Request for Proposal (RFP)

for

Selection of Vendor for

SECURITY OPERATIONS CENTRE (SOC) SERVICES

The Nainital Bank Limited
26th March 2019
RFP Reference - NTB/IT/SOC/2019/03/003

Table of Contents

1. Section I – Invitation to Bid

RFP No. NTB/IT/SOC/2019/03/003

The Nainital Bank Ltd.
Head Office,
Seven Oaks Building,
Mallital, Nainital, Uttarakhand - 263001

Dated:26.03.2019

The Nainital Bank Ltd. invites bids(Technical & Commercial) from eligible bidders which are valid for a period of 180 days from the last date of submission of bid date for "SELECTION OF SYSTEM INTEGRATOR FOR MANAGED SECURITY SERVICES TO RUN SECURITY OPERATION CENTRE (SOC) SERVICES WITH MANAGED, DETECTION AND RESPONSE (MDR) CAPABILITIES DESCRIBED UNDER SCHEDULE OF REQUIREMENTS READ WITH SERVICE DELIVERY METHODOLOGY, OF THIS RFP DOCUMENT FOR A PERIOD OF 5 YEARS."

Scope of Work	*SELECTION OF SYSTEM INTEGRATOR FOR MANAGED SECURITY SERVICES TO RUN SECURITY OPERATION CENTRE (SOC) SERVICES WITH MANAGED, DETECTION AND RESPONSE (MDR) CAPABILITIES DESCRIBED UNDER SCHEDULE OF REQUIREMENTS READ WITH SERVICE DELIVERY METHODOLOGY OF THIS RFP DOCUMENT FOR A PERIOD OF 5 YEARS.*	
Application Money	**Rs. 25,000/- (Rupees Twenty Five Thousand Only)**	*Application money has to be deposited as DD/PO* at the time of submission of Bid.*
EMD (Earnest Money Deposit) to be submitted	**Rs. 4,00,000/- (Rupees Four lakhs only)**	**Earnest Money Deposit (EMD) submitted in the form of DD/PO* or Bank Guarantee which should be valid for 6 months from last date for bid submission date to be deposited along with the bid.**(BG Format enclosed –clause 7.2)
Last date and time of submission of Bids		**15/04/2019 (1700 Hrs)**
Date and time of opening of Eligibility cum Technical Bids (envelope 1 and envelope 2)		**16/04/2019 (1100 Hrs)**

Interested parties may view and download the RFP Document containing the detailed terms & conditions, from the website www.nainitalbank.co.in

***DD/PO and Bank Guarantee should be made in favour of The Nainital Bank Limited and DD/PO be made Payable at Delhi.**

RFP Coordinator –Sunil Lohani, CISO
Contact No- 9870398868, 0120-2401083
e-mail- infra@nainitalbank.co.in

1.1. Document Control Sheet

Tender Reference No.	NTB/IT/SOC/2019/03/003
Name of Organization	The Nainital Bank Ltd.
Tender Type (Open/Limited/EOI/Auction/Single)	OPEN
Tender Category (Services/Goods/works)	Services
Type/Form of Contract(Work/Supply/ Auction/Service/Buy/Empanelment/Sell)	Supply/Service
Technical Evaluation(Yes/No)	Yes
Is Multi Currency Allowed	No(Only INR)
Payment Mode (Online/Offline)	Offline
RFP Issuance Date	26/03/2019
RFP Coordinator	Sunil Lohani, CISO Contact No- 9870398868, 0120-2401083 e-mail- infra@nainitalbank.co.in
Last date of receiving written request for clarifications before the pre-bid meeting	1700 Hrs. on 02/04/2019
Pre-bid meeting	1500 Hrs. on 08/04/2019 at THE NAINITAL BANK LTD., Regional Office, Naini Business Centre, 4th Floor, UPRNN Building, C-20/1A/7, Sector 62, Noida – 201 309. Uttar Pradesh
Last date and place of submission of RFP response (Closing date)	1700 Hrs. on 15/04/2019 at THE NAINITAL BANK LTD., Regional Office, Naini Business Centre, 4th Floor, UPRNN Building, C-20/1A/7, Sector 62, Noida – 201 309. Uttar Pradesh
Date and time and place of opening of Eligibility cum Technical Bids (envelope 1 and envelope 2)	1100 Hrs. on 16/04/2019 at THE NAINITAL BANK LTD., Regional Office, Naini Business Centre, 4th Floor, UPRNN Building, C-20/1A/7, Sector 62, Noida – 201 309 Uttar Pradesh
Date and place of Technical Presentation (Presentation will be given by the eligible bidder only)	24/04/2019 THE NAINITAL BANK LTD., Regional Office, Naini Business Centre, 4th Floor, UPRNN Building, C-20/1A/7, Sector 62, Noida – 201 309Uttar Pradesh
Contract Type (Empanelment/Tender)	Tender
Multiple Technical Annexure(s)	Yes
Quoting for all Technical Annexure is compulsory	Yes
Application Money	Rs.25,000/-(Rupees Twenty Five Thousand only)
Bid Security (Earnest Money Deposit)	Rs.4,00,000/- (Rupees Four Lakhs Only)
Bid Validity days	180 days from the last date for submission of bid
Location for Submission of Bid	THE NAINITAL BANK LTD., Regional Office, Naini Business Centre, 4th Floor, UPRNN Building, C-20/1A/7, Sector 62, Noida – 201 309Uttar Pradesh
Validity of Contract	Five years (may be extended at sole discretion of bank for next two years) from the date ofsigning the contract with the successful bidder.
Address for Communication	Vice President IT Department Nainital Bank Ltd Head Office, Mallital, Nainital -263001 (UK) e-mail - infra@nainitalbank.co.in

2. DISCLAIMER

Subject to any law to the contrary and to the maximum extent permitted by law, the bank and its Directors, Officers, employees, contractors, representatives, agents and advisors disclaim all liability from any loss, claim, expenses(including, without limitation, any legal fees, costs, charges, demands, actions, liabilities, expenses or disbursement incurred therein or incidental thereto) or damage, (whether foreseeable or not) ("losses") suffered by any person acting on or refraining from acting because of any presumption or information(whether oral or written and whether expressed or implied), including forecasts, statements, estimate or projections contained in this RFP document or conduct ancillary to it whether or not the losses arise in connection with any ignorance, negligence, inattention, casualness, disregard, omission, default, lack of care, immature information, falsification or misrepresentation on the part of the bank or any of it's Directors, officers, employees, contractors, representatives, agents, or advisors.

3. Section II: Instructions for Bid Submission

3.1. Executive summary of the project

The Nainital Bank Limited was established in the year 1922 with the objective to cater banking needs of the people of the region. Bank of Baroda, a premier nationalized bank, is managing the affairs of The Nainital Bank Limited since 1973. The Bank is having 139 branches operating in five states i.e. Uttarakhand, Uttar Pradesh, Delhi, Haryana and Rajasthan. Bank's Head Office is at Nainital, Uttarakhand and -3- Regional Offices are functioning at Delhi, Dehradun and Haldwani.

The total business of bank was Rs. 10722.09 crore as on 31/03/2018 registering a growth of 6.31% over previous F.Y. The Operating profit of Bank for 31/03/2018 stood at Rs. 97.68 crore.

The Bank is running with a Vision which states: "*To emerge as a customer centric National Bank & become the most preferred bank for its product, services, technology, efficiency & financials*."

The Brief RFP scope is mentioned below:

The Nainital Bank Limited is looking for the System Integrator (SI) for Managed Security Services to run Bank' Security Operation Centre (SoC) services with Managed, Detection and Response (MDR) capabilities in this RFP document, for a period of 5 years (which may be extended at sole discretion of the Bank for further period of 2 years) as under:

1. **Section V** **-Detailed Scope of Work**
2. **Section V, Point 5.1** **- Schedule of Requirements**
3. **Section III, Point 4.8** **-Deployment Models & Service Delivery Methodology**

3.2. Preparation of Bids

Bidder should consider clarification/corrigendum, if any published on bank's website related to the RFP Document before submitting their bids.

Please go through the tender advertisement and the RFP Document carefully to understand the documents which are required to be submitted as part of the bid. Please note the number of covers in which the bid documents have to be submitted, the number of documents - including the names and content of each of the document that are needed to be submitted. Any deviations from these may lead to rejection of the bid.

3.3. Submission of Bids

The bidder shall seal the original DD/PO or Bank Guarantee (BG Format enclosed –clause 7.2) as EMD and Application fees in form of DD/PO in envelope 1 along with other Pre-qualification documents. The Bidder shall mark its company/firm/LLP name and tender reference number on the back of the PO/Bank Draft before sealing the same. The address of The Nainital Bank Ltd., name and address of

the bidder and the Tender Reference Number shall be marked on the envelope. The envelope shall also be marked with a Sentence "NOT TO BE OPENED BEFORE the Date and Time of Bid Opening". If the envelope is not marked as specified above, THE NAINITAL BANK LTD. will not assume any responsibility for its misplacement, pre-mature opening etc.

The bidder shall deposit the **envelope in person in the tender box kept for this purpose at THE NAINITAL BANK LTD., Regional Office, Naini Business Centre, 4th Floor, UPRNN Building, C-20/1A/7, Sector 62, Noida – 201 309 (Reception area) on or before 1700 hrs**, on bid submission date.

3.4. Assistance to Bidders

Any queries relating to the RFP Document and the terms and conditions contained therein should be addressed to the RFP Coordinator indicated in the tender.

3.5. Cost to Bid

The Bidder shall bear all costs associated with the preparation and submission of its bid, including cost of presentation for the purposes of clarification of the bid or otherwise. The Bank, will in no case be responsible or liable for costs stated heretofore, regardless of the conduct or outcome of the Tendering process.

3.6. Contents of the RFP Document

The RFP Document is divided into following sections:

1. **Section I - Invitation for Bids**
2. **Section II - Instructions for Bid submission**
3. **Section III - General Conditions of the Contract, Service Level Agreement, Deployment Model& Service Delivery Methodology**
4. **Section IV - Bid Submission Format**
5. **Section V - Scope of Work**
6. **Section VI – Commercial Bid**

The Bidder is expected to examine all instructions, forms, terms & conditions, and scope of work in the RFP Document and furnish all information as stipulated therein.

3.7. Clarification on RFP Document

A prospective Bidder requiring any clarification on the RFP Document may submit his queries, through email, at the Bank's e-mail address i.e. ***infra@nainitalbank.co.in*** and as per schedule indicated in **Section I – Invitation for Bids.** The queries must be submitted in the following format (in Excel file,*.xls) only to be considered for clarification:

Sr.No	Page No.	Section No.	Clause No.	Reference/Subject	Clarification Sought
..	..	..	..	..	..

The Bank will only respond to queries submitted in the above format.

All queries on the RFP Document should be received on or before as prescribed by the Bank in Section 1 of this RFP Document. Bank's response (including the query but without identifying the source of inquiry) would be provided to respective bidders and shall be displayed in Bank's website and corrigendum (If any) would be uploaded on bank's website www.nainitalbank.co.in/english/tender.aspx Bidders are responsible for duly checking the above website for any clarification/corrigendum and Bank's response.

Note: Inputs/suggestions/queries submitted by bidders as part of the pre-bid queries and otherwise will be given due consideration by the Bank, however THE NAINITAL BANK LTD. is not mandated to accept any submission made by the bidder and nor the bidder will be given any written response to their submissions. If an input is considered valid by the bank the same will be accepted and incorporated as part of the corrigendum and shall be published on Bank's website.

3.8. Amendment of RFP Document

At any time prior to the last date for receipt of bids, the Bank, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the RFP Document through an amendment.

Amendments, if any will be notified in writing on bank's website www.nainitalbank.co.in under Tender Option and shall be binding on all bidders.

In order to provide prospective Bidders reasonable time in which to take the amendment into account in preparing their bids, the Bank may, at its discretion, extend the last date for the receipt of Bids.

3.9. Language of Bids

The Bids prepared by the Bidder and all correspondence and documents relating to the bids exchanged by the Bidder and the Bank, shall be written in **English language.**

3.10. Documents Comprising the Bids

The bid prepared by the Bidder shall comprise of the following components:

1. **Envelope 1 - Pre Qualification envelope**

   The Pre-qualification envelope, besides the other requirements of the Tender, shall comprise of the following: (The envelope should be marked as "Pre Qualification)"

   - Bid Submission Cover Letter
   - Bidder's Profile
   - Application Money in form of DD/PO in original
   - EMD (as mentioned in this RFP) shall be the DD/PO in original or Bank Guarantee (BG Format enclosed –clause 7.2) for EMD and must be submitted in a sealed envelope mentioning "EMD NTB/IT/SOC/2019/03/003" by Bid submission end date as mentioned in Section 1 – Invitation of Bids.
   - Compliance List of Documents.
   - Response to Eligibility criteria: Eligibility Criteria which should contain all the supporting documents asked for eligibility criteria.
   - Power of Attorney executed by the Bidder in favour of the Principal Officer or the duly Authorized Representative, certifying him as an authorized signatory for the purpose of this Tender.

2. Envelope 2 - Technical Bid envelope

The Technical Proposal shall include details such as all the Solution Components, Proposed Architecture, Technologies used, service delivery methodology, monitoring mechanism, Incident management process, SLA requirements etc. used as part of the solution. This shall include-:

(i) Eligibility Criteria Compliance with required documents.
(ii) Technical Solution Proposal with compliance against the specified technical requirements.

The Technical Bid, besides the other requirements of the Tender, shall comprise of the following: (The envelope should be marked as "Technical bid")

- Technical Bid Letter
- Bidder Solution, Methodology and Project Plan (Phase 1 & Phase 2 as defined in RFP Document)
- Requirement of Infra like hardware, OS, Software, bandwidth etc. separately for each phase.
- Cyber Security Technical Requirements compliances as per clause no. 8
- Supporting documents as required in technical score sheet
- All documents including Power point presentation in CD/DVD.

All documents should be signed and stamped by the authorized person.

3. Envelope 3 - Commercial Bid envelope

The Commercial Bid, besides the other requirements of the Tender, shall comprise of the following:(The envelope should be marked as "Commercial bid")

- Commercial Bid
- Commercial Bid Letter
- A standard format for submission of commercial (Section VI)bids has been provided with the RFP document to be filled by all the bidders. Bidders are requested to note that they should necessarily submit their commercial bids in the format provided and submission in any other format will lead to rejection of the bid.

Note -The offer may not be evaluated and can be rejected by the Bank in case of non-adherence to the format or partial submission of technical information as per the format given in the RFP Document. The Bank shall not allow/permit changes in technical specifications once the bid is submitted. Failure to submit the required information along with the Technical Offer could result in disqualification of the offer. It should be distinctly understood that in case of ambiguity or lack of clarity in the documents submitted by the bidders towards scoring criteria, the decision of the Bank is final for awarding the marks against each of the specified items. Hence, it is imperative that the bidder should submit all the documents / POs/ letters from other Banks with clarity of the services rendered. The Bank is not under any obligation to seek clarifications from the bidder in this regard, but will proceed to award marks on the basis of the documents submitted.

3.11. Bid Prices

The Bidder shall indicate in the proforma prescribed, the unit rates and total Bid Prices of the services,

it proposes to provide under the Contract. Prices should be shown as detailed in "Section VI" in RFP Documents.

In the absence of above information as requested, a bid may be considered incomplete and be summarily rejected.

The Bidder shall prepare the bid based on details provided in the RFP Documents. **It must be clearly understood that the Scope of Work (Section V) is intended to give the Bidder an idea about the order and magnitude of the work and is not in any way exhaustive and guaranteed by the Bank. The Bidder shall carry out all the tasks in accordance with the requirement of the RFP Documents and it shall be the responsibility of the Bidder to fully meet all the requirements of the RFP Documents.**

3.12. Firm Prices

Prices quoted in the bid must be firm and final and shall not be subject to any upward modifications, on any account whatsoever. However, the Bank reserves the right to negotiate the prices quoted in the bid to effect downward modification. The Bid Prices shall be indicated in Indian Rupees (INR) only.

The Commercial bid should clearly indicate the price to be charged and Taxes will be applicable as per actual. It is mandatory that such charges wherever applicable/payable should be indicated separately in **Section VI – Commercial Bid**. However, should there be a change in the applicable taxes, the same may apply.

3.13. Bidder Qualification

The "Bidder" as used in the RFP Documents shall mean the one who has signed the Tender Form. The Bidder may be either the **Principal Officer** or his duly **Authorized Representative**, in either cases he/she shall submit a certificate of authority. All certificates and documents (including any clarifications sought and any subsequent correspondences) received hereby, shall, as far as possible, be furnished and signed by the representative and the principal.

It is further clarified that the individual signing the tender or other documents in connection with the tender must certify whether he/she signs as the Constituted attorney of the firm, or a company.

The authorization shall be indicated by **written power-of-attorney** accompanying the bid.

The power or authorization and any other document consisting of adequate proof of the ability of the signatory to bind the Bidder shall be annexed to the bid.

Any change in the Principal Officer shall be intimated to THE NAINITAL BANK LTD. in advance.

3.14. Earnest Money Deposit (EMD)

The Bidder shall furnish, as part of its bid, an Earnest Money Deposit (EMD) of the amount Rs.4,00,000/- (Rupees Four Lakh Only).
The EMD is required to protect the Bank against the risk of Bidder's conduct which would warrant the security's forfeiture.

The EMD must be submitted, in form of DD/PO or Bank Guarantee (BG Format enclosed –clause 7.2)

valid for a period of -6- months from the last date of bid submission, of any Scheduled Commercial Bank favouring The Nainital Bank Ltd.

Unsuccessful Bidder's EMD will be discharged/ returned after award of contract to the successful Bidder. **No interest will be paid by the Bank on the EMD**.

The successful Bidder's EMD will be discharged upon the bidder executing the Contract, and furnishing the Bank Guarantee/security deposit. **No interest will be paid by the Bank on the EMD.**

The EMD may be forfeited:

a. if a Bidder withdraws its bid during the period of bid validity specified in the RFP; or

b. in the case of a successful Bidder, if the Bidder fails;

i. to sign the Contract in accordance; or

ii. to furnish Security Deposit/Bank Guarantee for contract performance.

3.15. Security Deposit

- The successful bidder will be required to submit Security deposit in the form of Bank Guarantee, favoring The Nainital Bank Ltd. equal to the 10% of purchase order value.
- Validity: Valid for the 60 Months (to be extended for further 2 years if contract is extended for further 2 years). The BG will be released after 60 months and/or extended period or execution of all pending Purchase Orders, whichever is later.
- In the event of termination, Bank may Invoke the Performance Bank Guarantee/Security Deposits, recover such other direct costs and other amounts towards direct damages from the Agency that may have resulted from such default and pursue such other rights and/or remedies that may be available to the Bank under law.

3.16. Period of Validity of Bids

Validity of bid will be 180 days from the last date of submission of bid. **Any bid of a shorter period may be rejected by the Bank as non- responsive.**

In exceptional circumstances, the Bank may request the Bidder(s) for an extension of the period of validity of bids upto 180 days more. The validity of EMD may also be extended if required. Any clarification or response thereto on extension of bid of period of bid submission or extension of period of validity of EMD shall be done as per clause 3.7 of this RFP document.

3.17. Format and Signing of Bid

The original and all copies of the bid shall be typed or written in indelible ink. **The original and all copies** shall be signed by the Bidder or a person or persons duly authorized to bind the Bidder to the Contract. All pages of the bid, except for un-amended printed literature, shall be initialed and stamped by the person or persons signing the bid.

The response to the bid should be submitted along with legible, appropriately indexed, duly filled Information sheets and sufficient documentary evidence as per Checklist. Responses with illegible, incomplete information sheets or insufficient documentary evidence shall be rejected.

The Bidder shall duly sign and seal its bid with the exact name of the firm/company/LLP to whom the contract is to be issued.

3.18. Revelation of Prices

Prices in any form or by any reason before opening the Commercial Bid should not be revealed, failing which the offer shall be liable to be rejected.

3.19. Terms and Conditions of Bidders

Printed terms and conditions of the Bidders will not be considered as forming part of their Bids. The terms and conditions mentioned the RFP will prevail.

3.20. Consortium

Consortium is not allowed.

3.21. Last Date for Receipt of Bids

Bids will be received by the Bank at the address specified under **Section I - Invitation for Bids** no later than the time and date specified in Section I -Invitation for Bids.

The Bank may, at its discretion, extend the last date for the receipt of bids by amending the RFP Document, in which case all rights and obligations of the Bank and Bidders previously subject to the last date will thereafter be subject to the last date as extended.

3.22. Late Bids

Any bid received by the Bank after the last date and time for receipt of bids prescribed by the Bank, pursuant to **Section I - Invitation for Bids, will be rejected.**

3.23. Modification and Withdrawal of Bids

No bid may be altered / modified subsequent to the closing time and date for receipt of bids. Unsolicited correspondences from Bidders will not be considered.

No bid may be withdrawn in the interval between the date for receipt of bids and the expiry of the bid validity period specified by the Bidder in the Bid. Withdrawal of a bid during this interval may result in the Bidder's forfeiture of its EMD.

3.24. Bidder's Address for Correspondence

The Bidder shall designate the official mailing address, place to which all correspondence shall be sent by the Bank.

3.25. Contacting the Bank

No Bidder shall contact the Bank on any matter relating to its bid, from the time of the bid opening to

the time the Contract is awarded.

Any effort by a Bidder to influence the Bank's bid evaluation, bid comparison or contract award decisions may result in the rejection of the Bidder's bid.

3.26. Opening of Bids by Bank

The Bank will convene a bid opening session as per time schedule where one representative from the Bidder, who has successfully submitted the bid, may participate. Subsequent to this, Bank will further evaluate the Bid of only those bidders whose Application fees, EMD and eligibility criteria is found to be in order.

3.27. Evaluation of Bids

Bank will evaluate the bids. Decision of the Bank would be final and binding upon all the Bidders.

The purpose of this clause is only to provide the Bidders an idea of the evaluation process that the Bank may adopt. However, the Bank reserves the right to modify the evaluation process at any time during the Tender process, without assigning any reason, whatsoever, and without any requirement of intimating the Bidders of any such change.

Bidder must possess the requisite experience, strength and capabilities in providing the services necessary to meet the Bank's requirements, as described in the RFP Documents. Bidder must possess the technical know-how and the commercial wherewith all that would be required to successfully Supply, Install, Configure, Maintain and Manage the Servers, Storage, Network, Cyber Security, etc.as part of the solution and also to provide the maintenance and management support services sought by the Bank, for the entire period of the contract. The Bidder's bid must be completed in all respect and covering the entire scope of work (Section V) as stipulated in the RFP Document.

3.28. Preliminary Examination

The Bank will examine the bids to determine whether they are complete, whether the bid format conforms to the Tender requirements, whether any computational errors have been made, whether required application money and EMD have been furnished, whether the documents have been properly signed, and whether the bids are generally in order.

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

3.29. Clarification

When deemed necessary, during the tendering process, the Bank may seek clarifications or ask the Bidders to make Technical presentations on any aspect from any or all the Bidders. However, that would not entitle the Bidder to change or cause any change in the substance of the tender submitted or price quoted.

THE NAINITAL BANK LTD. reserves the right to seek fresh set of documents or seek clarifications on the already submitted documents.

The proposal and all supporting documentation submitted by the Service Provider shall become the property of the Bank.

3.30. Evaluation of Eligibility Criteria

In this part, the bid will be reviewed for determining the Compliance of the general conditions of the contract and Eligibility Criteria as mentioned in the Tender. Any deviation for general conditions of the contract and eligibility criteria will lead to rejection of the bid.

Before opening and evaluation of their technical proposals, bidders are expected to meet all the general conditions of the contract and the eligibility criteria as mentioned below. Bidders failing to meet these criteria or not submitting requisite supporting documents / documentary evidence for supporting pre-qualification criteria are liable to be rejected summarily.

The bidder must possess the requisite experience, strength and capabilities in providing the services necessary to meet the requirements, as described in the RFP Document. The bidder must also possess the technical knowhow and the commercial wherewithal that would be required to successfully provide the SOC services sought by THE NAINITAL BANK LTD. for the entire period of the contract. The bids must be complete in all respects and should cover the entire scope of work (Section V) as stipulated in the RFP Document. The invitation to the bids is open to all bidders who qualify the eligibility criteria as follows:

ELIGIBILITY CRITERIA

Sr. No.	Clause	Documents Required
1	The bidder should be an established company registered under the Companies Act,1956/2013 or LLP/ firm/ Partnership firm under Partnership Act 1932 and is in operation in information technology for at least 7 years as on 31.12.2018 and should have their registered offices in India. The company/firm/LLP must be registered with appropriate authorities for all applicable statutory duties/taxes in India.	(a) Valid documentary proof of: Certificate of incorporation and Certificate consequent to change of name if applicable, Copy of Memorandum & Articles of Association, Registered Partnership deed and agreements, Certificate of commencement of business wherever applicable, CIN (b) Valid documentary proof of GSTN, TAN & PAN Registrations
2	a. The bidder's annual turnover should be at least (INR) 50 crores in each of the last three financial years in India. b. The bidder should have a positive net worth over the past 3 years in India. c. The bidder should have an annual turnover of atleast (INR) 10 crores in providing cyber security services in each of the last three financial years in India.	a. Certified copy of Audited Financial Statements for last 3 financial years - 2015-16, 2016-17, 2017-18. b. CA Certificate indicating turnover and net worth during last 3 financial years - 2015-16, 2016-17, 2017-18. c. CA Certificate indicating turnover from security services during last 3 financial years - 2015-16, 2016-17, 2017-18 in India.
3	The Bidder should have been managing a well-established own Security	Self-Declaration certificate, giving services details offered to BFSI/PSUs with relevant

	Operations Centre (SOC) including proposed SIEM tool in India for the past 3 years. The bidder should be offering SOC services to at least two BFSI (Banking, Financial services and Insurance) or PSU in India during last three years.	documents. Bidder must provide client reference like purchase orders etc. for confirming that it is providing SOC services including proposed SIEM tool.
4	The bidders organization should be ISO 27001 certified	Certified copy of Certificate issued by competent authority
5	The Bidder should not have been blacklisted by Govt. of India /Banks /PSU /BFSI/Govt. organization in India during last 3 years from the date of submission of bid.	Self-certification certificate duly signed by authorized signatory on Bidder's letter head.
6	The bidders should submit valid letter from all the OEMs confirming the following: • Authorization for bidder and Confirmation that the products quoted are not "end of life" for next 5 years from date of installation. • The bidder must be authorized partner of quoted OEM.	a. OEM Authorization Letter from all OEMs whose products are being proposed and confirmation letter that the products quoted are not "end of life" for next 5 years from date of installation b. MAF to be submitted as per point no. 5.2
7	Bidder shall provide the details of the SOC owned by them In India like the location, infrastructure, tools used, companies served, process and methodology, staff employed, availability of DR facilities etc.	Self-Declaration certificate, giving location details of the SOC owned by them in India along with details of the proposed location for Bank.
8	The bidder to provide declaration on its letter head that all the technical features highlighted as a part of technical scope are covered in totality in proposal submitted by the bidder.	Declaration from bidder.
9	Bidder to provide the declaration that any of its subsidiary or associates or holding company or companies having common directors or companies in same group promoters/management or partnership firms/ LLPs having common partners have not participated in bid process.	Declaration from bidder.

3.31. Evaluation of Technical Bids

Only those bidders who qualify all Pre-qualification / Eligibility Criteria requirements will be qualified for technical bid evaluation.

Technical presentation, will be a part of the process for evaluation of the bids.

The Bank reserves the right to reject a Product/Solution/Service if it is of an opinion that the offered product/service does not match the technical requirements /objectives specified in Technical Bid –

Bank's Requirements.

The technical bid will first be reviewed for determining the Compliance of the Technical bids with the Tender terms and conditions, Minimum/ Mandatory Technical requirements and the scope of work as defined in this tender.

Any bid found to be non-compliant to the mandatory Technical Requirements, Tender terms and conditions and the scope of work shall be rejected and will not be considered for further evaluation. Bids that are technically compliant would only be taken up for commercial evaluation.

Bidders should submit the Technical Specification compliance sheet as a part of technical bid.

If the bidder is found to be non-compliant to any of the mandatory technical specifications, then the respective bid would be summarily rejected without assigning any score.

Bidder is required to submit all the supporting documents as per the criteria mentioned in the Tender. Bank reserves right to summarily reject any bid which does not contain all the mandatory supporting document or may ask bidder to resubmit documents, the decision of Bank will be final and binding in this regards.

Bids that are technically qualified would only be taken up for commercial evaluation.

Bidders are required to comply with all the Technical Specifications as mentioned in Tender, no deviation will be accepted. Any deviation would be summarily rejected without assigning any score.

Bank reserves the right to disqualify any bidder based on any criteria considered relevant and its decision is binding. Representations, if any from disqualified bidders will not be entertained and will be summarily rejected. THE NAINITAL BANK LTD. will not respond to any query raised by bidders seeking reasons for rejection of the bid.

Technical Bids will be evaluated for the following broad parameters and a score would be given to each bidder by the Bank based on the scoring criteria mentioned below-

Criteria	**Evaluation Parameters/Credentials**	**Credentials for awarding score** (It should be clearly understood that in case of ambiguity or lack of clarity in the documents submitted, the decision of the Bank is final for awarding the marks against each of the specified items.)	**Max Marks**
1	Bidders no. of Years of experience in providing Managed Security Services(MSS) to run Security Operation Centre (SOC) services with Managed, Detection and Response (MDR) capabilities in India (As on 31.12.2018)	The marks to be awarded as per the credentials submitted in respect of clients serviced in India:	20
		20 Marks for 10 years and above	
		15 Marks for less than 10 years and more than or equal to7 years	
		10 Marks for less than 7 years and more than or equal to 5 years	
		05Marks for less than 5 years and more than or equal to 3 years	

		Please provide relative document like PO copies of the customers serviced fulfilling the mentioned criteria.	
2	The Bidder's experience in providing Managed Security Services(MSS) to run Security Operation Centre (SOC) services with Managed, Detection and Response (MDR) capabilities in India to BFSI/PSUs in India . (As on 31.12.2018)	The marks to be awarded as per the credentials submitted in respect of BFSI/PSUs serviced: 20 Marks for 5 BFSI/PSUs or above. 15 Marks for 4 BFSI/PSUs. 10 Marks for 3 BFSI/PSUs. 05 Marks for 2BFSI/PSUs Please provide relative document like PO copies of the customers serviced fulfilling the mentioned criteria.	20
3	No. of BFSI/PSUs where the proposed SIEM solution should have been providing SOC services in India during the last three years (As on 31.12.2018)	The marks to be awarded as per the credentials submitted in respect of BFSI/PSUs serviced: 20 Marks for 5 BFSI/PSUs or above. 15 Marks for 4 BFSI/PSUs. 10 Marks for 3 BFSI/PSUs. 05 Marks for 2BFSI/PSUs Please provide relative document like PO copies of the customers serviced fulfilling the mentioned criteria.	20
4	The bidder's inclusion in the Gartner or Forrester reports on Managed Security Services (MSS) or Managed Detection &Response Services (MDR) specifically in past 3 years (2018, 2017 & 2016)	The marks to be awarded as per the credentials submitted in respect of no. of years: 20 marks for past 3 years or more 15 marks for past 2 years 10 marks for past 1 year Please provide relative document of the Gartner or Forrester reports fulfilling the mentioned criteria.	20
5	Bidder's technical presentation showcasing Solution Description, Functionality, Architecture & Deployment model.	Maximum 10 marks	20
	Clarification in understanding of requirements	Maximum 10 marks	
	Detailed approach & methodology for providing Managed Security Services(MSS) to run Security Operation Centre (SOC) services with Managed Detection and Response (MDR) capabilities		
	Project Plan for installation and rollout of the solution in Phase 1 and 2 as mentioned in point no. 4.7 of RFP document.		
	Coverage of entire details as per scope of work with value add/proposition so as to ensure a complete effective and efficient security solution.		
	Operation and Maintenance services and Technical support desk for a period of contract.		

Further the Bank's officials would visit reference sites provided by the Vendor if deemed necessary.

Note:

- Banks include Scheduled Commercial banks, excluding RRBs, Cooperative Banks
- Terms – Bidder, Service Provider [SP], System Integrator and Vendor are used interchangeably
- The bidder is required to provide documentary evidence for each of the above criteria.
- The Bank shall verify the credentials submitted with the respective issuer and understand the credentials claimed for the purpose of evaluation and awarding marks
- The vendor to submit appropriate credentials [other than self- certification] in respect of each of the item
- The technical score will be allotted by Bank to each bidder against each section and will be considered final.

Method to calculate Scoring -

The bidder scoring the maximum score in the technical scoring shall be allocated T score of 100. T score of other bidders will be calculated as under: -

T score of current bidder =(Total of current bidder × 100) /Maximum Total

For Example-:

Bidder	Table Score	Maximum Total	T Score
A	80	80	100
B	60	80	(60*100/80)=75.00
C	70	80	(70*100/80)=87.50
D	61	80	(61*100/80)=76.25

Score will be considered up to two decimal places. Only the Bidder/s scoring minimum technical score (T) of 70% and above shall be considered as technically qualified and are further eligible for Commercial evaluation. Commercial bid will not be opened for technical dis-qualified bid.

3.32. Evaluation of Commercial Bids

Commercial bids submitted by only those bidders, who have qualified both pre- qualification and Technical evaluation, will be eligible for further evaluation.

The Commercial Bids of only those Bidders short listed from the Technical Bids by Bank will be opened in the presence of their representatives on a specified date and time to be intimated to the respective Bidders, and the same will be evaluated by Bank.

Bidders will be ranked as per the ascending order of value of their Commercial Bids.

The bidder with the lowest Total cost will be allocated L score of 100. The L score for other bidders will be calculated on the following basis:

L score of current bidder = (Cost of Lowest Cost bidder × 100) / Cost of Current bidder

For Example-:

Bidder	Cost	Minimum Cost	L Score
A	80	60	(60*100/80)=75.00
B	60	60	100
C	70	60	(60*100/70)=85.71
D	81	60	(60*100/81)=74.07

Score will be considered up to two decimal places.

Bidders quoting incredibly low or unrealistic high cost of items leading to unrealistic total value with a view to subverting the tender process shall be rejected straight away by Bank and EMD of such vendor will be forfeited. Any bid found to be unsatisfactory in terms of any of the evaluated parameters as mentioned may be rejected and will not be considered for further evaluation.

3.33. Final Bid Evaluation (Techno commercial bid):

The evaluation of the tender is based on QCBS (Quality and Cost Based Selection).

The Combined Final Score contains 60% weightage for technical evaluation and 40% weightage for commercial evaluation. Therefore, combined and final evaluation will be done on the following basis:

Proposals will finally be ranked according to their combined Techno commercial score (TC) based on the below mentioned formula:

TC = T*0.6 + L*0.4

Bidders will be ranked basis their Final Techno Commercial Score (TC) i.e. TC1, TC2, TC3…and so on, TC1 being the highest Combined Final Score.

The shortlisted bidder will be declared after thorough evaluation of commercial bid by Bank. During the evaluation if the Bank finds that the detailed commercial bid is not in order or not complete etc. then Bank will treat his bid as non- viable and same will be rejected, and EMD will be forfeited. In such case the next ranked techno commercial bidder will be considered for further evaluation and so on till a bidder is selected.

If any bidder withdraws his bid, at any stage after the submission of the bid, till the final evaluation or declaration of the final selected bidder, it will be declared a defaulting bidder and EMD of such defaulting bidder will be forfeited and THE NAINITAL BANK LTD. reserves right to blacklist such bidders for next three years from participating in any THE NAINITAL BANK LTD. tender. In such situation the tendering process will be continued with the remaining bidders as per their ranking.

If the bidder backs out after being declared as selected bidder, it will be declared a defaulting bidder and EMD of such defaulting bidder will be forfeited and THE NAINITAL BANK LTD. reserves right to blacklist such organization for next three years from participating in any THE NAINITAL BANK LTD. Tender. In such case the detailed commercial bid of next ranked techno commercial bidder will be evaluated,

a) If the detailed commercial bid is found in order, complete and its Techno commercial score (TC) is less than the withdrawing bidder, than this bidder will be declared as selected bidder and will provide services at its own mentioned rates.

b) Next ranked techno commercial bidder also backs out then the Bank will complete the tender process by following the same process again for other remaining techno- commercial ranked

bidders.

3.34. Bank's Right to Vary Scope of Contract at the time of Award

The Bank may at any time, by a written order given to the Bidder, make changes to the scope of the Contract as specified.

If any such change causes an increase or decrease in the cost of, or the time required for the Bidder's performance of any part of the work under the Contract, whether changed or not changed by the order, an equitable adjustment shall be made in the Contract Value or time schedule, or both, as decided by the bank and the Contract shall accordingly be amended. Any claims by the Bidder for adjustment under this Clause (Clause 3.34) must be asserted within thirty (30) days from the date of the Bidder's receipt of the Bank's changed order.

3.35. Bank's Right to Accept Any Bid and to Reject Any or All Bids

The Bank reserves the right to accept any bid, and to annul the Tender process and reject all bids at any time prior to award of Contract, without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for the Bank's action.

3.36. Notification of Award

Prior to the expiration of the period of bid validity (180 days from last date of bid submission or any extended period), the Bank will notify the successful Bidder in writing that its bid has been accepted.

The notification of award will constitute the formation of the Contract, requiring the successful Bidder to furnish Bank Guarantee, favouring The Nainital Bank Ltd. of 10% of the Work/Purchase Order Value for contract performance. Thereafter the Bank will notify each unsuccessful Bidder and will discharge its EMD.

3.37. Award of Contract

There will be only one vendor.

At the same time as the Bank notifies the successful Bidder that its bid has been accepted, the Bank will send the Bidder the Proforma of Contract.

Within 30 days of receipt of the Proforma of Contract, the successful Bidder shall sign and date the Contract and return it to the Bank along with the Bank Guarantee, favouring The Nainital Bank Ltd. of 10% of the Work/Purchase Order Value for contract performance

The contract period will be commencing from the date of signing of contract and will be valid for 5 years (which may be extended for next 2 years at sole discretion of the Bank).

Keeping in view the project commitment, THE NAINITAL BANK LTD. reserves the right to ask the vendor to add new features/ process or modify the existing solution to take care the service delivery

for matching the project requirements as and when required.

Vendor has to agree for honouring all tender conditions and adherence to all aspects of fair trade practices in executing the purchase orders placed by THE NAINITAL BANK LTD.

If the name of the system/service/process is changed for describing substantially the same system/service/process in a renamed form then all techno-fiscal benefits agreed with respect to the original product, shall be passed on to THE NAINITAL BANK LTD. and the obligations with THE NAINITAL BANK LTD. taken by the Vendor with respect to the product with the old name shall be passed on along with the product so renamed.

The Security Deposit shall be in the form of Bank Guarantee (BG) of any Scheduled Commercial Bank. Security Deposit should be valid for the entire period of 60 months and shall be renewed if required. Thereafter on satisfactory performance and completion of contract, the Security Deposit shall be refunded to the vendor without any interest.

THE NAINITAL BANK LTD. may, at any time, terminate the contract by giving written notice of -30- days to the vendor without any compensation, if the vendor becomes bankrupt or otherwise insolvent, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to THE NAINITAL BANK LTD. If at any point during the contract, if the vendor fails to, deliver as per the tender terms and conditions or any other reason amounting to disruption in service, the Termination and Exit Management clause to be incorporated in contract, will be invoked.

In case of any takeover/merger/acquisition/transfer of ownership of bidder, the responsibility for smooth transition to the new entity lies with the bidder.

3.38. Placing of Purchase Orders

Quantities mentioned in BoQ (Bill of Quantity) are indicative and THE NAINITAL BANK LTD. reserves the right at the time of award of purchase order to increase or decrease the quantity of goods and / or services from what was originally specified while floating the RFP without any change in unit price or any other terms and conditions.

For procurement of Hardware/software/solution/system/service the Bank will issue Purchase order and will be placed on the vendor in hardcopy format.

Objection, if any, on the Purchase Order must be reported to the Bank by the vendor within five (5) working days counted from the date of Purchase Order for modifications, otherwise it shall be assumed that the vendor has accepted the Purchase Order in toto.

If the vendor is not able to supply/deploy/operationalize the ordered Hardware/software system / service / process completely within the specified period, the penalty clause shall be invoked.

The decision of THE NAINITAL BANK LTD. shall be final and binding on all the vendors to this document. THE NAINITAL BANK LTD. reserves the right to accept or reject an offer without assigning any reason whatsoever.

3.39. Bank Guarantee for Contract Performance

Within thirty days of the receipt of notification of award from the Bank, the successful Bidder shall furnish the performance security in the form of Bank guarantee, favouring The Nainital Bank Ltd. valid for a period of 60 months from the date of Signing of Contract in accordance with the Conditions of Contract.

Failure of the successful Bidder to comply with the requirement mentioned in document shall constitute sufficient ground for the annulment of the award and forfeiture of the Bank Guarantee/Security Deposit. In case of exigency, if the Bank gets the work done from elsewhere, the difference in the cost of getting the work done shall be borne by the successful Bidder.

Performance bank Guarantee as per following schedule:

S.no.	Item	Value
1	Instrument	One single Deposit in the form of Bank Guarantee
2	Validity of Performance Bank Guarantee	Bank Guarantee to be submitted along with the Signed Contract and should be valid for a period of 60 months from the date of Signing of Contract.
3	Amount	10%of Purchase Order value

3.40. Confidentiality and Non-Disclosure of the Document

The RFP Document to be submitted by bidder is confidential and the Bidder shall ensure that anything contained in RFP Document shall not be disclosed in any manner, whatsoever.

The document contains information confidential and proprietary to the Bank. Additionally, the bidder will be exposed by virtue of the contracted activities to internal business information of the Bank and Associates. The bidder shall ensure that its employees shall maintain full confidentiality of the entire information. Disclosure, reproduction, transmission of this RFP, any amendment to the RFP, any specifications, plan, drawing, pattern, sample data or any part of the aforementioned information to parties not directly involved in providing the services requested could result in disqualification of bidder, premature termination of the contract and legal action against the bidder for breach of trust.

No media release/public announcement or any other reference to the RFP or any programme thereunder shall be made without written consent of the Bank. Reproduction of the RFP or any other written document without written consent of the Bank by Photographic, electronic or other means is strictly prohibited. The Successful bidder will be required to sign a Confidentiality and non-disclosure agreement with Bank.

3.41. Tender Related Condition

The Bidder should confirm unconditional acceptance of full responsibility of completion of job and for executing the 'Scope of Work' of this tender. This confirmation should be submitted as part of the Technical Bid. The Bidder shall also be the sole point of contact for all purposes of the Contract.

The Bidder should not be involved in any major litigation/arbitration that may have an impact of affecting or compromising the delivery of services as required under this contract. If at any stage of Tendering process or during the currency of the Contract, any suppression / falsification of such information is brought to the knowledge of the Bank then the Bank shall have the right to reject the bid or terminate the contract, as the case may be, without any compensation to the Bidder and/or claim for damages before the court of law, resulting from such rejection/termination as the case may be.

3.42. Rejection Criteria

Besides other conditions and terms highlighted in the RFP Document, bids may be rejected under following circumstances:

3.42.1 General Rejection Criteria

- Bids submitted without or improper EMD and/or Application Money.
- Bids received through Telex /Telegraphic / Fax/E-Mail will not be considered for evaluation.
- Bids which do not confirm unconditional validity of the bid as prescribed in the Tender.
- If the information provided by the Bidder is found to be incorrect / misleading at any stage / time during the Tendering Process.
- Any effort on the part of a Bidder to influence the Bank's bid evaluation, bid comparison or contract award decisions.
- Bids received by the Bank after the last date and scheduled time for receipt of bids as prescribed by the Bank.
- Bids without power of authorization and without any other document consisting of adequate proof of the ability of the signatory to bind the Bidder.

3.42.2 Technical Rejection Criteria

- Technical Bid containing commercial details.
- Revelation of Prices in any form or by any reason before opening the Commercial Bid.
- Failure to furnish all information required by the RFP Document or submission of a bid not substantially responsive to the RFP Document in every respect.
- Bidders not quoting for the complete scope of Work as indicated in the RFP Documents, addendum (if any) and any subsequent information given to the Bidder.
- Bidders not complying with the material technical requirement by way of functionality, specifications and General Terms and conditions as stated in the RFP Documents.
- The Bidder not confirming unconditional acceptance of full responsibility of providing services.
- If the bid does not conform to the timelines indicated in the bid.
- Bidder not scoring minimum marks as mentioned in Tender.

3.42.3 Commercial Rejection Criteria

- Incomplete Commercial Bid.
- Financial Bids that do not conform to the Tender's Commercial bid format.
- Total price quoted by the Bidder does not clarify regarding all statutory taxes and levies applicable.

- If there is an arithmetic discrepancy in the commercial bid calculations the Bank shall rectify the same at its discretion. If the Bidder does not accept the correction of the errors, its bid may be rejected.

3.43. Liquidated Damages

If the selected Bidder fails to complete the due performance of the contract in accordance with the specifications and conditions agreed during the agreement, the Bank reserves the right to recover LD @ 0.5% of the Total Charges per week of the yearly order value , subject to a maximum of 10 % of total charges as LD for non-performance/delayed performance.

LD is not applicable for delay due to reasons attributable to the Bank and Force Majeure. However, it is the responsibility of the Bidder to prove that the delay is attributable to the Bank or Force Majeure.
The selected Bidder shall submit the proof authenticated by the Service Provider and Bank's official that the delay is attributed to the Bank or Force Majeure along with the bills requesting payment. If the delay is attributable to the Bank or Force Majeure or any other circumstances beyond the control of the Service Provider, then the Bank will continue with the contract without claiming any Liquidated Damage. Bank reserves the right to adjust the penalty and Liquidated Damages if any against the Security Deposit.

3.44. Force Majeure

The Bidder or the Bank shall not be responsible for delays or non-performance of any or all contractual obligations, caused by war, revolution, insurrection, civil commotion, riots, mobilizations, strikes, blockade, acts of God, Plague or other epidemics, fire, flood, obstructions of navigation by ice of Port of dispatch, acts of government or public enemy or any other event beyond the control of either party, which directly, materially and adversely affect the performance of any or all such contractual obligations.

Provided either party shall within ten (10) days from the occurrence of such a cause notify the other in writing of such causes. Unless otherwise directed by the Bank in writing, the bidder shall continue to perform his obligations under the contract as far as possible, and shall seek all means for performance of all other obligations, not prevented by the Force Majeure event.

4. Section III – General Conditions of the Contract, Service Levels Agreement (SLA)& Deployment Model and Service Delivery Methodology

Quality: The quality supplied shall be as per approved sample / certified by Principal vendors. Material not confirming to given specifications will be rejected & it will be replaced by the vendor, free of cost. The material must be as per the detailed specifications listed out in BoQ and shall be as per standard engineering practice, relevant IS/ International code of practice, and shall be as per the Specifications as mentioned in RFP Document.

Statutory Laws: Vendor shall abide by all applicable statutory rules/regulations/notification regarding taxes, duties, labour etc., in force from time to time, also registration, labour laws, payments, ESIC, PF, insurance etc. Vendor shall coordinate for all these matters with concerned authorities directly.

Confidential Information: All information exchanged between the parties will be confidential. If the implementation project requires disclosure of, or receipt of, confidential information, such disclosure or receipt will be made with mutual agreement and may be with a separately executed MoU / Non-Disclosure agreement with Vendor by the Bank.

Extra Deviated Items: Any extra item like variation in quantity, deviated item should be executed only after getting the appropriate approvals with written confirmation, from the bank. At the time of submitting the invoice, all the documentary evidence of appropriate approvals for Extra / deviated Items / Variation in Quantities should be attached. Payments will not be made without proper approvals.

Arbitration: The Bank and the Bidder shall make every effort to resolve amicably, by direct negotiation between the respective Designated Officials of the bank and the Bidder, any disagreement or dispute arising between them under or in connection with the RFP and or contract thereafter.
If the designated official of the Bank and the Bidder are unable to resolve the dispute within -30- days from the commencement of such informal negotiations, they shall immediately escalate the dispute to their Senior Authorized Personal.

If within -30- days from the commencement of such negotiations between the Senior Authorized Personal designated by the Bidder and Bank, are unable to resolve their dispute amicably, in such case the dispute shall be settled finally by arbitration in Nainital, Uttarakhand, India under and in accordance with the provisions of the Arbitration and Conciliation Act, 1996 or any statutory modification or re-enactment thereof. The right to appoint arbitrator shall lie with the bank only.

Jurisdiction: The Jurisdiction for all disputes will be in the city of Nainital (Uttarakhand), India.

Safety: All the safety codes and the preventive measure for this type of work shall be strictly followed. All the personnel and staff shall be under the authority of Vendor, in case of any mishap which causes injury, disability or death on site or offsite during or after the duration of the project due to negligence of the staff of the vendor, this shall not be responsibility of Bank in any case. No Claims in this regards shall be paid by Bank.

4.1 Stipulated Time Schedule

The key milestone dates as anticipated by the Bank are-

Date of release of Purchase Order and project timelines viz-a-viz penalties-

Date of release of Purchase Order-**T day**
Purchase Order acceptance by successful bidder-**T+5 days**

Sr.	Roadmap as per phases mentioned under point no.4.8 of Section-III	Project Timelines i.e. "T"	Penalties	Remarks
1.	**Phase 1–** -List of requirements to be shared with the Bank. -Bank's readiness with requirements -Delivery, installation, configuration and commissioning of all of Managed Security Services as defined in RFP document.	-T+10 days -T+15 days -30 days from date of confirmation letter for bank's readiness	For any delay in operationalization beyond scheduled timelines, a penalty of 0.5% of yearly order value per week will be charged from successful bidder. For any delay less than a week, the penalty will be charged proportionately.	On Successful signoff by the THE NAINITAL BANK LTD. Authority
2.	**Phase 2-** -List of requirements to be shared by the bidder with the Bank. -Delivery, installation, configuration and commissioning of all of Managed Security Services as defined in RFP document.	-T+15 days -30 days from date of confirmation letter for bank's readiness for Phase 2		On successful acceptance and signoff

The Bidder shall perform the Services and comply in all respects with the critical dates and failure on part of the Bidder to meet the critical dates without prejudice to any other rights that the Bank may have, may lead to the imposition of such obligations as are laid down in the Delay and Deterrent Mechanism and/or levy of penalty and/or termination of the Contract at the discretion of the Bank.

4.2 Term and Extension of the Contract

The term of this Contract will commence from the date of signing of contract and will be valid for a period of five years (including both Phases1& 2) and may be extended for next 2 years at sole discretion of the Bank.

The Bank shall reserve the sole right to grant any extension to the term above mentioned and shall notify in writing to the Bidder, at least 6 months before the expiration of the Term hereof, whether it will grant the Bidder an extension of the Term. The decision to grant or refuse the extension shall be at the Bank's discretion.

During extended period (if any) if deemed appropriate (THE NAINITAL BANK LTD. reserve right to extend the agreement with Bidder), the term and conditions for SLA, penalty and Prices for services, AMC & Manpower shall remain same as given for 5th Year.

Where the Bank is of the view that no further extension of the term be granted to the Bidder, the Bank shall notify the Bidder of its decision at least 6 (six) months prior to the expiry of the Term. Upon receipt of such notice, the Bidder shall continue to perform all its obligations hereunder, until such reasonable time beyond the Term of the Contract within which, the Bank shall either appoint an alternative Bidder/service provider or create its own infrastructure to operate such Services as are provided under this Contract. In such scenario, the terms and conditions for SLA, penalty and Prices for services, AMC & Manpower shall remain same as given for 5th Year.

4.3 Prices

Prices quoted must be firm and shall not be subject to any upward revision on any account whatsoever throughout the period of contract. However, if there is any increase/decrease in taxes/

duties due to any reason whatsoever, after Notification of Award, the same shall be passed on to The Nainital Bank Limited.

The cost quoted should include the licensing, monitoring services rendered through the vendor's SOC on 24 x 7x365 basis.
The cost should include Integration of bidder's SIEM solution with the existing Bank's devices, as no Separate charges will be paid.
In any circumstances no other additional cost shall be payable by the Bank on account of any software / tools used by the Service Provider for rendering the services as required in the Tender. The bidder should make his own arrangement for providing such software / tools used at his own cost. The responsibility to ensure that only legal, authorized, licensed versions of software / tools provided by the bidder and used by its employees are used for extending the required services, lies solely with the bidder.
The Bank in no way be a part of any litigation arising out of using unauthorized software / tool used by the bidder/service provider.

4.4 Payment Schedule

Payments will be released only on satisfactory acceptance of the deliverables for each Task as per the following schedule (for both phases):

Sr. No.	Item	Payment Schedule	Deliverables
1	Managed Services	100% payment of OPEX in Arrear shall be made after completion of every Month.	Copy of single Bill to be submitted to bank, with the corresponding SLA Report

All Payments shall be made in Indian Rupees Only and shall be released by the Bank against the invoices raised by bidder within 30 calendar days given all the relevant documents are submitted timely and are complete in all reference.

Note:

- All payments will be made through electronic mode only.
- Payments should be subject to deductions of any amount for which the Bidder is liable under the tender conditions. Further, all payments shall be made subject to deduction of TDS (Tax deduction at Source) as per the applicable Income-Tax Act.

4.5 Service Level Agreement (SLA) & Targets

SLA as described under point no.4.6, provides for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof. The Vendor shall ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the performance levels.

The services provided by the Vendor shall be reviewed by the THE NAINITAL BANK LTD. on quarterly basis and THE NAINITAL BANK LTD. shall:

- Check performance of the Vendor against this SLA over the review period of 3 month and consider any key issues of the past period's performance statistics including major incidents, service trends, etc.
- Discuss escalated problems, new issues and matters still outstanding for resolution.
- Review of statistics related to rectification of outstanding faults and agreed changes.
- Obtain suggestions for changes to improve the service levels.

In case, if desired, THE NAINITAL BANK LTD. may initiate an interim review to check the performance and the obligations of the Agency. The Bank will conduct quarterly review of the services rendered by the Service Provider at mutually agreed schedules, dates and representatives from both the Bank and Service Provider should attend such performance review meetings. The SLA may be reviewed periodically i.e. quarterly and revised, if required.

The Bank shall have the right to inspect / audit the SOC, Tools, Techniques and procedure adopted by the Service Provider in line with security activity outsourced by the Bank, independently or through the outsourced experts and call for detailed report without compromising the Service Provider's Security.

The SLA takes into consideration the following aspects-

1. Equipment Availability Related Service Levels
2. Technical Support desk Services
3. Compliance and Reporting Procedures

The following measurements and targets shall be used to track and report performance on a regular basis. The targets shown in the following table are applicable for the duration of the contract.

4.6 Service Level Agreements*

<table>
<tr><th>S N</th><th>Service Area</th><th>Service Level</th><th>Penalty</th></tr>
<tr><td>1.</td><td>Monitoring & Incident Alerting</td><td>Log Analysis Services

24x7 monitoring of all in-scope devices. Categorization of Incidents into Critical, High, Medium and Low priority shall be carried out in consultation with the selected bidder during the contract period.

All Critical, High and Medium priority incident should be logged as incident tickets and alerted as per SLA.

1 Critical incident within 15 minutes of the event identification.
2 High priority incident within 30 minutes of the event</td><td>
<table>
<tr><td colspan="2">1) Critical incident within 15 minutes
2) High priority incident within 30 minutes
3) Medium priority incident within 60 minutes</td></tr>
<tr><td>97.5% and above</td><td>N.A.</td></tr>
<tr><td>95% to 97.49%</td><td>1% of monthly payment</td></tr>
<tr><td>92.5% to 94.99%</td><td>3% of monthly payment</td></tr>
<tr><td>90% to 92.49%</td><td>5% of monthly payment</td></tr>
<tr><td><90%</td><td>25 % of monthly payment</td></tr>
</table>

Threshold: SLA compliance measured per month</td></tr>
</table>

<table>
<tr><td></td><td></td><td>identification.
3 Medium priority incident within 60 minutes of the event identification</td><td></td></tr>
<tr><td>2.</td><td>Incident Investigation Reports</td><td>Sending out detailed investigation report post alert notification. Action plan/ mitigation steps should be alerted to designated bank personnel as per the below SLA:

1 Critical incident within 60 minutes of the event identification.
2 High priority incident within 90 minutes of the event identification.
3 Medium priority incident within 180 minutes of the event identification</td><td>1) Critical incident within 60 minutes
2) High priority incident within 90 minutes
3) Medium priority incident within 180 minutes
<table><tr><td>97.5% and above</td><td>N.A.</td></tr><tr><td>95% to 97.49%</td><td>1% of monthly payment</td></tr><tr><td>92.5% to 94.99%</td><td>3% of monthly payment</td></tr><tr><td>90% to 92.49%</td><td>5% of monthly payment</td></tr><tr><td><90%</td><td>25 % of monthly payment</td></tr></table>Threshold: SLA compliance measured per month</td></tr>
<tr><td>3.</td><td>Network Threat Hunting Report</td><td>Once in 24 hours</td><td>N.A.</td></tr>
<tr><td>4.</td><td>Reports Dashboard</td><td>• Daily Reports: By 10:00 AM everyday
• Weekly Reports: By 10:00 AM, Monday
• Monthly Reports: 5th working day of each month</td><td>Threshold: SLA compliance 95%, measured per month

Penalty: 3% of monthly payment.</td></tr>
<tr><td>5</td><td>Service uptime</td><td>• 99.5% and above
• 98% to 99.4%
• 95% to 97.99%
• 90% to 94.99%
• Less than 90%</td><td>No penalty
3% of monthly billing
5% of monthly billing
10% of monthly billing
100% of monthly billing</td></tr>
</table>

*SLA may be changed by the bank at its discretion during signing of agreement with the qualified bidder.

Maximum penalty in a month will be capped to 25% of monthly SOC operations charges except service uptime.

4.7 Deployment Models & Service Delivery Methodology

The Bank is envisaging a model that will be a combination of onsite and remote services offered by the Bidder. Remote services shall be offered by the Bidder from their own Security Operations Centre (SOC). Onsite service shall include deployment of one (01 no.) resource (L2 level) for coordinating incident management, at Bank's preferable premise at Delhi NCR during business hours (10 am- 6 pm; Monday to Saturday).

Bidder to note that currently the Bank has its Data Centre hosted at Mumbai and DR Centre at Hyderabad. However, in future the hosted Data Centre & DR location may change subject to RFP (NTB/IT/INFRA/2018/12/002) notified for selection of vendor for DC DR Services. Therefore, the deployment of SoC Services in the Bank is divided into two phases which is described below-

Phase 1-
The vendor shall deliver the Security Monitoring Services by deploying a model in which the log collector is deployed at bank's premise and other components like log storage, correlation and monitoring happens at bidder's SOC. Log Storage shall be done at bidder's SOC as well other components such as SIEM/ Rules & correlation engine, Advanced Detection, triggering & response platforms are at bidder's SOC. Bidder will have to provide a declaration that bank's log data are stored within India boundaries and under no circumstances shall leave country's jurisdiction.

Phase 2-
Bidder to note that, bank at any point of time within six to twelve months from Phase 1, may ask bidder to change the log storage requirement from bidder's SOC to bank's hosted data Centre (which is under process through RFP). Under this phase, log collectors & central log manager (for log storage) shall be deployed at Bank's Premises i.e. hosted DC and DR and other components such as SIEM/ Rules & correlation engine, Advanced Detection, triaging & response platforms remains at bidder's SOC. Under such condition, all necessary hardware which is required to be at on-premises (hosted DC DR) will be arranged by the bank.

The SOC Service price including one time charges under this phase needs to be separately mentioned, as described in the commercial section (Section VI).

In the above phases the management of devices, platforms & 24x7 monitoring, incident analysis etc. shall be performed from vendor's SOC.

In any case bank shall not procure any SIEM license required for setup.

Bidder to consider near DR and far DR requirements in the proposed design since the monitoring service is required for devices installed at Bank's near DR and far DR site as well.

Bidders should clearly mention the type of technologies to be used for creating the SOC setup for the bank such as SIEM & other related technologies.

Any interfaces/custom connectors required for integration be developed by the bidder for successful implementation of the SOC at no extra cost to the bank.

Vendor to provide support to the Bank's team in integration of the in-scope devices & identification of correct log baselines & configuration changes required for effective correlation & monitoring.

Overall scope to ensure full coverage of 24*7*365 log monitoring aspects of various security solutions, devices, software, applications like firewalls, network intrusion prevention systems, WAF, DAM, PIM, DLP, Anti-DDOS, Anti-APT, Deception, etc. and critical network security devices at the Data Centres, DR Site (near DR and far DR), branches and other locations identified by Nainital Bank. Scope involves on-boarding of such devices to the monitoring platform, transition to new devices, at no additional cost to the Bank.

Development and implementation of processes for management and operation of the SOC including (but not limited to) the following processes:

- Configuration and Change Management
- Incident triaging and Escalation management processes
- Daily standard operating procedures
- Training procedures and material
- Reporting metrics and continuous improvement procedures
- Data retention and disposal procedures
- BCP and DR plan and procedures for SOC

4.8 Business continuity

The bidder shall be responsible for defining a DR/ BCP plan for the SOC operations and also ensures that periodic tests are conducted as per the testing calendar agreed or as per regulation with the bank to ensure that all deliverables /SLAs are met in case the SOC operations are switched to alternate site (DR-SOC). The proposed DR site should mandatorily be located in India.

5. Section IV – Bid Submission Format

5.1 Bidder Profile

Sr	Particulars	Details
1.	Name of the Bidder	
2.	Address of the Bidder	
3.	Status of the Company (Public Ltd/ Pvt. Ltd)/Firm/LLP	
4.	Details of Incorporation of the Company/Firm	
5.	Details of Commencement of Business	
6.	GST registration no.	
7.	a. Permanent Account Number (PAN) & b. TAN	
8.	Name & Designation of the contact person to whom all Correspondence shall be made regarding this tender	
9.	Telephone No. (with STD Code) a) Landline b) Mobile	
10.	E-Mail of the contact person:	
11.	Fax No. (with STD Code)	
12.	Website	
13.	Financial Details (as per audited Balance Sheets) (Rs. in Cr)	

14.	Year	2015-2016	2016-2017	2017-2018
15.	Net Worth			
16.	Turn Over (Total)			
17.	Turn Over (from Indian Operations)			
18.	Turn Over (from Cyber Security Services)			
19.	Profit After Tax (PAT)			

5.2 Manufacturer Authorization Format

Manufacturer's Authorization Form

To,
The Vice President
IT Department
Nainital Bank Limited
Head Office
Mallital, Nainital -263001 (Uttarakhand)

Madam/Dear Sir,

Ref: - RFP no…… dated ……..*for SELECTION OF SYSTEM INTEGRATOR FOR MANAGED SECURITY SERVICES TO RUN SECURITY OPERATION CENTRE (SOC) SERVICES WITH MANAGED, DETECTION AND RESPONSE (MDR) CAPABILITIES DESCRIBED UNDER SCHEDULE OF REQUIREMENTS READ WITH SERVICE DELIVERY METHODOLOGY OF RFP DOCUMENT REF No. _____FOR PERIOD OF 5 YEARS.*

1) We, M/s._____, who are established and reputable manufacturers/producers of_____ having factories/development facilities at _____(address of factory/facility) do hereby authorize……., (Name and address of the bidder) to submit a Bid, and sign the contract with the Bank against the above Bid Invitation.

2) We hereby extend our warranty for the Solution, Products and services offered by the above firm against this Bid Invitation for contract duration.

3) We confirm that products quoted shall not be declared "end of life" for next 5 years from date of installation. Support including spares, patches for the quoted products shall remain available for next 7 years from date of installation.

For

(Authorised Signatory)
Name:
Designation:

Date:
Place:

5.3 Declaration for Non-Blacklisting

To be provided on letter head of the Bidder's Company

UNDERTAKING FOR NON- BLACKLISTED

Dated:
Place:

The Vice President
IT Department
Nainital Bank Limited
Head Office
Mallital, Nainital -263001 (Uttarakhand)

Sir,

Reg.: RFP Reference No: NTB/IT/SOC/2019/03/003

We M/s _____, a company incorporated under the companies act, 1956/2013 bearing CIN No._____ with its Registered Office at_____ Head Quarter at_____, do hereby confirm that we have not been blacklisted/ debarred by the Government / Government agency / Banks / Financial Institutions in India during last 3 years.

This declaration has been submitted and limited to, in response to the tender reference mentioned in this document

Thanking You,

Yours faithfully,

Signature of Authorized Signatory

Name of Signatory:

Designation:

Seal of Company

6. Section V - Detailed Scope of Work:

The minimum specified scope of work to be undertaken by the bidder shall be for SELECTION OF SYSTEM INTEGRATOR FOR MANAGED SECURITY SERVICES TO RUN SECURITY OPERATION CENTRE (SOC) SERVICES WITH MANAGED, DETECTION AND RESPONSE (MDR) CAPABILITIES DESCRIBED UNDER SCHEDULE OF REQUIREMENTS (Point no.5.1), READ WITH SERVICE DELIVERY METHODOLOGY, OF THIS RFP DOCUMENT FOR PERIOD OF 5 YEARS (which may be extended for next 2 years at sole discretion of Bank).

(Scope of Work is aligned with the Deployment Models & Service Delivery Methodology as described in Clause No.4.8 under Section III)

The project scope in terms of the number of services /devices is as follows-:

1. **For Phase 1-**

SOC Integration		
Sr No.	**Item Description**	**Total No of units***
1	No. of Windows servers at DC-Primary	12
2	No. of Windows servers at DR	07
3	No. of Windows Severs at Bank's premises	05
4	No. of Security & Network Devices	25
5	Active Directory	02
6	SAN Storage	02
7	Web Server	02
8	Database Server	05
9	Database server at Other location	05
10	Onsite Resource (L2)	01
11	Application	06

**10% variance be considered on total number of units*

Note- If bank extends the monitoring period beyond six months in the above Phase, then same rate will be applicable on pro-rata monthly basis.

2. **For Phase 2-**

SOC Integration		
Sr No.	**Item Description**	**Total No of units***
1	No. of Windows servers at DC-Primary	25
2	No. of Windows servers at DR	20
3	No. of Windows Servers at NDR	01
4	No. of Windows Servers at Bank's Premises	05
5	Active Directory at DC	02
6	Active Directory at DR	02
7	No of Database server at DC	07
8	No of Database server at DR	07
9	No of Database server at Other location	05
10	No of Web Server at DC	01
11	No of Web Server at DR	01
12	Storage	03
13	No of applications	06
14	No of Security & Network Devices	35

15	PIM- DC	18
16	PIM- DR	18
17	DAM – DC	08
18	DAM – DR	08
19	HIPS	All Servers
20	IDAM – DC	100
21	IDAM – DR	100
22	MFA (Multi Factor Authentication)- DC	100
23	MFA (Multi Factor Authentication)- DR	100
24	Hardware Load Balancer – DC	02
25	Hardware Load Balancer – DR	01
26	Patch Management Server	02
27	Anti Virus Server	02
28	No. of Routers at Branches/Offices (End point security)	175
29	Anti-Phishing & Brand-Monitoring Managed Services.	as per the scope defined in the RFP
30	Onsite Resource (L2)	01

Bidder to note that currently the Bank has Data Centre hosted at TCL Data Ltd. in Mumbai and DR at Hyderabad. However, in future the Data Centre & DR location may change as the process of scouting vendor for DC DR services is in process vide RFP No.NTB/IT/INFRA/2018/12/002. Incase this happens, bidder to take responsibility of integration of assets/ devices from new DC and DR to SIEM platform.

SCOPE OF ANTI-PHISHING & BRAND MONITOIRNG MANAGED SERVICES-

- 24x7x365 monitoring & mitigating/take-down of different phishing, pharming, Trojans, spyware, Brand-abuse, defacement of websites, etc. attacks on Bank's IT infrastructure. The bank should get alerts in the event of above attacks on real time basis.
- 24x7x365 monitoring of social media sites, FTP and distribution sites, grey markets, auction sites, job sites etc. for cases of brand abuse, bank's Trademark or Copyright property infringement.
- The selected bidder should respond within 30 minutes upon detection of any of the above attack and should work to shut down/take-down the detected site, anywhere in the world. The bidder should assist the bank in identifying customers affected by phishing attacks.
- Selected vendor should be able to report incident through all modes of communication that should include email, phone calls, SMS and dashboard. Details of compromised accounts should be shared immediately with the Bank.
- The bidder should ensure bringing down the reactivated phishing site at earliest which was earlier detected as phishing site.
- Alternative response mechanisms other than web site take down should be explored to minimize impact of phishing such as baiting, automatic dummy responses to phishing site using fictitious details.
- Gathering the Forensic information such as IP address, exact URL, source of attack, images, screen shots, email, account details, card details, compromised data etc. from the attacks and sharing the same with the Bank.
- Selected Bidder should have the reach on their own or through official business partnerships to take up closure/ mitigation measures on phishing sites anywhere in the world.
- Track hosting of phishing sites through digital watermark, monitoring web-server referrer logs
- Monitoring similar domain name registration - Track new domain name registrations to detect any spoofed or similar site being registered and shut down/take down the same
- Monitor spoofed email ids that may be used for sending emails to the customers of the Bank and take appropriate steps to protect the bank interest.
- Monitor anti-phishing forums.
- Selected bidder should assist the Bank for coordination with law enforcement agencies like CERT-IN, Banking Ombudsman etc. (with prior permission from Bank).

- Website Defacement monitoring services: Bidder should monitor bank's websites for defacement activities and should alert the Bank.

The overall Scope of Work (SoW) for the bidder to be appointed through this Tender includes the following but not limited to-

6.1 Schedule of Requirements

Through this Request for Proposal (RFP), the Bank wants to identify competent Vendors for designing and implementing the cost effective and comprehensive IT security log monitoring service as per the below criteria:

Functional Principles: The Intent for implementing a SOC at The Nainital Bank is covered in the below functional principles:

- **Detection of Information Security Threat & Prevention of Impact/ Breach:** The SOC should be able to identify information security threats/ vectors targeting bank's environment and prevent impact or breach due to them through implementation of adequate security mechanisms.
- **Incident Management:** Reporting and logging of information security incidents through the use of appropriate ticketing tools. Track and monitor the closure of these information security incidents and Escalation of these incidents to appropriate teams/ individuals in the bank if required.
- **Continuous Improvement:** Continuously improve SOC operations.

The Bank is envisaging a Managed Security Services model under which the prospective vendor shall provide 24x7x365 monitoring from vendor's SOC. The scope would involve monitoring of core infrastructure & security components at Bank's Managed Data Centre Mumbai & Disaster Recovery Centre Hyderabad(Managed DC, DR Sites are likely to be shifted to new locations within India), Head Office, Nainital, RDC Haldwani, Service Branch Delhi, RTGS Cell Delhi, branches and any other offices.

The bidder is required to integrate the core Infrastructure (Servers, Network) Devices including Firewalls/UTM, IPS devices, Web Security Appliances, Host Intrusion Prevention Systems, File Integrity Monitoring Solution, Data Leakage Prevention Solution, Web Application Firewalls, Privilege identity Management Solution, Anti APT Solutions, Network Behavioral Anomaly Detection, Network Access Control, DAM etc.with the proposed SIEM solution. Logs received from all these devices have to be correlated, analyzed for detection of threats, unusual user behavior & proactive incident analysis in real time manner.

Bank is looking for a Security Service Player which shall provide a "second layer of eyes approach" on the existing internal Security Controls & Monitoring services & help in augmenting the existing internal capabilities by having advanced SOC capabilities focused on detection of advanced threats apart from the traditional rule based SIEM capabilities such as-: MDR Methodology (Managed Detection & Response), which can help bank to have a proactive approach in determining the known & unknown threats faced by the Bank to reduce the risk of breach of data & systems, the advanced features/capabilities expected out of the vendor apart from rule based monitoring such as employing off the shelf SIEM solutions are as follows-

a. Security Analytics , Monitoring& Feeds services
b. Threat Hunting
c. Incident Analysis & Response
d. Detect Unknown attacks, blind spots & deep detection.
e. Augmentation of rule-based detection systems with new approaches such as machine learning & Artificial Intelligence to detect patterns, abnormalities.

f. Anti Phishing and Brand Monitoring

Other/optional Services -

g. Forensic as a SERVICE - forensic , log and advance malware analysis/ Forensic and Log Analysis

Onsite Resource (L2)

- Onsite resource should be trained or certified on the proposed SIEM solution used by the bidder for providing services to the bank.
- Technically qualified onsite resource should have minimum experience of 2-3 years in SOC operations, Log & Event Correlation and Analysis.
- Resource should be available at Bank's Delhi NCR location or Bank's preferred location during business hours (10 am- 6 pm; Monday to Saturday).
- The onsite resource will work in close association with bank's data center team and bidder's SOC Team for resolving / implementing any security issues.

6.2 High Level Deliverables

Areas	Activities	Deliverables
Security Monitoring	Log Monitoring; Server Monitoring; Security and Network Device monitoring	• 24*7*365 log monitoring • Detection of threats from integrated log sources and based on the use cases defined. • Event Analysis • Alerts as per defined escalation matrix
Network Threat Hunting	Analytics Based Hunting & IOC Based Hunting	• Once in 24 hours • Notification of alerts generated through analytical models on Threat Hunting enabling hunting for attacks including but not limited to Lateral Movement, Malware Beaconing, Data Exfiltration, Watering Hole, Targeted network attacks, Dynamic DNS attacks etc.
Incident Management	Incident Analysis, Identification of all components of the incident, root cause analysis and mitigation plans	• Provide logs and incident report for any identified security incident. • Coordinate with Bank's Team and help to contain attack/incident. • Provide evidences for legal and regulatory purpose in the form of log data.
SOC Maturity Improvement		• Quarterly briefings on Analysis and insights from data: trends, high risks areas, roadmap for strategic improvements, security posture benchmarking. Briefings on global threat trends, regulatory trends and cyber technology trends.
Report	Periodic reports; Trend analysis;	• Review multiple reports including

Management	Customized reports	top attackers, attacks, attack targets, trends. • Monthly MIS reports for monitored devices. • Recommendation for improvement of security posture and threat landscape.
Global Intelligence Feeds(Optional)	Continuous and regular global feeds from external known agencies.	• Threat & Vulnerability advisories in form of E-mails. • Recommendations for security improvements. • Provide Historical, Operational, Analytical and predictive Analysis.

6.3 Technical Specifications:

S. No	Requirement	Reply/Comments
1	**Threat Intelligence & Analytic**	
1.1	The Service Provider is expected to have a Threat Intelligence & Analytics platform which can be used to detect threats & can further enhance integration with SIEM.	
1.2	Service Provider should anticipate likely threats to the Bank both from outside (global intelligence) as well as arising from bank's internal infrastructure.	
1.3	Service Provider should support integration of machine readable threat intelligence from different open and commercial sources. It should support providing weightage against sources and support algorithms to reduce noise & false positives in threat intelligence feeds.	
1.4	Service Provider should apply threat intelligence received from different sources against the data received from different assets, network traffic, security events & users to determine likelihood of threats & impact & suggest preventive measures.	
1.5	Service provider should track status of assets against IoCs, Common Vulnerabilities and Exposures (CVEs) and support the workflow for remediation. As an example, CVEs related to shadow broker release should be used to identify potentially affected assets. Workflow should enable tracking the CVEs to closure through patching/other activities	
1.6	The Vendor should support an asset tracking mechanism wherein knowledge about assets in the Bank's Network is maintained which can help in Threat Anticipation by mapping threat intelligence/Vulnerability data to applicable assets.	
2	**Threat Hunting**	
2.1	Solution should support all four categories of threat hunting including Network Threat Hunting, User Behavior Anomaly Hunting, End Point Threat Hunting, and Application Threat Hunting. Bank would initially start with Network Threat Hunting services and later stage may add upon other categories of threat hunting.	
2.2	Network threat hunting should use AI (Artificial Intelligence)& Machine Learning abilities on network sources and enable hunting for attacks including but not limited to: • Lateral Movements • Malware Beaconing	

	• Data Exfiltration • Watering Hole attacks • Targeted network attacks • Dynamic DNS attacks	
2.3	Vendor should have capabilities to detect access anomalies e.g. Detection of deviation in the interaction of one server with another to detect attacks such as lateral movements.	
2.4	Network Threat hunting should utilize existing logs from security controls such as firewalls (at different layers such as Three Tier Architecture, WAN Edge, Partner Network), IPS devices , Web Security Appliance(Proxy), NBAD, Anti APT solutions to detect targeted attacks.	
3	**Advanced Alert Analytics & Attack Detection Capabilities**	
3.1	The solution should have capabilities to detect any compromises by linking related alerts collected together over a period of time.	
3.2	Solution should have capabilities to correlate alerts between sources & destination IPs to find similar or colluding threat signals.	
3.3	Solution should have a knowledge base on methods used by attackers in various past breaches globally to create models to detect such attacks.	
3.4	Solution should utilize data science techniques to identify kill chains for attacks such as lateral movements e.g. If a destination IP of one alert later becomes a source IP of another alert this suggests existence of a sequence.	
3.5	Solution should have detection models to find out threats sources are linked to the same attacker by grouping alerts with common characteristics like time, day location , target asset profiles etc.	
4	**Rule Based Detection (Traditional SIEM Capabilities)**	
4.1	In addition to the advanced analytics capabilities like MDR, solution should have capabilities to define rules on event logs captured from various sources to detect suspicious activities Examples • Failed login attempts • Login attempts from suspicious locations • Authorization attempts outside of approved list • Vendor logins from unauthorized subnets • Vertical & Horizontal port scans • Traffic from blacklisted IPs • Login attempts at unusual timings	
5	**Incident Analysis**	
5.1	Solution should support auto-triaging of alerts from a number of security products including Firewalls, PIM, DLP, IPS, WAF, Anti-APT, HIPS ,AV etc.	
5.2	Solution should have advanced techniques such as machine learning that considers contextual parameters, historical behavior& external threat intelligence to score an alert based on criticality in real time.	
6	**Incident Response**	

6.1	The Service Provider should provide automated incident analysis features/service for analysis of alerts received to answer the following • Impact on the assets. • Attributes of an attacker. • Determine other assets which may have been compromised. • Determine how long the attack campaign was & where was first compromise. • Maintain artifacts& IOCs of an incident.	
6.2	Bidder to describe how it performs a strong Incident Response Mechanism in providing Bank a comprehensive information about a potential incident , assemble the appropriate context , investigate as make recommendations so that Bank starts containment & remediation activities.	
6.3	Vendor to help Bank's team in performing the post incident analysis & RCAs which shall help in improvising the Incident Management process & learning.	
6.4	The Vendor should maintain an Incident Management Plan with at least the following-: • Incident Management Plan &Governance. • Incident Response plan &Governance • Workflows for Incident Management & Response • Communications & escalations Plan, Process & Metrics • Incident Management & Response Case Management	
7	**Other requirements**	
7.1	The proposed solution should support collection of events through customization of connectors or similar integration for the assets that are not natively supported. Solution should adhere to industry standards for event collection : syslog, OPSEC, WMI, SDEE,ODBC, JDBC, FTP, SCP, HTTP, text file, CSV,XML file etc.	
7.2	The proposed solution should be able to collect data from new devices added into the environment, without any disruption to the ongoing data collection.	
7.3	The proposed solution should have connectors to support listed devices/ applications, wherever required the vendor should develop customized connectors.	
7.4	All logs transferred to bidder's SOC should be Authenticated (time-stamped across multiple time zones) encrypted and compressed before transmission.	
7.5	The proposed solution provides options to load balance incoming logs to multiple collector instances.	
7.6	The proposed solution should support log collection from all major operating systems and their versions but not limited to Windows, Linux, AIX, Solaris etc.	
7.7	The collectors should be able to store/retain both normalized & raw data for forensic purposes	
7.8	In case of the connectivity issues, the data collector should be able to store the data for a period of 4 hours at its own repository. The retention, deletion, synchronization with SIEM database should be automatic but it should be possible to control the same manually.	
7.9	The proposed solution should ensure that the overall load on the network bandwidth at DC, WAN level is minimal	
7.10	The proposed solution should have the capability to compress the logs	

	by at least 70 % for storage optimization.	
7.11	The proposed solution should have capabilities to store the event data in its original format in the central log storage	
7.12	The proposed system shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.	
7.13	The proposed solution should support the following log collection protocols: Syslogover UDP / TCP, Syslog NG, SDEE, SNMP Version 2 & 3, ODBC, FTP, Windows Event Logging Protocol, Opsec, Netflow at a minimum.	
7.14	The proposed solution should prevent tampering of any type of logs and log any attempts to tamper logs. It must provide encrypted transmission of log data to the log management.	
7.15	The proposed solution should be able to perform the following correlations (but not limited to): Rule based, Vulnerability based, Statistical based, Historical based, Heuristics based, Behavioral based etc. across potentially disparate devices	
7.16	The dashboard provided to Bank should be in the form of a unified portal that can show correlated alerts/ events from multiple disparate sources such as security devices, network devices, enterprise management systems, servers, applications, databases, etc.	
7.17	Events should be presented in a manner that is independent of device specific syntax and easy to understand for all users	
7.18	Any failures of the event collection infrastructure must be detected and operations personnel must be notified as per SLA.	
7.19	The proposed system should display all real time events. The proposed solution should have drill down functionality to view individual events from the dashboard.	
7.20	Dashboard should support reporting for consolidated relevant compliance across all major standards and regulatory requirements. This includes ISO 27001, RBI regulations, IT ACT, PCI DSS standards etc.	
7.21	The proposed solution should support creation of automated incident management workflows to track incident from creation to closure, provide reports on pending incidents. It should also permit upload of related evidences such as screenshots etc.	
7.22	The proposed solution should support creation of automated Incident management workflows to track incident from creation to closure, provide reports on pending incidents. It should also permit upload of related evidences such as screenshots etc.	
7.23	Vendor to ensure logs are transmitted using strong encryption & no PII data is moved out of Bank's Environment.	
7.24	The devices /log sources to be monitored shall be from Bank's DC as well as DR.The solution should be able to collect logs from both DC-DR locations & the architecture proposed should clearly consider this requirement.	
7.25	The proposed solution should have high availability feature built in. There should be an automated switch over to secondary collector in case of failure on the primary collector. No performance degradation is permissible even in case of collector failure.	
7.26	a. Log storage& retention during Phase 1 is at Bidder's SOC. b. Log storage & retention at Bank's premises in Phase 2, shall be for a period of 1 year (1 month online and 11 months offline)	

6.4 Scalability

a) All components of the SOC must support scalability to provide continuous growth to meet the requirements and demand coming in from various user departments.
b) Modular design of the SOC is an excellent strategy to address growth without major disruptions.
c) A scalable SOC shall easily be expanded or upgraded on demand. Scalability is important because new computing component is constantly being deployed, either to replace legacy component or to support new missions.

6.5 Availability

a) All components of the SOC must provide adequate redundancy to ensure high availability of the Governance applications and other SOC services.
b) Designing for availability assumes that systems will fail, and therefore the systems are configured to mask and recover from component or server failures with minimum application outage.
c) The bidder shall make the provision for high availability for all the services of the data Center.

6.6 Interoperability

a) The entire proposed system/ subsystem should be interoperable, in order to support information flow and integration.
b) Operating systems and storage technologies from several vendors must interact well with each other. These systems should also support the open architecture solutions where information/ data can be ported to any system, whenever desired.

7. Section VI –

7.1 Commercial Bid Format-SOC Services

Phase 1:Log collectors shall be deployed at Bank's Premise & other components such as log storage, rule correlation engine, advanced detection, triaging & response platforms are at bidder's SOC.

Server/Device/Services	Total No of units*	Per Unit Price	Cost for six months
No. of Windows servers at DC-Primary	12		
No. of Windows servers at DR	07		
No. of Windows Severs at Bank's premises	05		
No. of Security & Network Devices	25		
Active Directory	02		
SAN Storage	02		
Web Server	02		
Database Server	05		
Database server at other locations	05		
Onsite Resource (L2)	01		
Application	06		
Additional Log Sources (Server/ Network Device/ Security Device)	Per Log Source		
Cost of Anti-Phishing & Brand-Monitoring Managed Services as per the scope defined in the RFP. -This cost includes unlimited no. of takedowns of phishing sites/brand-abuse incidents in a year.			

**10% variance be considered on total number of units*

A) Recurring charges- Total Cost for 6 Months- Rs._____

Note- If bank extends the monitoring period beyond six months in the above model the Bank reserves its right to charge the same rate on pro-rata monthly basis.

Phase 2:Log Manager shall be deployed at Bank's Premise & other components such as rule correlation engine, advanced detection, triaging & response platforms are at bidder's SOC.

Services	One time charges in Rs.
Charges towards One-time transition due to change in deployment model from Phase 1 to Phase 2-	

B) One time charges- Rs._____

Server/Device/Services	Total No of units*	Per Unit Price	Charges for one year	Charges for 5 years
No. of Windows servers at DC-Primary	25			
No. of Windows servers at DR	20			
No. of Windows Servers at NDR	01			
No. of Windows Servers at Bank's Premises	05			
Active Directory at DC	02			
Active Directory at DR	02			
No. of Database server at DC	07			
No. of Database server at DR	07			
No. of Database server at other locations	05			
No. of Applications	06			
No. of Storage	03			
No of Web Server at DC	01			
No of Web Server at DR	01			
No of Security & Network Devices	35			
PIM- DC	18			
PIM- DR	18			
DAM – DC	08			
DAM – DR	08			
HIPS	All Servers			
IDAM – DC	100			
IDAM – DR	100			
MFA (Multi Factor Authentication)- DC	100			
MFA (Multi Factor Authentication)- DR	100			
Hardware Load Balancer – DC	02			
Hardware Load Balancer – DR	01			
Patch Management Server	02			
Anti Virus Server	02			
No. of Routers at Branches/Offices (End point security)	175			
Onsite Resource (L2)	01			
Additional Log Sources(Server/ Network Device/ Security Device)	Per Log Source			
Cost of Anti-Phishing & Brand-Monitoring Managed Services as per the scope defined in the RFP. -This cost includes unlimited no. of takedowns of phishing sites/brand-abuse incidents in a year.				

**10% variance be considered on total number of units*

C) Recurring charges- Total Cost for 5 years- Rs._____

SOC Services includes device integration, log monitoring, threat hunting & other requirements defined under schedule of requirements (Point 5.1 of section V).

Commercial for Other/optional Services	
Sr. No.	**Activity* and (Price (INR) on Per Man-day basis)**
1.	On-Demand Forensic/ Breach Investigation Services • Activities should include the below but not limited to-: o File system examination and analysis o User accounts and access analysis o Windows Registry analysis o Event logs - System, Security and Application logs analysis o Anti-virus and other security software logs analysis o Network Connections, Wireshark, Open Shares, RDP and other connection analysis o Disk Analysis o Text view analysis of files o Application Component Analysis o Database analysis o Keyloggers analysis o Deleted files recovery and analysis o Corrupted Executable analysis • Collection of evidence in a manner that protects the chain of custody, should include the following but not limited: o Retrieval of Deleted artefacts o Timeline analysis of installed applications o USB Device analysis – attached USB devices o USB devices to files correlation o Remote Connections analysis o Malware Analysis o Timeline analysis of emails • Provide technical support for containment, mitigation and recovery activities such as reimaging, rule changes in security product, patch and configuration changes in assets, deactivating accounts etc.

*While the breadth of the incident cannot be determined now, the actual efforts will be discussed between bank and the service provider with every incident that happens. Bidders are required to quote per man-day pricing for the On-Demand Forensic/ Breach Investigation Services.

D) Commercial for Other/optional Services on Per Manday basis- Rs._____

Summary of Commercials-

Sr	Services	Amount in Rs.
1	A) Phase 1- Recurring charges- Total Cost for 6 Months	Rs.
2	B) One time charges (transition from Phase 1 to Phase 2)	Rs.
3	C) Phase 2 - Recurring charges- Total Cost for 5 years	Rs.
4	D) Commercial for **Other/optional Services :** Forensic as a SERVICE - forensic , log and advance malware analysis/ Forensic and Log Analysis	Rs.
	Total Cost (Commercial bid) of the project (A+B+C+D)*	**Rs.**

*The total cost will be considered as 'L' during the commercial evaluation process as described under point 3.32 of RFP Document.

7.2 Bank Guarantee (BG) Format

BANK GUARANTEE ("BG") IN LIEU OF EARNEST MONEY DEPOSIT)

The Chief Operating Officer,
The Nainital Bank Limited,
Head Office, Seven Oaks,Mallital,
Nainital- 263001, (Uttarakhand)

WHEREAS _____(hereinafter called "the **Bidder**") has submitted its bid dated _____("Date of Submission of Bid") for selection of System Integrator for Managed Security Services to run Security Operation Centre (SOC) Services with Managed, Detection and Response (MDR) capabilities described under schedule of requirements read with Service Delivery Methodology of this RFP document for period of 5 years for The Nainital Bank Limited (hereinafter called "the **Purchaser**") in response to Request for Proposal ("**RFP**")NTB/IT/SOC/2019/03/003(hereinafter called "the **Bid**") issued by the Purchaser.

KNOW ALL PEOPLE by these presents that We_____(Name of Bank)having our registered office at_____(hereinafter called "the **Bank**")are bound unto the Purchaser to the sum of **INR Rs. 4,00,000/- (Rupee Four lakh only)** for which payment will and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents.

Sealed with the seal of the said Bank this _____ day of _____,20___.

THE CONDITIONS of this obligation are:

1 If the Bidder withdraws its Bid during the period of bid validity specified in the RFP aforesaid; or
2 If the Bidder, having been notified of the acceptance of its bid by the Purchaser during the period of bid validity, the Bidder:
   a) fails or refuses to execute the Contract; or
   b) fails or refuses to furnish the Security Deposit/ Bank Guarantee for contract performance.

We undertake to pay the Purchaser upto the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

This Guarantee will remain in force up to and including ____months i.e. upto _____and any demand in respect thereof should reach the Bank not later than the above date i.e. _____

Notwithstanding any other term contained herein-

a) this Guarantee shall be valid only upto_____where upon it shall automatically expire irrespective of whether the original guarantee is returned to the Bank or not; and
b) the total liability of Bank under this Guarantee shall be limited to **INR Rs. 4,00,000/- (Rupee Four lakh only)**.

Place :
SEAL Code No. Signature

NOTE:
1. BIDDER SHOULD ENSURE THAT THE SEAL & CODE NO. OF THE SIGNATORY IS PUT BY THEBANKERS, BEFORE SUBMISSION OF BG.
2. STAMP PAPER IS REQUIRED FOR THE BG ISSUED BY THE SCHEDULED COMMERCIAL BANKS IN SOME STATES.

---End of Document---