- **Supply of tools**

The vendor should supply

i. Ticketing System,
ii. Change Management and
iii. Security Device Health Monitoring System as a service model.

- **Reporting to BPCL**

The vendor should prepare and share various reports as per annexure IV.

2. Scope of Work

The scope of work & specifications based on which the Security Operation Center (SOC) is to be implemented at BPCL's primary data center in Mumbai using Managed Security Services [MSS] as follows:-

a. Security Device Health Monitoring
b. Security Attack / Event Monitoring
c. Attack / Event analysis and submission of mitigation plan.
d. Anti-phishing and Anti-Rogue Monitoring & Management
e. Reporting and Dash board creation
f. Installation, implementation and configuration of required tools

2.1. Security Device Health Monitoring Service

- Vendor is to provide 24x7 Security Devices Monitoring service using resources working from their SOC.
- Vendor is to provide tool required for monitoring the health of security devices in scope. Tool is to be provided as a service and required to be commissioned in BPCL's premise.
- Vendor is to provide 24x7 event logging service using offered ticketing tool
- BPCL shall provide the required hardware on VMWARE platform. Bidder is to propose required VM specification for the supplied tools.
- Alerts are to be configured with threshold values approved by BPCL's team.
- In the beginning of setting up the MSS setup for BPCL, the vendor is expected to carry out the comprehensive health check of all security devices including SIEM and perform fine tuning wherever required to optimize the volume of events generated per day.

Device Monitoring & Providing Recommendations

- Managing security devices monitoring tool and carrying out required configuration and integration
- Capacity monitoring and advising on required hardware upgrade etc.
- Proactive status monitoring for availability and performance of the devices in scope
- Advise changes related to device alerts threshold configuration, monitoring, and logging functions
- Logging calls and follow-ups for recommendation implementation

Change Management Process

- Change management of security devices is to be handled by BPCL security team. Rule modification/creation and upgrade of SIEM is to be executed by BPCL team.

- BPCL team shall be able to use the change management tool of MSSP for registering the change request & obtaining the necessary approval before carrying out the change.

2.2. Security Attack / Event Monitoring

This service will cover following, but not limited to:

- 24x7 Security Attack / Event Monitoring in real-time using SIEM system
- 24x7 Logging Security Attack / Event using MSSP's Ticketing system
- Tracking the progress & updating the status
- Escalating call to next level for analysis, mitigation plan & implementation
- Execute call closure process and ensuring the availability of root cause analysis report in central knowledge base before closing the call.
- Alert for the viruses, worm, malware and any other security violation's activity observed at the security devices under scope including the follow-ups & call closure.
- Generate tickets for risks identified by 3rd party security agencies/VA-PT/NCIIPC/Vulnerability Scanner tool as & when shared by BPCL.

2.3. 24x7 Attack / Event analysis and submission of mitigation plan

This service will cover scope of work as follows, but not limited to:

- Attack / Event Analysis and recommending mitigation plan for implementation.
- Providing root cause analysis report as per SLAs
- Assist BPCL teams in resolving reported security incidents
- Liaison with respective BPCL internal team for implementation of trouble tickets as per defined SLAs.
- BPCL's existing SIEM system shall be used as the core tool for 24x7 Security monitoring & analysis service.
- Vendor shall extend the SIEM console to their SOC over secure network connectivity. Our existing security devices are integrated with SIEM.
- Analyzing advisories and providing mitigation plan on applicable advisories
- Recommendation for correlation rules to be provided on events across various logs of networks, systems, devices, applications etc.
- Timely notification and escalation of threats, anomalies and suspicious security events along with details of events and recommendation to mitigate the risk.
- Vendor is to provide inputs and technical knowhow to BPCL team on improving the monitoring processes, SIEM dashboards, reports and alerts during the contract period. The improvement areas are to be identified and action plan is to be discussed with BPCL team. BPCL team shall carryout the change in SIEM.

2.4 Continuous Improvement & Technical Consultation

- As a part of managed security services, the SIEM specialist service is to be provided to BPCL on call basis.
- Rule modification/creation and upgrade of SIEM is to be handled by BPCL's team.

BPCL's shall take professional services of SIEM specialist on call basis for following areas, but not limited to:

- Advanced configuration of SIEM rules & false positive elimination
- Create advanced dashboards & reports on SIEM
- Onboarding of new devices
- Risk assessment & audit SIEM tool
- Vulnerability scanner integration with SIEM
- Threat Intelligence (GTI) integration with SIEM
- Build custom connectors for log collection
- Incident life cycle management & risk mitigation

2.5 Technical Coordinator Service

Vendor shall provide 8x6 technical coordinator required to visit BPCL site as & when requested.

The scope of service include following but not limited to –

- 8x6 SPOC for overall SOC operation, coordination, and problem escalation.
- Monitor and manage SLAs as per contract
- Prepare and submit reports on deviations in SLAs and management summary
- Coordinate the regular reviews and technical discussions onsite & offsite
- Provide strategic directions to SOC team for security posture improvements
- Organize debriefing and takeaway sessions on major incidents encountered, complying with submission of different reports & dashboards/matrix etc.
- For major incidents, coordinate with the all stakeholders and collect forensic evidence etc. and prepare the report for submission to various authorities.
- Analyze security risks identified by 3rd party security assessment or vulnerability assessment tools and prepare risk mitigation plan.
- Vendor shall facilitate BPCL teams to implement the risk mitigation plan submitted by them.

2.6 Anti-phishing & Anti-Rogue Service

- The vendor shall proactively monitor BPCL's websites for any phishing attempt and advise BPCL about the incident with details of action plan.

Anti-phishing services will have following scope, but not limited to:

- Track hosting of phishing websites.
- Track new Domain Name Registrations to detect any spoofed or similar site being registered.
- Initiate and manage takedown of the phishing websites.
- Provide alerts on detection of phishing websites, daily status report on the phishing websites detected
- Provide Anti-rogue Services to detect and shut down rogue mobile apps on mobile stores.
- Vendor shall be liable for taking down the anti-phishing website & rouge applications. BPCL shall not have any liability caused due to false positive due to vendor's assessment and service execution.

2.7 Reporting and dashboard creation

- Vendor shall prepare and submit reports as per annexure – VI.
- Vendor shall submit the recommendation on creation of new dashboards and improvements.

2.8 Installation, implementation and configuration of required tools

- Vendor shall implement and integrate the tools with SIEM as per the scope.

2.9 Security Incidents Priority Classification

- Incident priority classification is to be considered based on the severity of events reported by SIEM tool of BPCL.
- All devices required for monitoring the security event/attack are integrated with central SIEM tool, working at BPCL's data center located at Sewree, Mumbai.

2.10 Vendor shall follow-up with respective stakeholders as per following schedule:

Service	**Critical: Priority 1 Calls**	**High: Priority 2 Calls**	**Medium: Priority 3 Calls**	**Low: Priority 4 Calls**
Security Device Health Monitoring	Follow-ups (update): 30 Min	Follow-ups (update): 90 Min	Follow-ups (update): 120 Min	Follow-ups (update): Same Day
Incident Management	Follow-ups (update): 30 Min	Follow-ups (update): 90 Min	Follow-ups (update): 120 Min	Follow-ups (update): Same Day

3. Evaluation Methodology

3.1. Bid Qualification Criteria for bidders

Bidders meeting the following criteria are eligible to submit their Bids along with supporting documents as per prescribed format. If the Bid is not accompanied by all the required documents supporting eligibility criteria, the same may be rejected:

Criteria-1: Bidder should be a registered company in India for providing IT Security Solutions under the Company Act 1956 and should have a valid registered office in India with a valid Service tax registration. Bidder should have minimum 3 years (2012-13, 2013-14, & 2014-15) experience in providing Managed Security Services (MSS) in India.

Required supporting documents: Bidder to provide copy of the following:

- Certificate of Incorporation and Memorandum & Articles of Association.
- Certificate of Service Tax Registration.
- Certificate from authorized signatory / Company Secretary of bidder indicating that they are providing Managed Security Services (MSS) in India for last 3 years during 2012-13, 2013-14, & 2014-15.

Criteria-2: Bidder should have minimum of 2 customers in India at present to whom they are currently providing Managed Security Services (MSS). For each customer, Bidder should be providing MSS covering the following:

a. Minimum 100 devices integrated with SIEM (Security Information & Event Management) for security event / attack monitoring & analysis
b. Minimum 10 security devices of at least 4 types from the following:
    i. Enterprise Class Firewall
    ii. Intrusion Prevention System (IPS)
    iii. Unified Threat Management (UTM)
    iv. Web gateway or Internet Proxy Server
    v. Anti-virus Server Management
    vi. Application Delivery Controller (ADC)

Required supporting documents: Bidder to provide copy the following as evidence against the criteria from at least two customers.

- Purchase Order, Invoice and list of devices (minimum 100 devices integrated with SIEM and 10 security devices) of two customers in India.
- Work implementation completion Certificate from these two customers along with contact person's name and phone number of each customer reference.

Criteria-3: The Bidder should own and operate Security Operations Centre (SOC) in India for at least last **3** years reckoned from the release of this tender.

Required supporting documents: Bidder to submit declaration on company letterhead duly signed by authorized signatory /Company Secretary furnishing following details of SOC, operating in India:

- SOC commissioning date,
- Location address, contact person name/email/phone number.

Criteria-4: Bidder should have disaster recovery (DR) for SOC located in different state in India other than the primary SOC.
Required supporting documents: Bidder is to submit declaration on company letterhead duly signed by authorized signatory / Company Secretary furnishing the details of location address, contact person name/email/phone number for the DR for SOC.

Criteria-5: Bidder should have valid ISO27001:2013 certified SOC in India as on tender release date.

Required supporting documents: Bidder is to provide copy of valid certificate.

Criteria-6: All resources required to run BPCL's Managed Security Services (MSS) In-Scope should be on bidder's payroll.
Evidence: Bidder to provide undertaking on letterhead duly signed by authorized signatory / Company Secretary confirming that all resources required to run BPCL's MSS In-scope shall be on bidder's payroll.

Criteria-7: Bidder should not have been be blacklisted by any of the Public Sector/ Central/State Governments or any Financial Institution in India.

Required supporting documents: Bidder to provide undertaking on letterhead duly signed by authorized signatory / Company Secretary that they are not currently blacklisted by any of the Public Sector/ Central/State Governments or any Financial Institution in India.

Criteria-8: Bidder should have average annual turnover of Rs 30.7 Lacs for last 3 financial years (2012-13, 2013-14, 2014-15) and during any of these 3 years the annual turnover should be at least Rs. 1.02 Crs.
Evidence: Bidder must submit the following:

- Copy of Audited Balance sheets/Annual reports for last three years (2012-13, 2013-14, 2014-15).
- Bidder should submit declaration on company letterhead duly signed by authorized signatory / Company Secretary furnishing the details that they have average annual turnover of at least Rs. 30.07 Lacs during last 3 financial years (2012-13, 2013-14, 2014-15) and during any of these 3 financial years the annual turnover is at least Rs. 1.02 Crs.

Criteria-9: Bidder should have positive net worth in last financial year (2014-15).
Required supporting documents: Provide audited balance sheet for last financial year (2014-15).

Bidders are required to qualify each of the above mentioned Bid Qualification Criteria to become eligible for the Techno-commercial bid evaluation.

3.2. Technical Evaluation Criteria

Technical bid will be accepted only if they are in the prescribed format in e-tender, with complete information and technical conditions have been complied with. Bidders qualifying the Bid –Qualified criteria shall be considered for technical evaluation:

i. Bidder shall submit CV's of minimum **15** Security professionals with CISSP/CISM/CEH/CCNP (Security)/ITIL certifications and minimum **5** professional with OEM certifications on Security devices (Firewall, IPS, SIEM, Secure Web Gateway).
ii. Bidder should submit names of the proposed SOC tools and documentary proof in support of functional specification and compliance as per Annexure-VIII.
iii. Bidder should submit resource sizing (manpower headcount and Bandwidth) as per the tender.
iv. Bidder must submit a declaration on company letterhead duly signed by authorized signatory / company secretary, that the bidder will retain the ISO 27001 certification for their SOC during the entire period of contract.
v. The Bidder has to make a technical presentation on the proposed architecture to BPCL team at Mumbai. Presentation should contain:

a. Proposed Services
b. Tools implementation & integration plan
c. Project execution Plan
d. Support Plan
e. Project Risk
f. BPCL obligations
g. Manpower resource plan
h. Incident Life Cycle Management Process & Workflow

3.3. Commercial Bid Evaluation

Price bids of Technically Qualified bidders will be evaluated using criteria of 'Overall Lowest Quote basis' considering quoted price of all the items / quantity mentioned in commercial bid format and applicable taxes.

4. Service Level Agreement

4.1 SOC operation team is to comply with Service Level Agreement (SLA) while handling calls related to any service of MSS contract. SLA includes both call response and resolution time (includes analysis and advising mitigation plan).

4.2 Call closure is to be done post submission of Root Cause Analysis (RCA) report.

4.3 The following escalation process to be followed:

Service	Critical: Priority 1 Calls	High: Priority 2 Calls	Medium: Priority 3 Calls	Low: Priority 4 Calls
Security Device Health Monitoring	**Fault, Configuration, Availability Management**			
	Response: 15Min			
	Communication Channel			
	Telephone and Ticketing System	Email, Ticketing System	Ticketing System	Ticketing System
Incident Management	Response: 15Min Resolution (mitigation plan): 1 Hour	Response: 30Min. Resolution (mitigation plan): 4 Hours	Response: 90Min Resolution (mitigation plan): 8 Hours	Response: 12 Hours Resolution (mitigation plan): Same Day
	Communication Channel			
	Telephone and Email, Ticketing System	Email, Ticketing System	Ticketing System	Ticketing System
Tools Uptime	**Tools Uptime Availability Management** SLA: 99.5% measured quarterly			
MSSP Network Link Uptime	MSSP Link Uptime Availability Management SLA: 99.5% (including both Link and required devices) measured quarterly			
Regulatory Security Advisory Management	Analyze NCIIPC/CERT-IN advisories & advise implementation plan and get logged in ticketing systems for BPCL's implementation teams.			
	Response: Within Two days (patch advisory) Same day (Malicious IP advisory)			
Anti-phishing & Anti-Rogue Management	24x7 Monitoring of BPCL's Web sites & Internet mobile stores			
	Response: 30 Min Submit detailed resolution plan with timeline: Within two days Plan must cover all steps including coordination activities with relevant 3rd parties and regulatory authorities for necessary website takedown & rogue mobile application shutdown. Follow-ups (update): 8 Hours			
Reports	Daily	Weekly	Monthly	Process Improvement
	By 9.30 AM:	By 1st day of each Week	By 1st day of each Month	As & when required
	Reports as mentioned in Annexure-VI	Reports as mentioned in Annexure-VI	Reports as mentioned in Annexure-VI	Prior to fortnightly review meeting

4.4 Vendor needs to strictly adhere to Service Level Agreements (SLA). Any SLA violation will attract penalties as per the terms of the RFP.

5. Penalty

5.1. Any deviation from SLA shall be measured on quarterly basis and corresponding penalties shall be recovered from next payment.

5.2. Every SLA violation related to Security Device Monitoring / security incident shall attract a penalty at the rate of **Rs. 500**/- per incident per hour and subsequent hours thereon.

5.3. For change of Technical Coordinator without BPCL's consent, BPCL shall deduct **Rs. 1000**/- per day till the replacement as per BPCL's requirement.

5.4. The maximum penalty shall not exceed **5% of total contract value.** In such scenario, the contract shall be refer to Project committee. The committee shall reserve the rights to terminate the contract fully or partly, by serving 30 days' notice.

5.5. The cumulative penalty for a **single year** shall be maximum **2% of contract value.** This penalty shall be calculated for a year on quarterly basis and shall not be carried forward to the next year.

5.6. All the penalties shall be recovered with applicable taxes.

Delay in operationalizing the services

5.7. For each week beyond or part thereof, the stipulated time frame, a penalty of Rs. **1000** shall be levied for each of the instances.

6. Payment Terms

- Payment shall be made quarterly at end of quarter (item no. 10 to 240) within 30 days from the date of submission of invoice.
- Payment for other charges (item no. 250 to 270) shall be paid on completion of activity duly approved by BPCL authority and submission of invoice on actuals.
- For tender evaluation cost of anti-phishing and anti-rouge services of 10 website would be considered. However, payment for line item 220,230 & 240 would be made as per actual consumption.
- The payment will begin after signoff of quarterly SLA reports submitted by the vendor which should be duly approved by BPCL designated authority.
- Bidder shall submit an undertaking on quarterly basis declaring the details of resources deployed by vendor for this project on bidders' letterhead with duly signed by vendor authorized signatory/ company secretary.
- Payment shall be made through NEFT.
- Variation Clause

As the implementation goes forward, if there are any major variations in the scope of work then the rates will be mutually agreed and settled.

BPCL along with the bidder will create a Design Review Committee which will review all change request created by the Project Team. They will analyse the impact of the change request on the project and will either approve or reject the same. BPCL and the bidder shall agree on the commercials during project preparation phase.

7. Other Terms & Conditions

7.1 Contract Period

- The contract shall be valid for **three years**, from the date of issue of Outline Agreement and it is subject to a review of performance at the end of every year.
- The successful bidder is to extend support for additional one year on demand by BPCL after expiry of three years contract period on same commercials, terms and conditions.
- BPCL reserve the rights to audit the MSS process at MSSP's SOC.
- PO for line item no.10 to 240 shall be issued yearly in the beginning of the year. PO for other items (250 to 280) shall be issued as and when services are required.
- Successful Bidder has to submit NDA (Non Disclosure Agreement) and TPOSP (Third Party Outsourcing Service Provider) Agreement within 15 days from date of placement of Out Line Agreement / LOI.
- Successful bidder has to enter into agreement with BPCL in line with Out Line Agreement on stamp paper within 15 days from the date of issue of Out Line Agreement.

7.2 **Start of Service**

- Within 45 days from date of OLA, vendor should setup MSS connectivity and finish onboarding activities which includes installation & configuration of tools, finalization of team etc.
- Standard operating procedures are to be prepared by MSSP before start of the services (45 days from date of OLA) in coordination with BPCL's team.
- Vendor to deploy resources within 15 days from the date of Purchase Order and start transition and setup process.
- Vendor needs to submit the CVs of proposed MSS team to BPCL within 10 days from the date of PO to identify the qualify candidate as per BPCL requirements.
- The responsibility of collecting all the required information pertaining to BPCL systems shall be with the vendor.
- All tools/software used by the Service Provider should be authenticated and licensed. Quoted Commercials shall include costs of all tools / software as per the specified criteria in this RFP. There shall not be any additional commercial implication on this account like TA/DA/ any other charges.
- Tools like ticketing, change management and security devices monitoring are to be installed, configured and integrated with BPCL setup by vendor to operationalize the MSS.

7.3 **Termination of Contract**

In case of any deficiency in the quality of services (as per the RFQ) rendered by the vendor, BPCL shall refer the tender to Project Committee. The committee reserves the rights to terminate the contract in whole or in parts at any time during the contract period by giving a written notice of one month to the vendor, for any valid reason, including but not limited to the following reasons:

a. Laxity in following security standards laid down by BPCL
b. Excessive delay in execution/ Inability to start the service more than 90 days from the date of Purchase Order / Outline Agreement / LOI placed by BPCL.
c. Discrepancies / deviations in the agreed processes and/or products. i.e.
    i. SLA deviation for number of response / resolutions instances exceeding more than 36 per year.
    ii. Unavailability of technical coordinator exceeding more than 30 days over a period of 3 years.
d. Violation of terms & conditions stipulated in this RFP

8. Performance Bank Guarantee (BG)

The selected bidder would be required to submit a performance Bank Guarantee to BPCL for an amount equivalent to 10% of basic order value within 15 days of purchase order issue date. The bank guarantee will be valid for period of 3 years.

The Performance Bank Guarantee is required to protect the interest of purchaser against the risk of non-performance of the successful bidder in respect of successful implementation of the project which may warrant the invoking of Bank Guarantee (BG).

9. Summary of Annexure

i.	Bill of Material	- Annexure - I
ii.	SOC's Tools & Specifications	- Annexure - II
iii.	SOC's Team Structure & Remote Connectivity	- Annexure – III
iv.	SOC's Team Members Profile & Selection Criteria	- Annexure - IV
v.	SOC Team resource Sizing	- Annexure - V
vi.	Reports & Integrated Dashboard	- Annexure – VI
vii.	Security Devices in Scope	- Annexure - VII
viii.	Technical Bid compliance sheet	- Annexure –VIII
ix.	NIL deviation Statement format	- Annexure – IX
x.	Integrity Pact	
xi.	NDA	
xii.	TPOSP	

ANNEXURE –I

Bill of Material

#	Line Item	Duration (in year)
A	**SOC Operation Charges**	
10	24x7 Monitoring Services	3
20	24x7 Security Analyst Services	3
30	8x6 Technical Coordinator	3
40	24x7 Anti-phishing & Anti-Rogue Monitoring for BPCL websites (10 No#)	3
50	Ticketing Tool (As a service)	3
60	Change Management Tool (As a service)	3
70	Security Device Health Monitoring Tool (As a service)	3
80	2 Mbps MPLS Network link from MSS SOC to BPCL DC and DR	3
B	**Other charges (need basis)**	
90	SIEM specialist Services (i.e. SIEM configuration, Advanced threat Analysis Modeling, etc.)	90 Days over 3 years
100	Ant-phishing takedown service charges per takedown	30 Events over 3 years
110	Anti-Rogue Shut down service per shutdown	30 Events over 3 years

ANNEXURE –II

SOC's Team Structure & Remote Connectivity

The dedicated separate pool of resources will be performing the BPCL's operation from offsite during the required service window on 24X7 basis. SOC's team sizing is to be proposed by MSSP considering the BPCL's requirement. BPCL has mentioned the minimum indicative headcount against the each manpower resource. Analyst team will analyze and recommend mitigation suggestions to BPCL's security & other internal teams for mitigation implementation. BPCL internal teams may require subject matter expert while implementing the mitigation suggestion proposed on case to case basis. Technical coordinator needs to plan and conduct such coordination activities with Specialist team on need basis.

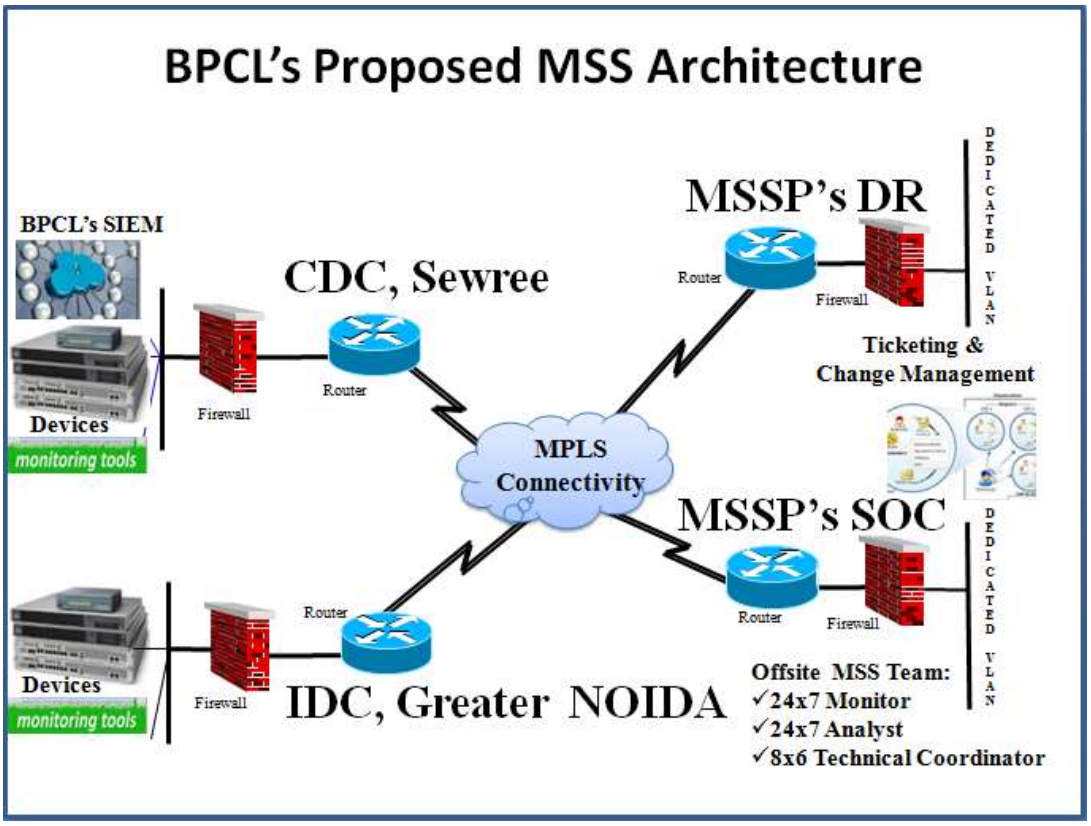
24x7 Security Attack / Event Monitoring and mitigation plan service is to be operated from offsite. The offsite operation is to be handled by identified & consistent shared pool of resources, fulfilling the requirements of BPCL's contract in terms of qualification, experience and professional certifications. Also, resources need to be completely familiarized with BPCL's IT environment and procedures as part of on-boarding exercise and during as & when there is any change in availability of resource pool members.

BPCL's internal teams will implement the mitigation suggestions provided by MSS team with the help of device specific OEM. However, if any specific details related to implementation is needed; technical coordinator will arrange it from MSSP's team.

Roles and responsibilities of Monitor, Analyst, SIEM Specialist and Technical Coordinator are given in scope of work.

MPLS connectivity of required capacity is expected to be commissioned & maintained by MSSP. BPCL's DC and DR located in Sewree, Mumbai and Greater NOIDA respectively are to be connectivity with primary & DR SOCs of MSSP. Vendor needs to submit the required link capacity estimation chart and connectivity implementation & failover plan. BPCL has provided the indicative link capacity required. The connectivity is to be protected against the cyber threats and unauthorized access using security devices like Firewall and IPS. BPCL's end network link shall be protected using BPCL's own security devices. Network link and network router are to be provided and maintained by MSSP.

The proposed SOC logical architecture diagram depicting connectivity and cross functioning of different groups of SOC team is as follows:


BPCL's Proposed MSS Architecture
BPCL's SIEM
Devices
monitoring tools
Firewall
CDC, Sewree
Router
MPLS
Connectivity
MSSP's DR
Router
Firewall
DEDICATED VLAN
Ticketing &
Change Management
MSSP's SOC
Router
Firewall
DEDICATED VLAN
Offsite MSS Team:
✓24x7 Monitor
✓24x7 Analyst
✓8x6 Technical Coordinator
Router
Firewall
IDC, Greater NOIDA
Devices
monitoring tools

ANNEXURE –III

SOC's Team Members Profile & Selection Criteria

24x7 Monitor: Required experience, skill sets and qualification is as follows:

1. Educational Qualification: Graduate in any discipline
2. Experience: Minimum total **3** years and **1** Year relevant experience in information Security
3. Should be able perform tasks listed in scope of service deliverables
4. Candidate with experience of technologies used in BPCL, like SIEM (furnish evidence) is must.

24x7 Analyst: Required experience, skill sets and qualification is as follows:

1. Educational Qualification: Bachelor of Engineering (Preferably Computer Science/ Electronics)
2. Experience: Minimum total experience **6** years & relevant Information Security experience **3** years (preferably in SOC operation)
3. Professional Certifications (mandatory to have at least one): CEH, CCNP (Security), CISSP, CISM.
4. Technology / Product Certifications (mandatory to have at least one): Firewall, NIPS, SIEM , Microsoft, Cisco, VPN, SAP, Redhat and VMware.
5. Should be able perform tasks listed in scope of service deliverables
6. Should be able to work in 24x7 service window

8x6 Technical Coordinator: Required experience, skill sets and qualification is as follows:

1. Educational Qualification: Bachelor of Engineering (Preferably Computer Science/ Electronics)
2. Experience: Minimum total experience **10** years & relevant information security experience **5** years (preferably in SOC operation)
3. Professional Certifications (mandatory to have min one): CISSP, CISM, ISO 27001, & ITIL
7. Technology / Product Certifications (Mandatory to have min two): Firewall, NIPS, SIEM , Microsoft, Cisco, VPN, SAP, Redhat and VMware.
4. Should be able perform tasks listed in scope of service deliverables
5. **Soft Skills**: Good written and oral communication, should able to drive the thought leadership for Information Security, able to convey the message in clear and crisp manner, impactful presentation skills, good listening skills, self-driven and self-motivated, dynamic personality, able to resolve conflicts between internal and external teams

SOC's Team Selection Criteria

I. Resources selected by prospective vendor before on-boarding, shall be screened by BPCL for their knowledge and competencies.
II. Prospective vendor should submit validated copy of all credential documents of candidates identified for carrying out the BPCL's services.
III. In case BPCL finds any behavioral / code of conduct or performance related issue, BPCL retains the rights to terminate the specific SOC team member from the resource pool identified for BPCL's services.
IV. In case SOC staff leaves the MSSP's team, replacement shall be trained for a period of two weeks by vendor. The vendor is to submit the credential documents of candidate to BPCL and arrange an interview by BPCL. The resource will only be inducted into resource Pool of BPCL after getting same approved by BPCL, post interview process.
V. Vendor is to ensure that all resources identified for BPCL's MSS must be permanent employees on their payroll.

ANNEXURE -IV

SOC's Tools & Specifications

Central Ticketing System for Security Incidents			
SL No	**Requirement**	**Compliance (YES / NO)**	**Evidence / Remarks**
1	Tool should be used for logging all security events and incidents.		
2	Tool should provide built-in call tracking and escalation work flow system.		
3	This tool should be of enterprise class.		
4	Tool installed in MSSP's SOC should be accessible by BPCL team.		
5	Tool should be installed, configured and maintained by MSSP. Tool should have provision for fixed IP address.		
6	Tool should integrate with Security health monitoring & BPCL's SIEM tools for automatic ticket generation process.		
7	Tool is to be provided as a service for the entire period of MSS contract.		
8	Vendor shall coordinate with BPCL team to integrate SIEM for real-time call logging in ticketing system.		
General			
9	One single web based tool to manage all MSS calls.		
10	Tool should comply with BPCL password policy.		
11	The system should maintain a tamperproof audit trail of all the tasks performed on the registered trouble tickets.		
12	Tool should be ITIL compliant		
13	MSSP's ticketing tool should have the flexibility to provide daily ticketing data to BPCL's Ticketing system using some methods like Web service integration, API integration or Excel data file upload utility etc.		
Functional			
14	Tool should provide customized reporting & dashboard.		
15	Should have provision to update detailed information about the asset inventory such as IT Asset owner, location, department, IP address etc.		
16	Should have provision for uploading the asset inventory in xls format or via database import		
17	Should have provision for data extraction and upload to BPCL's system.		

18	Should have end-to-end ticket tracking feature like assignment, assignee, data and time for reported, response and resolution etc.		
19	Should have search feature for incident, change, knowledge base etc.		
20	Should have granular access control of MSS tool based on defined roles and responsibilities.		
21	MSS vendor should have ticketing tool deployed in High availability mode.		
22	Tool should have following Incident management features: i. Logging ii. Classifying iii. Configurable escalation matrix iv. Distributing v. End to end management till resolution vi. Building knowledge base vii. workflow for assigning and tracking remediation activity of threats and vulnerabilities to respective asset owners		
23	Tool should have following Problem Management features: ✓ Process of identifying root cause ✓ Logging ✓ Escalation ✓ Problem management till resolution		
24	Tool should have following Integrated change management features: ✓ Change request creation ✓ Classification of severity of incidents ✓ Assessment & Assignment ✓ Approval workflow ✓ Execution		

Change Management Process tool			
SL No	**Requirement**	**Compliance (YES / NO)**	**Evidence / Remarks**
1	Tool should have pre-defined change management workflow process as per ITIL standard.		
2	This system requires being integrated with MSS central ticketing system.		
3	Tool should have provision to register change requests in this system.		
4	Tool installed on MSSP's SOC should be scalable and should have provision to be used by multiple teams of BPCL.		
5	Tool is to be provided as a service.		
6	Tool should flexibility to create multiple login accounts based on roles and responsibilities.		

General			
7	Compliance with the password security policy of BPCL		
8	The system should maintain a tamperproof audit trail of all the tasks performed on the registered change requests.		
9	Should have flexibility in registering the change requests and obtaining the approvals as per defined approval workflow matrix.		
Functional			
10	Should have following Change management features: ✓ Change request creation ✓ Assessment & Assignment ✓ Customizable Approval work flow ✓ Execution ✓ Email notification ✓ Emergency approval		
Administration			
11	User access interface provided to BPCL mush be secure (Encrypted Web UI based access).		

Security Devices Health Monitoring Tool			
SL No	**Requirement**	**Compliance (YES / NO)**	**Evidence / Remarks**
1	This tool is required to perform health monitoring of all security devices in-scope on premise.		
2	Tool is to monitor each security device at hardware / software component level (i.e. device interfaces, CPU/Memory load, Status, Battery status, Fan status, Throughput etc.) and raise an alert to MSS & BPCL's teams appropriately.		
3	This tool is required only for security devices. This tool is to be installed and implemented in BPCL's data center.		
4	MSS vendor is to provide the hardware resource requirement for this tool.		
5	Security Device Health Monitoring tool should be deployable on VMWARE platform. BPCL shall provide the required Hardware/OS resource on VM platform.		
6	Security Device Health Monitoring tool's perpetual license shall be in the name of BPCL. However, the MSSP shall maintain the Support / Administration Contract of tool back to back with OEM directly during the entire contract period.		
7	Tool is to be installed, configured and maintained by the MSSP.		
8	Tool is to be provided As a Service.		
General			
9	Compliance with the password security policy of BPCL		
10	Tool must be deployed without any agent on security devices.		
Functional			
11	Tool must provide Historical Monitoring Data Analysis.		
12	Tool must provide Device Availability Monitoring.		
13	Tool should provide Integration with Ticketing tool.		
14	Tool is to be configured for generating Email alert and notification		
15	MSSP needs to define the threshold parameters in coordination with BPCL for automatic generation of Alerts.		

ANNEXURE -V

SOC Team resource Sizing

Bidders are to carry out the sizing of MSS's resources to meet BPCL's requirements and provide the head count of each resource as follows:

#	Roles	Service Window (Hours)	Min No# of people as per BPCL's Estimation	Operating Location	Vendor's proposal for number of people (in numbers)
1	Technical Coordinator Service	8x6	1	Offsite/Onsite	
2	Monitor Service	24x7	4	Offsite	
3	Analyst Service	24x7	4	Offsite	
4	SIEM Specialist Service	On demand	1	Onsite	

Bandwidth sizing:

#	Description	Min bandwidth as per BPCL's Estimation	Vendor's bandwidth proposal in Mbps	Number of network links proposed
1	MPLS Network Link from MSSP's SOC to BPCL DC and DR	2 Mbps per link		

ANNEXURE –VI

Reports & Integrated Dashboard

SOC team is expected to generate and provide following reports, but not limited to, as per defined frequency & timeline:

#	Description of Reports	Frequency	Compliance / Remark
1	Service Management SLA Compliance	Monthly	
2	Operations Management – Total Incidents detected and Status	Daily	
3	Operations Management - Total Threat intelligence raised and Status	Daily	
4	Availability and Performance of devices	Monthly	
5	Executive summary report for management	Weekly	
6	Summary & the percentage of incident notification determined to be false positives	Monthly	
7	Summary & the average time to define as false positive or negative	Monthly	
8	Summary & the time needed to detect advanced attacks	Monthly	
9	User activity monitoring reports including: ✓ Account Lock-out events ✓ Failed log on activities ✓ Administrative access ✓ Blocked user account access	Daily	
10	Operations monitoring reports: ✓ Change request reports ✓ Configuration changes ✓ Operations overview reports ✓ Account management & user ✓ management reports	Daily	
11	Configuration change monitoring ✓ Top Configuration Changes	Daily	
12	Incident monitoring reports ✓ Top Targeted Ports ✓ Top Targets ✓ Top Attackers ✓ Attackers by geography ✓ Top Internal Attackers ✓ Top Destinations	Daily	
13	Security devices monitoring: Summarize the list of incidents, and security recommendations.	Daily	
14	Security devices monitoring: Summarize the list of incidents, security advisories, vulnerability management, and other security recommendations. It should include the	Monthly	

	operations trend analysis with the reports correlation of the present and past data.		

Vendor is expected to develop an integrated dashboard for BPCL team for the purpose of reporting, analysis and trending on overall MSS operation:

#	Feature Description	Compliance (Y/N, remark if any)
1	A provision for creating & maintaining an inventory of key IT assets that can be used for security risk assessment with respect to threats encountered	
2	A provision to select the assets from the IT Asset inventory for the purpose of assessing the current security state of asset, pending calls etc.	
3	A provision to upload 3rd party vulnerability assessment scan report for further analysis and implementation	
4	Provision to track & monitor open tickets progress throughout the life cycle till closure	
5	Provision to track affected IT assets by a specific vulnerability using collective intelligence of tools available	
6	A facility for asset owners and security managers to approve security exceptions along with expiry date for exception	
7	The solution should provide a facility for tracking remediation tasks/ security exceptions that cross their target/expiry dates	
8	A facility to have a comprehensive views on following, but not limited to: ✓ Overall vulnerability posture ✓ Open tickets along with age analysis ✓ Critical issue pending ✓ Summary status of all MSS services along with KPIs	

ANNEXURE – VII

Details of Security Devices in scope are as follows:

#	Service / Solution	Volumetric	
1	Firewalls	Enterprise Class Firewall	17 No#
		UTM	4 No#
2	Intrusion Prevention System	7 No#	
3	Internet Secure Web Gateways	4 No#	
4	Security Information and Event Management (SIEM)	1 No#	
5	Central Endpoint Antivirus Protection System	1 No#	
6	Application Delivery Controller	3 No#	
7	Indicative Servers and Devices(Integrated with SIEM)	400 Nos.	

ANNEXURE-VIII

Technical bid - Compliance Sheet

Please provide the following information as part of your RFP bid. All information required herein must be provided. Please upload this Compliance sheet along with the evidence during submission of your technical bid.

Sr. No.	Description	Evidence /Remark	Compliance (YES/ NO)	Remark
1	Submit CV's and certificate of minimum 15 Security professionals with CISSP/CISM/CEH/CCNP (Security) /ITIL certifications and minimum 5 professional of OEM certifications on Security devices (Firewall, IPS, SIEM, Secure Web Gateway, Microsoft, Cisco, SAP, VMware and Redhat).	Bidder must submit the following: • CVs & Copy of valid certificates of minimum 15 Security professionals with CISSP/CISM/CEH/CCNP (Security)/ITIL certification. • CVs & Copy of valid certificates of minimum 5 professionals of OEM certification on security devices (Firewall, IPS, SIEM, Secure Web Gateway, Microsoft, Cisco, SAP, VMware and Redhat).		
2	Submit Name of the proposed SOC tools and supportive documentary proof in support of functional specifications compliance.	Bidder must submit the details (spec, make and model) of following: • Details of Ticketing Tool • Details of Device Management Tool • Details of Change management tool • For Compliance Refer Annexure-IV • Submit Compliance as per Annexure VI.		
3	Submit resource sizing deployed for BPCL as per the tender.	Bidder must submit the following:		

		• CVs of manpower resource • Headcount of each manpower resource as per Annexure V.		
4	Submit a declaration on company letterhead duly attested by competent authority/ company secretary, that the bidder will retain the ISO 27001 certification for their SOC during the contract period.	Bidder must submit the declaration.		
5	Copy of the technical presentation specifying: i. Proposed Services & tools, ii. Project execution Plan, iii. Support Plan, iv. Project Risk, v. BPCL obligations	Bidder must submit the technical write-up.		
6	BPCL's RFP duly stamped & signed by the authorized signatory in token of acceptance of all terms & conditions mentioned in this document.	Bidder must submit the details of item compliance.		
7	Duly signed by 'Authorized signatory' an Integrity Pact (IP)	Bidder has to submit IP document before due date physically.		
8	Details of EMD	Bidder has to submit EMD before due date physically.		
9	List of Deviations, if any else submit NIL deviation statement (Specimen enclosed).	Bidder must submit the list of deviation, if any in given format.		

Commercial Bid Format

For setting up Security Operation Center of BPCL using Managed Security Services in scope, bidder should provide cost breakups for below mentioned line items:-

Sr. NO.	Description	Qty.	UOM	Total (excl. taxes)	Ser. Tax (per cent)	Ser. Tax Amt	Total (incl. taxes)
10	1st year MSS operation charges - 24x7 Monitoring Services	1	**Year**				
20	2nd year MSS operation charges - 24x7 Monitoring Services	1	**Year**				
30	3rd year MSS operation charges - 24x7 Monitoring Services	1	**Year**				
40	1st year 24x7 Security Analyst Services	1	**Year**				
50	2nd year 24x7 Security Analyst Services	1	**Year**				
60	3rd year 24x7 Security Analyst Services	1	**Year**				
70	1st year 8x6 Technical Coordinator	1	**Year**				
80	2nd year 8x6 Technical Coordinator	1	**Year**				
90	3rd year 8x6 Technical Coordinator	1	**Year**				
100	1st year Ticketing Tool (As a service)	1	**Year**				
110	2nd year Ticketing Tool (As a service)	1	**Year**				
120	3rd year Ticketing Tool (As a service)	1	**Year**				
130	1st year Change Management Tool (As a service)	1	**Year**				
140	2nd year Change Management Tool (As a service)	1	**Year**				
150	3rd year Change Management Tool (As a service)	1	**Year**				

160	1st year Security Device Health Monitoring Tool (As a service)	1	**Year**				
170	2nd year Security Device Health Monitoring Tool (As a service)	1	**Year**				
180	3rd year Security Device Health Monitoring Tool (As a service)	1	**Year**				
190	1st year 2Mbps Network Connectivity (Vendor to provide link capacity estimation) Charges for DC and DR - including required Routers	1	**Year**				
200	2nd year 2Mbps Network Connectivity (Vendor to provide link capacity estimation) Charges for DC and DR - including required Routers	1	**Year**				
210	3rd year 2Mbps Network Connectivity (Vendor to provide link capacity estimation) Charges for DC and DR - including required Routers	1	**Year**				
220	1st year 24x7 Anti-phishing & Anti-Rogue Monitoring for 10 BPCL websites. Please quote cost per website for a period of one year.	10	**Nos.**				
230	2nd year 24x7 Anti-phishing & Anti-Rogue Monitoring for 10 BPCL websites. Please quote cost per website for a period of one year.	10	**Nos.**				
240	3rd year 24x7 Anti-phishing & Anti-Rogue Monitoring for 10 BPCL websites. Please quote cost per website for a period of one year.	10	**Nos.**				
250	SIEM specialist - Services (i.e. SIEM configuration, Advanced threat Analysis Modeling, etc.) As and when required. (Estimate - 90 days over 3 years). Please quote rate per day	90	Day				
260	Ant-phishing takedown service charges per takedown (Estimate - 30 Events over 3 years). As and when required. Please quote rate per event	30	Event				
270	Anti-Rogue Shut down service per shutdown (Estimate - 30 Events over 3 years) As and when required. Please quote rate per event.	30	Event				

Format of NIL deviation Statement

<On bidder letter head>

This is to certify that, the specifications of the services which I/we have mentioned in the Technical Bid, and which I/we shall supply if I/we am/are awarded with the work, are in conformity with the specifications of the bidding document and that are no deviations of any kind from the requirement specifications.

Also, I/we have thoroughly read the bidding document and subsequent corrigendum. By signing this certificate, we hereby submit our token of unconditional acceptance to all the terms and conditions of the bidding document without any deviations.

I/we also certify that the price I/we have quoted is inclusive of all the cost factors involved in the end-to-end execution of the project, to meet the desired Standards/Requirements set out in the bidding document.

Thank you,

Signature:

Name of the bidder:

Authorized signatory/Company Secretary Designation:

Seal of the Organization:

Date:

Place: