Request for proposal for engaging a Managed Security Service Provider for Security Operations Centre (SOC) Services with Managed, Detection and Response (MDR) Along with Brand Monitoring, Breach Investigation, AD Security and Threat Hunting Capabilities for a period of 3 Years

RFP Reference No: RFP # NTBL/ISC/SOC/2024/11/22
Dated: 06-11-2024

DISCLAIMER

The information contained in this Request for Proposal (RFP) document, or subsequently provided to Bidders, whether verbally or in documentary form by or on behalf of The Nainital Bank Limited or any of its representatives, employees, or advisors (collectively referred to as "Bank Representatives"), is provided to Bidders under the terms and conditions set out in this RFP document and any other applicable terms and conditions. This document shall not be transferred, reproduced, or otherwise used for any purpose other than its intended use.

This RFP document is not an agreement and does not constitute an offer or invitation by the Bank representatives to any party other than those qualified to submit their proposals (Bidders). Its purpose is to provide Bidders with information to assist in the formulation of their proposals. This RFP document does not claim to contain all the information that each Bidder may require and may not be suitable for all recipients. It is not possible for the Bank representatives, their employees, or advisors to consider the investment objectives, financial situation, and particular needs of each party that reads or uses this RFP document.

The Bank, its employees, and advisors make no representations and shall have no liability to any person, including any applicant or bidder, under any law, statute, rule, regulation, tort, or principles of restitution or unjust enrichment for any loss, damages, costs, or expenses that may arise from or be incurred as a result of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness, or reliability of the RFP and any assessments, assumptions, statements, or information contained therein, or arising from participation in this bidding process.

The Bank also accepts no liability of any nature, whether resulting from negligence or otherwise, for reliance by any Bidder on the statements contained in this RFP. Bidders are expected to examine all instructions, forms, terms, and specifications in the bidding document. Failure to furnish all required information or to submit a Bid that is not substantially responsive to the bidding document may be at the Bidder's risk and may result in the rejection of the Bid. The Bank representatives may, at their absolute discretion and without any obligation to do so, update, amend, or supplement the information in this RFP document.

Subject to any contrary law and to the maximum extent permitted by law, the Bank and its Directors, Officers, Employees, Contractors, Representatives, Agents, and Advisors disclaim all liability for any loss, claim, expense (including, without limitation, any legal fees, costs, charges, demands, actions, liabilities, expenses, or disbursements incurred or incidental thereto), or damage (whether foreseeable or not) ("losses") suffered by any person acting on or refraining from acting based on any presumption or information (whether oral or written, expressed or implied), including forecasts, statements, estimates, or projections contained in this RFP document or conduct ancillary to it, regardless of whether the losses arise in connection with ignorance, negligence, inattention, carelessness, disregard, omission, default, lack of care, erroneous information, falsification, or misrepresentation on the part of the Bank or any of its Directors, Officers, Employees, Contractors, Representatives, Agents, or Advisors.

Checklist (for indicative purposes only)

The following items must be checked before submitting the Bid:

1. **Application Money:** Online transfer of ₹29,500 (Rupees Twenty-Nine Thousand Five Hundred only, inclusive of GST @ 18%) in Envelope A (Eligibility Criteria Response).
2. **Bid Security (EMD):** Application money has to be deposited as DD/PO/NEFT/RTGS* at the time of submission of bid. of ₹7,00,000 (Rupees Seven Lakhs only) in Envelope A (Earnest Money Deposit).

    - Remittance proof in favor of "The Nainital Bank Limited," payable at Nainital/Delhi, amounting to ₹29,500 (₹25,000 plus GST @ 18%) for Application Money and ₹7,00,000 for Bid Security (EMD). *DD/PO and Bank Guarantee should be made in favor of The Nainital Bank Ltd. and be made Payable at Nainital.
    - The electronic/wire transfer should be made to the designated bank account as detailed below:
    - **Account Name:** Adjusting Account
    - **Bank Name:** The Nainital Bank Limited
    - **Account No:** 0999420300000001
    - **IFSC Code:** NTBL0NAI999
    - **Branch Name:** Head Office, Nainital
    - **Address:** 7 Oaks Building, Mallital, Nainital
    - The bidder should mention the RFP number and description in the electronic transfer details.

3. **Bid Preparation:** Eligibility Criteria, Technical, and Commercial Bids must be prepared in accordance with the RFP document.
4. **Envelope A:** Include the Eligibility Criteria Response.
5. **Envelope B:** Include the Technical Criteria Response.
6. **Envelope C:** Include the Financial Criteria response.
7. **RFP Document:** The RFP document must be duly sealed and signed by the authorized signatory on each page and enclosed in Envelope A.
8. **Pricing:** Prices must be quoted in Indian Rupees (INR).
9. **Supporting Documents:** All relevant certifications, audit reports, etc., must be enclosed to support claims made in the bid in the relevant envelopes.
10. **Signature Requirement:** All pages of documents submitted as part of the Bid must be duly sealed and signed by the authorized signatory.
11. Amendments notified to be checked by the bidder before final submission of the bid on the Bank's website i.e. www.nainitalbank.co.in .

Abbreviations (For reference)

1. **Bank**: Refers to 'The Nainital Bank Limited.'
2. **NTBL**- Refers to 'The Nainital Bank Limited.'
3. **Bidder**: Refers to the respondent to the RFP document.
4. **RFP**: Refers to the Request for Proposal document.
5. **DC**: Data Center; **DR**: Disaster Recovery Site; **NDR**: Near Disaster Recovery Site.
6. **SOC**: Security Operations Center.
7. **SIEM**: Security Information and Event Management.
8. **Collector**: The device that collects logs from security devices in raw format and forwards them to the SIEM solution database, applying necessary filters if configured to do so.
9. **CBS**: Core Banking Solution implemented by the Bank.
10. **Party**: Refers to either the Bidder or the Bank; **Parties**: Refers to both collectively.
11. **APT**: Advanced Persistent Threat.
12. **PIM/PAM**: Privileged Identity Management (PIM) and Privileged Access Management (PAM).
13. **FIM**: File Integrity Monitoring.
14. **Bidder / Respondent**: Refers to those who purchase this tender document and submit a response to it.
15. **SMTP**: Simple Mail Transfer Protocol.
16. **IDS / IPS**: Intrusion Detection System / Intrusion Prevention System.
17. **MDR/XDR**: Managed detection and response (MDR) and extended detection and response (XDR)
18. **AD**: Active Directory
19. **HLD**: High Level Diagram
20. **LLD**: Low level Diagram
21. **OEM**: Original Equipment Manufacturer
22. **DLP**: Data Leak & Prevention
23. **LD:** Liquidated Damages
24. **SLA:** Service Level Agreement
25. **AMC:** Annual Maintenance Contract
26. **OWASP:** Open Web Application Security Project
27. **NSIC:** National Small Industries Corporation
28. **UTM:** Unified Threat Management

Table of Contents

1. Section 1 – Invitation to Bid 9
1.1 Document Control Sheet 10
2. Section 2 – Instruction for bid submission 12
2.1 About the Nainital Bank Limited 12
2.2 Objective of this RFP 12
2.3 Invitation of Bids 12
2.4 Preparation of Bids 13
2.5 Submission of Bids 13
2.6 Document description 13
2.7 Bidding Cost 14
2.8 Clarification on RFP Document 14
2.9 Amendment of RFP Document 14
2.10 Bidder Qualification 14
2.11 Application Money & Earnest Money Deposit (EMD) 15
2.12 Return of EMD for successful Bidder 15
2.13 Security Deposit/ Performance Guarantee 15
2.13.1 Validity 16
2.14 Period of Validity of Bids 16
2.15 Extension of Period of Validity 16
2.16 Format and Signing of Bid 16
2.17 Documents comprising the Bids 16
2.17.1 Envelopes A - Eligibility / Pre-Qualification envelope 16
2.17.2 Envelope B - Technical Bid envelope 17
2.17.3 Envelope C - Commercial Bid envelope 17
2.17.4 Revelation of Prices 17
2.17.5 Terms and Conditions of Bidders 18
2.17.6 Consortium 18
2.17.7 Last Date & time for Receipt of Bids 18
2.17.8 Late Bids 18
2.17.9 Modification and Withdrawal of Bids 18
2.17.10 Bidder's Address for Correspondence 18
2.17.11 Contacting the Bank 18
2.17.12 Opening of Bids by Bank 18
2.17.13 Evaluation of Bids 18
2.17.14 Preliminary Examination 18
2.18 Assistance to bidders 18

2.19 Micro and Small Enterprise (MSE/ NSIC - with valid number) 19
2.20 Due Diligence 19
2.21 Language of Bids 19
2.22 Contract Period 19
2.23 Clarification 19
2.24 RFP Abandonment 19
3. Section 3 – Scope of Work 20
3.1 Technical Specifications: Security Operation Centre (SOC) 20
3.1.1 A. SOC Monitoring 20
3.2 Scalability 20
3.3 Project Timeline 21
3.4 Project Structure 21
3.5 Subcontracting 21
3.6 Implementation Phase 21
3.6.1 Roles and Responsibilities: 21
3.6.1.1 Team Lead 21
3.7 Operations Phase 21
3.8 Manpower Support working days' schedule (onsite/off site) 21
3.9 Manpower at The Nainital Bank Limited 22
3.10 Security Device Management / Support 22
3.11 Security Advisory Services/ Security Incident and Crisis Management Services 22
3.12 Pert Chart 22
4. Section 4 – Eligibility Criteria 23
4.1 Eligibility Criteria 23
A. Start-ups: 23
B. Other than start-ups: 23
C. Other Eligibility Criteria 24
5. Section 5 - Bid Opening 26
5.1 Opening of Eligibility and Technical Bids Envelope A and Envelope B 26
5.2 Opening of Commercial Bids Envelope C 26
6. Section 6 - Bid Evaluation 27
6.1 Stage 1 – Evaluation of Eligibility Criteria 27
6.2 Stage 2 – Evaluation of Technical Criteria 27
6.3.1. Commercial Bid Format - SOC Services 28
6.3. Rate Discovery for Resident Engineer 28
7 Section 7 - Terms and Conditions 29
7.1 Bank's Right to Vary Scope of Contract at the Time of Award 29

7.2 Bank's Right to Accept Any Bid and Reject Any or All Bids 29
7.3 Notification of Award 29
7.4 Award of Contract 29
7.5Termination of contract: 29
7.6 Conflict of Interest 30
7.7 Placing of Purchase Orders 30
7.8 Performance Bank Guarantee Schedule: 31
7.9. Confidentiality and Non-Disclosure of the Document 31
7.10. Prevention of Corrupt and fraudulent practices: 31
7.11. Tender Related Condition 31
7.12. Rejection Criteria 32
7.13. General Rejection Criteria 32
7.14. Technical Rejection Criteria 32
7.15 Commercial Rejection Criteria 32
7.16 Liquidated Damages 32
7.17 Force Majeure 32
7.18 Arbitration 33
7.19 Jurisdiction 33
7.20 Safety 33
7.21 Statutory Laws: 33
7.22 Confidential Information: 33
7.23 Extra Deviated Items: 33
7.24 Term and Extension of the Contract 33
7.25 Prices 34
7.26 Payment Terms 34
8. Section 8: Service Level Agreement & Penalties 35
8.1 Service Levels during implementation phase 35
8.2 Responsibility Matrix 35
8.3 Service Level Agreement (SLA) & Targets 36
8.4 Service Level Agreements Matrix Operations Phase 36
8.4.1 Uptime of the solution 36
8.4.2 Security Incident Alerting & Reporting 37
Severity Categorization 39
8.5 Deployment Models & Service Delivery Methodology 39
8.6 Business Continuity 40
1. Annexure A1 - Bidder's Letter for Application Money & EMD Details 69
2. Annexure A2 - Bid Security (Bank Guarantee) 70

3. Annexure A3 - Bid Security 71
4. Annexure B - Bid Offer Form (without Price) 74
5. Annexure C - Bidder Information 75
6. Annexure D - Declaration for Clean Track Record 77
7. Annexure E - Declaration for Acceptance of RFP Terms and Conditions 78
8. Annexure F - Declaration for Acceptance of Scope of Work 79
9. Annexure G - Format Power of Attorney 80
10. Annexure H1 - Eligibility Criteria Compliance 81
11. Annexure H2 – Other Than Start Ups. 82
12. Annexure H3 Turnover Certificate 85
13. Annexure I - Requirement of manpower skillset 86
14. Annexure J - Client Details 87
15. Annexure K - Manufacturer's (OEM) Authorisation Form 89
16. Annexure L – Hardware Requirement 90
17. Annexure M - Commercial Bid Form 90
18. Annexure N- Commercial Bid 91
19. Annexure O - Declaration for Undertaking of Information Security 92
20. Annexure P: Non-Disclosure Agreement 93

1. Section 1 – Invitation to Bid

The Nainital Bank Ltd. Invites Bids (Technical & Financial) from eligible bidders which are valid for 180 days after the last date of submission of the bid date for "Engaging a Managed Security Service Provider for Security Operations Centre (SOC) Services with Managed, Detection and Response (MDR) Along with Brand Monitoring, Breach Investigation, AD Security and Threat Hunting Capabilities for a period of 3 Years may be extended at sole discretion of the Bank for the next 2 years."

Name of Project	Request for proposal for engaging a Managed Security Service Provider for Security Operations Centre (SOC) Services with Managed, Detection and Response (MDR) along with Brand Monitoring, Breach Investigation, AD Security and Threat Hunting Capabilities for a period of 3 Years may be extended at sole discretion of the Bank for the next 2 years.
RFP Reference Number	NTBL/ISC/SOC/2024/11/22
Date of commencement of issue of tender document	06-11-2024
Application Money	Rs. 29,500/- (Rupees twenty-nine thousand five hundred only) (Rs. 25,000/- plus GST@18 %) (Non-Refundable)
	Application money must be deposited as DD/PO/NEFT/RTGS* at the time of submission of Bid.
Bid Security Amount/ EMD (Earnest Money Deposit)	Rs. 7,00,000/- (Rupees Seven Lakh only)
	Earnest Money Deposit (EMD) submitted in the form of DD/PO/NEFT/RTGS * 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)
Last date and time of submission of Bids	26-11-2024 (1700 Hrs)
Date and time of opening of Eligibility and Technical Bids (Envelope A and Envelope B)	Date and time of opening of envelope A & B will be shared later to the Bidders (through the authorized e-mail ID shared by the Bidders.) preferably before 06-12-2024
Validity Period	180 days after the last date of submission of bid date
RFP Coordinator	Pankaj Adhikari

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

*Note: DD/PO/NEFT/RTGS and Bank Guarantee should be made in favor of The Nainital Bank Limited. and be made payable at Nainital. Exemption for Micro and Small Enterprises (MSEs) are exempted from paying the Application Money and Bid Security Amount/EMD, provided they submit the necessary documentary evidence. Government of India provisions for MSEs shall be considered while evaluating the tender. (Please refer to Pt. 2.20 of this RFP document for details on the MSE clause.)

RFP Coordinator –
Pankaj Adhikari,
Contact No- +91-9456108588
e-mail- infosec@nainitalbank.co.in
Ciso@nainitalbank.co.in

1.1 Document Control Sheet

Tender Reference No.	NTBL/ISC/SOC/2024/11/22
RFP Issuance Date	06-11-2024
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)	Online/Offline
RFP Coordinator	Pankaj Adhikari| Contact: +91 9456108588 Email id: infosec@nainitalbank.co.in
Bid Related Queries	Deepak Rautela| Contact: +91 98703988 68 Email id: ciso@nainitalbank.co.in
Last date of receiving written request for clarifications before the pre-bid meeting	17:30 hrs. on 11-11-2024 e-mail– infosec@nainitalbank.co.in
Pre-bid meeting	Pre bid meeting will be held through the online mode on 14-11-2024 between 11:00 AM and 5:00 PM. Bidder to submit the names of -2- authorized officials/persons (Maximum) along with their contact numbers, designations, and e-mail IDs on **infosec@nainitalbank.co.in** and **ciso@nainitalbank.co.in** Invitation link of the meeting will be sent by the Bank to email IDs (max 2) of authorized officials/persons of the Bidder to join the Online Pre-Bid Meeting as per the schedule mentioned above. To join the On-Line Pre-bid meeting, the Bidder's representatives will have to click the link provided through E-mail by the Bank.
Visit of SOC	Bank may ask Eligible bidders for Bidders SOC Visit before the Technical presentation/ Financial Bid Opening.
Last date and place of submission of RFP response (Closing date)	5:00 PM on 26-11-2024 at Information Security Cell, CISO Office The Nainital Bank Ltd, Railway Bazar Haldwani, Nainital(UK) 263139
Mode of Submission of Bid	The Bidder shall send the Bid Envelope through Courier / Registered Post / Speed Post at the above address on or before 26-11-2024 (bid submission date). The date on dispatch of Courier / Registered Post / Speed Post receipt should be on or before the last date of bid submission. The receipt of Courier / Registered Post / Speed Post for tracking purpose should be sent to email id of RFP Coordinator mentioned in the Document Control Sheet. However, if the said Bid Envelope sent through Courier / Registered Post / Speed Post is lost in transit or is not delivered within 3 days from the last date of bid submission in such circumstances the Bank shall not be liable, whatsoever, for such misplacement or non-delivery of the said bid envelope.

	Further, the Bidder, whose bid envelope is lost in transit, misplaced in transit or undelivered during 3 days since the last date of bid submission cannot resubmit his bid on the pretext of lost in transit, misplacement, or non-delivery of the Bid envelope.
Date and time and place of opening of Eligibility and Technical Bids (envelope A and envelope B)	Date and time of opening of envelope A & B will be shared later to the Bidders (through the authorized e-mail ID shared by the Bidders.)
Date and place of Technical Presentation (Presentation will be given by the eligible bidder only)	Date of technical presentation will be shared later to the eligible Bidders through authorized e-mail ID shared by the Bidders.
Contract Type (Empanelment/Tender)	Tender
Multiple Technical Annexure(s)	Yes
Quoting for all Technical Annexures is compulsory	Yes
Application Money	Rs. 29,500/- (Rs. 25,000/- plus GST @18 %) (Non-Refundable)
Bid Security (Earnest Money Deposit)	Rs. 7,00,000/-
Bid Validity days	180 days after the last date of submission of bid date
Location for Submission of Bid	The Nainital Bank Limited, Information Security Cell, CISO Office Railway Bazar, Haldwani Uttarakhand- 263139
Validity of Contract	Three (03) years from the date of signing of the contract with the successful bidder. (may be extended at sole discretion of the bank further for the next two years)
Address for communication	Chief Information Security Officer The Nainital Bank Limited, Information Security Cell, Railway Bazar, Haldwani, Nainital Uttrakahnd- 263139

2. Section 2 – Instruction for bid submission

2.1 About the Nainital Bank Limited

The Nainital Bank Limited was established in 1922 with the objective of catering to the banking needs of the people in the region. Bank of Baroda, a premier nationalized bank, has managed the affairs of The Nainital Bank Limited since 1973. Currently, the bank operates in five states: Uttarakhand, Uttar Pradesh, Delhi, Haryana, and Rajasthan, with 171 branches, which may increase in the future as new branches open. The bank's Head Office is in Nainital, Uttarakhand, and its Regional Offices are located in Delhi, Dehradun, and Haldwani. The bank operates with a vision that states: "To emerge as a customer-centric national bank and become the most preferred bank for its products, services, technology, efficiency, and financials."

For further details, you can visit the Bank's website www.nainitalbank.co.in

2.2 Objective of this RFP

The Nainital Bank Limited intends to strengthen its information systems security for monitoring and compliance by engaging a managed security service partner to implement and maintain a Cyber Security Operation Centre (SOC) for its IT setup. This includes critical locations such as the Data Centre (DC), Disaster Recovery (DR), Near Disaster Recovery (NDR), (DIT-Department of Technology), RTGS Cell, Project Management Office, Head Office, and other IT locations that may arise in the future as business requirements evolve. The Bank has undergone many upgradations in its IT Infrastructure, IT manpower and underlying technology such as upgradation of CBS application to Finacle with the underlying Core infrastructure at DC/DC and NDR. Also, with the addition of many new applications and associated technologies in the bank. The bank now needs to focus on comprehensive security measures for protecting the Bank's IT infrastructure (including everything from the Bank's websites, databases, servers, applications, networks, desktops, data centers, and a variety of endpoints), Different Applications and User data. These comprehensive security measures include mandatory SIEM Services including MDR/EDR (which provides real-time threat detection, incident response, and continuous monitoring to safeguard sensitive financial data), Brand Monitoring (to track and mitigate reputational risks, ensuring that any potential breaches or negative perceptions are addressed promptly.), and AD security has become critical. Engaging a New Managed Security Service Provider (MSSP) to establish a Security Operations Centre (SOC) is a strategic move to enhance our cybersecurity framework.

Furthermore, Breach Investigation capabilities will be essential for conducting thorough analyses of any security incidents, allowing us to understand vulnerabilities and prevent future occurrences. Active Directory (AD) security measures will also be implemented to protect user credentials and prevent unauthorized access to critical systems.

Lastly, threat-hunting capabilities will proactively identify and neutralize threats before they can inflict damage. By partnering with a new MSSP, we aim to leverage their expertise, advanced technologies, and threat intelligence to create a resilient and adaptive security environment

The contract period shall be for three years, starting from the date of acceptance of the project by the bank.

2.3 Invitation of Bids

This request for proposal document ('RFP document' or RFP) has been prepared solely to enable The Nainital Bank Limited ('Bank') to select a bidder for engaging a Managed Security Service Provider for Security Operations Centre (SOC) Services with Managed Detection and Response (MDR), along with Brand Monitoring, Breach Investigation, Active Directory (AD) Security, and Threat Hunting capabilities for a period of three years may be extended for 2 years on sole discretion of the Bank.

Bidders interested in implementing and managing the SOC with the aforementioned solutions for The Nainital Bank Limited are invited to submit their technical and commercial proposals in response to this OPEN RFP.

This OPEN RFP seeks proposals from bidders who possess the necessary experience, capability, and expertise to provide The Nainital Bank Limited with the required SOC services, adhering to the requirements outlined in this document. The criteria and actual process for evaluating the responses and selecting the successful bidder will be at the bank's discretion. This OPEN RFP is not an offer by The Nainital Bank Limited but an invitation to receive responses from bidders. No contractual obligation shall arise from this process unless a formal contract is signed and executed by duly authorized

officials of The Nainital Bank Limited with a selected bidder. Preference will be given to bidders who have demonstrated experience in implementing and managing SOC services within the banking industry.

2.4 Preparation of Bids

Before Final submission, the Bidder should consider all clarifications/corrigendum/s, (if any), published on the Bank's website related to the Tender Document.

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

2.5 Submission of Bids

The bidder shall seal the original DD/PO or Bank Guarantee as EMD and Application fees in the form of DD/PO in an envelope which must be marked as **Envelope A along with other Pre-qualification documents.**

In case the Application fees and EMD are sent through NEFT/RTGS, such details must be submitted in the Format as mentioned in the Annexure. **(Annexure A1 - Bidder's Letter for EMD)**

The Bidder shall mark its company/firm/LLP name and Tender reference number on the back of the Bank Demand 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 send the Bid Envelope through Courier / Registered Post / Speed Post at The Nainital Bank Limited, Information Security Cell, CISO Office, Railway Bazar, Haldwani Uttarakhand- 263139**.**

The date on dispatch of Courier / Registered Post / Speed Post receipt should be on or before the last date of bid submission. The receipt of Courier / Registered Post / Speed Post for tracking purpose should be sent to the email id of RFP Coordinator mentioned in Document Control Sheet.

However, if the said Bid Envelope sent through Courier / Registered Post / Speed Post is lost in transit or not delivered within 3 days from the last date of bid submission in such circumstances the Bank shall not be liable, whatsoever, for such misplacement or non-delivery of said bid envelope.

Further, the Bidder, whose bid envelope is misplaced in transit or is undelivered within 3 days from last date of bid submission, cannot resubmit his bid on the pretext of misplacement or non-delivery of the Bid envelope.

One paper copy and one electronic copy of the technical Presentation (PowerPoint or Microsoft Word and Excel contained in storage media) with all documents submitted under the Technical Bid (Envelope B) must be supplied to the Bank at The Nainital Bank Limited, Information Security Cell, Railway Bazar, Haldwani, Uttarakhand- 263139 on or before the last date of bid submission and addressed as **"Technical Presentation of RFP Reference No: RFP # NTBL/ISC/SOC/2024/11/22.".(Technical Presentation may also be submitted over the email: infosec@nainitalbank.co.in also CC to ciso@nainitalbank.co.in &**

Bidders are requested to note that they should necessarily submit their commercial bids in the format provided and no other format is acceptable. If the Bidder(s) adopts any other format, such bid(s) shall be rejected.

2.6 Document description

In this document, "RFP" shall mean "Request for Proposal." The terms "Bid," "Tender," and "RFP" are used interchangeably. Additionally, "Bank" refers to "The Nainital Bank Limited."

Before submitting the bid, the Bidder is expected to examine all instructions, forms, terms and conditions, and technical specifications in the bidding document. Submitting a bid that is not responsive to the bidding document in every respect will be at the Bidder's risk and may result in the rejection of the bid without further reference to the Bidder.

2.7 Bidding Cost

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

2.8 Clarification on RFP Document

A prospective bidder requiring clarification on the RFP document may submit queries via email to the Bank's email address: infosec@nainitalbank.co.in. Queries must be submitted in the following format (in an Excel file, *.xls) to be considered for clarification:

Email Subject: Pre-bid Queries - RFP # NTBL/ISC/SOC/2024/11/22 dated 06-11-2024.

Sr. No.	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	Additional Remarks (if any)

The Bank will only respond to queries submitted in the above excel format. All queries must be received on or before pre bid meeting, the last date and time specified by the Bank as per the document control sheet of this RFP document. The Bank's responses (including the queries, without identifying the source of inquiry) will be provided to respective bidders and published on the Bank's website: www.nainitalbank.co.in. Bidders are responsible for checking this website for any clarifications or corrigenda, as well as the Bank's responses. Please note that responses to pre-bid queries will become part of this RFP document.
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 the Bank's website.

2.9 Amendment of RFP Document

1. 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.
2. Amendment/s, if any, will be notified in writing on the Bank's website www. nainitalbank.co.in under the Tender Section and shall be binding on all bidders. Amendments will be provided in the form of addenda to the bidding documents and will be binding on bidders. It will be assumed that bidders have taken into account the amendments in their bids.
3. From the date of issue, addenda to the tender shall be deemed to form an integral part of the RFP.
4. To afford bidders reasonable time to incorporate the amendments into their bids, the Bank may, at its sole discretion, extend the last date for the receipt of Bids. The extended deadline will be posted on the Bank's website.

2.10 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 their duly authorized representative; in either case, he/she shall submit a certificate of authority. All certificates and documents (including clarifications sought and subsequent correspondence) received hereby, should, 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 as a duly authorized representative of the company.
The authorization must be indicated by a written power of attorney accompanying the bid. Any change in the Principal Officer must be communicated to The Nainital Bank Ltd. in advance. The power of attorney and any other document consisting of adequate proof of the ability of the signatory to bind the Bidder shall be annexed to the bid.

2.11 Application Money & Earnest Money Deposit (EMD)

Bidders shall furnish, as part of their bid, an Application Money & Earnest Money Deposit (EMD) of Rs. 29,500/- (Rupees twenty-nine thousand five hundred only) (Rs. 25,000/- plus GST @18 %) (Non-Refundable) & Rs. 7,00,000/- (Rupees Seven Lakhs Only) respectively as a security. The EMD protects the Bank against risks associated with the bidder's conduct that could warrant forfeiture of the security.

The EMD must be submitted in the form of a Demand Draft/Pay Order/ NEFT/RTGS or Bank Guarantee (BG Format enclosed), valid for six months from the last date of bid submission, from any Scheduled Commercial Bank (except the Nainital Bank Ltd.) favoring The Nainital Bank Ltd., with a claim period of 12 months after the expiry of the validity of the Bank Guarantee, as per statutory provisions. In case the EMD is sent through NEFT/RTGS, such details are to be submitted in Format. **Use the format in Annexure A1 (Bidders letter for EMD)**

In case of bidders being an MSE (with valid Udyog number) under registration of any scheme of the Ministry of MSE, they are exempted from the submission of EMD. A valid certificate in this regard issued by the MSE/NSIC must be submitted along with the bid. **(Please refer pt. no. 2.20 Micro and Small Enterprises clause for details)**

The unsuccessful Bidders EMD will be returned after award of the contract to the successful Bidder by the Bank. **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.**

Electronic or wire transfers can be made to the designated account of The Nainital Bank Limited as detailed below:

- **Account Name:** Adjusting Account
- **Name:** The Nainital Bank Limited
- **Account No:** 0999420300000001
- **IFSC Code:** NTBL0NAI999
- **Branch Name:** Head Office, Nainital
- **Address:** 7 Oaks Building, Mallital, Nainital

The bidder should mention the RFP number and description for reference in the electronic transfer details to the Bank.

2.12 Return of EMD for successful Bidder

The successful bidder's EMD will be returned upon executing the contract and furnishing the Bank Guarantee/security deposit. No interest will be paid on the EMD. The EMD of unsuccessful bidders will be returned after the expiration of the bid validity or the award of the contract to the successful bidder, whichever is earlier. No interest will be paid on the EMD.

The EMD may be forfeited if:

1. The bidder withdraws their bid before the opening of bids.
2. The bidder withdraws their bid after the opening but before notification of award.
3. The selected bidder withdraws their bid/proposal before furnishing the Performance Bank Guarantee.
4. The bidder violates any provisions of the RFP prior to submission of the Performance Bank Guarantee.
5. The selected bidder fails to accept the order within ten days from the date of receipt of the order. The Bank reserves the right to consider late acceptance at its discretion.
6. The bidder fails to submit the Performance Bank Guarantee within the stipulated period from the date of acceptance of the Purchase Order. In this case, the Bank may cancel the order without notice.
7. To comply with any other condition precedent to signing the contract specified in the RFP documents.

2.13 Security Deposit/ Performance Guarantee

The successful bidder will be required to submit a security deposit in the form of a Bank Guarantee favoring The Nainital Bank Ltd. equal to 10% of the purchase order value.

The Guarantee should be issued from any Schedule Commercial Bank Only, other than Nainital Bank Ltd. In the event of non-performance of obligation or failure to meet terms of this RFP or subsequent agreement, the Bank shall be

entitled to appropriate/invoke the security Deposits/Performance Bank Guarantee as the case may be without notice or right of demur to the Bidder. The Bank reserves the right to recover any dues payable by the selected Bidder from any amount outstanding to the credit of the selected Bidder, including the pending bills and/or invoking Guarantee, if any, under the agreement.

2.13.1 Validity

The BG will be valid for 36 months and may be extended for an additional two years if the contract is extended. The BG will be released after 36 months or the extended period, or upon execution of all pending Purchase Orders, whichever is later.

In the event of termination, the Bank may invoke the Performance Bank Guarantee/security deposits, recover direct costs, and pursue other rights or remedies available under the law due to such default and pursue such other rights and/or remedies that may be available to the Bank under law.

2.14 Period of Validity of Bids

Bids shall remain valid for 180 days after the last date of submission of bid date as mentioned in Section 1 or as may be extended. The Bank reserves the right to reject any bid valid for a shorter period as non-responsive, without any correspondence.

2.15 Extension of Period of Validity

In exceptional circumstances, the Bank may request the Bidder(s) for an extension of the period of validity of bids. This request and response shall be made in writing. The extension should be unconditional and irrevocable. The EMD provided shall also be suitably extended. A bidder may refuse the request without forfeiting the bid security.

2.16 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 Agreement/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 the 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/agreement is to be issued.

The bid shall contain no interlineations, erasures, or overwriting, except to correct errors made by the bidder, which must be initialed by the person signing the bid. The bid must be signed by a person or persons duly authorized to bind the bidder to the contract. Such authority must be in the form of a written and duly stamped **Power of Attorney (Annexure- G)** or a Board Resolution certified by the Company Secretary, accompanying the bid.

2.17 Documents comprising the Bids

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

2.17.1 Envelopes A - Eligibility / Pre-Qualification envelope

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

The following documents, in the listed sequence, shall be included in Envelope A:

1. Index
2. Bid submission cover letter
3. Application money in the form of DD/PO in original or details of NEFT (**Annexure A1**)

4. Earnest Bid Money in the form of DD/PO/NEFT/RTGS (**Annexure A2**) or Bank Guarantee (format provided in **Annexure A3**).
   Note: Original EMD in the form of DD / PO or in the form of Bank Guarantee (BG) must be submitted in a sealed envelope mentioning "EMD- RFP Reference No: RFP # NTBL/ISC/SOC/2024/11/22.
5. Bid Offer Form (without price) – **Annexure B**.
6. Bidder Information – **Annexure C.**
7. Declaration of Clean Track Record by Bidder – **Annexure D**.
8. Declaration of Acceptance of Terms and Conditions – **Annexure E.**
9. Declaration of Acceptance of Scope of Work – **Annexure F.**
10. Power of Attorney for signing the bid – **Annexure G.**
    Note: Written power-of-attorney or latest Board Resolution in case of company authorizing the Principal Officer/Authorized representative to submit and duly sign the bid. The power of attorney and any other document consisting of adequate proof of the ability of the signatory to bind the Bidder shall be annexed to the bid
11. Eligibility Criteria Matrix – **Annexure H.**
12. Audited Balance Sheet and Profit and Loss Statements, along with Auditor Reports and Notes to Accounts for the last three years. **Turnover Certificate**
13. CA Certificate stating that the total turnover has never exceeded Rs. 100 Cr since incorporation/registration (if applicable and only for start-ups).
14. RFP Document duly sealed and signed by the authorized signatory on each page.
15. Additional necessary supporting documents.

2.17.2 Envelope B - Technical Bid envelope

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

1. Index
2. Technical / Functional Specifications (Annexure 2)
3. Undertaking for Information Security as per format provided in **Annexure O**
4. Client Details as per – **Annexure- J** also include **Performance Certificate/ Email Confirmation/ Purchase Order** from each client
5. Manufacture Authorization Format (all applicable Original Equipment Manufacturer OEM) **Annexure K**
6. Requirement of manpower skillset **Annexure I**
7. Supporting documents as required in technical score sheet
8. All documents including PowerPoint presentation, solution document, technical compliance, and bill of material in a storage media. Technical compliance and bill of material must be submitted in excel format.
   All documents should be signed and stamped by the authorized person.

Note: The Technical Bid Envelope shall not include any financial information. The inclusion of such information will result in the rejection of the entire bid.

2.17.3 Envelope C - 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")

1. Commercial Bid
2. Commercial Bid Letter
3. Breakdown of Cost Components
4. A standard format for submission of commercial bids has been provided with the tender to be filled by all the bidders. Bidders are requested to note that they should necessarily submit their commercial bids in the format provided in Commercial Bid Format and submission in any other format will lead to rejection of the bid
5. Commercial Bid Form **– Annexure M**
6. Commercial Bid- **Annexure N**

Note: Bidders are requested to compile all the documents in the file and in the sequence as mentioned in points 2.17 , also ensure to index all the papers/documents.

2.17.4 Revelation of Prices

Prices must not be disclosed in any form before the opening of the Commercial Bid; failure to comply will lead to rejection of the offer.

2.17.5 Terms and Conditions of Bidders

Printed terms and conditions of the Bidders will not be considered part of their bids. The terms and conditions outlined in the RFP will prevail.

2.17.6 Consortium

Consortium bids are not allowed.

2.17.7 Last Date & time 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.

2.17.8 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 1- Invitation for Bids, shall stand rejected.

2.17.9 Modification and Withdrawal of Bids

No bid may be altered or modified after the closing time for receipt of bids. Unsolicited correspondence will not be considered. No bid may be withdrawn in the interval between the receipt date of bids and the expiration of the bid validity period. Withdrawal of a bid during this interval may result in forfeiture of the EMD submitted by bidder.

2.17.10 Bidder's Address for Correspondence

The Bidder must designate an official mailing address for all correspondence from the Bank.

2.17.11 Contacting the Bank

Bidders shall not contact the Bank regarding their bids from the time of bid opening until the Contract is awarded. Any attempt or effort by a bidder or any person acting on its behalf, to influence the Bank's bid evaluation or contract award decisions may lead to rejection of the Bidder's bid.

2.17.12 Opening of Bids by Bank

The Bank will conduct a bid opening session as per time schedule and may ask one representative from each bidder After this, Bank will further evaluate the Bid of only those agencies whose application fees, EMD and eligibility criteria are found to be in order.

2.17.13 Evaluation of Bids

Bank will evaluate the bids. The decision of the Bank would be final and binding upon all the Bidders. The purpose of this clause is only to provide the Bidders with an idea/overview 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 RFP 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. The Bidder's bid must be completed in all respect and covering the entire scope of work (Section 3) as stipulated in the RFP Document.

2.17.14 Preliminary Examination

The Bank will examine the bids to determine whether they are complete, whether the bid format conforms to the RFP 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 as required under this RFP.

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.

2.18 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 this RFP.

2.19 Micro and Small Enterprise (MSE/ NSIC - with valid number)

As per recommendations of GOI, the Bank has decided to waive off EMD and tender cost (application money) for Micro and Small Enterprise MSE.

- MSEs/ NSIC with valid number are exempted from paying the application money and Bid security amount for which the concerned enterprise needs to provide necessary documentary evidence. For MSEs Government of India provisions shall be considered while evaluating the tender. Bids received without EMD and tender cost (application money) from bidders not having valid NSIC/ UDYOG number for exemption will not be considered.
- To qualify for EMD & Tender Fee / Cost (application fee) exemption, firms should necessarily enclose a valid copy of registration certificate which is valid on last date of submission of the tender documents. MSE firms who are in the process of obtaining registration will not be considered for EMD & Tender Fee / Cost exemption (application fee).
- MSE bidder must submit a self-declaration accepting that if they are awarded the contract and they fail to sign the contract or to submit a Performance Bank Guarantee before the deadline defined by the Bank, they will be suspended for a period of three years from being eligible to submit bids for contracts with the Bank.
- Bids received without EMD for bidders not having valid registration documents for exemption will not be considered. However, Performance Bank Guarantee has to be submitted by the bidder under any circumstance.

2.20 Due Diligence

Bidders are expected to examine all instructions, terms, and specifications stated in this RFP. The bid shall be deemed to have been submitted after careful study and examination of this RFP document. Bids should be precise, complete, and in the prescribed format as per the requirements of this document. Failure to furnish all information or submitting a bid that is not responsive to this RFP will be at the bidders' risk and may result in rejection of the bid. The decision of The Nainital Bank Limited regarding the rejection of bids shall be final and binding, and the grounds for rejection shall not be questioned after the final declaration of the successful bidder.

2.21 Language of Bids

The bids prepared by the Bidder, along with all correspondence and documents related to the bids exchanged between the Bidder and the Bank, shall be written in English language.

2.22 Contract Period

The Nainital Bank Limited intends for the contract contemplated herein with the successful Bidder for a period of three years, subject to satisfactory SOC services may be extended for 2 years on sole discretion of the Bank.

2.23 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.

2.24 RFP Abandonment

The Bank reserves the right to abandon the selection process at any time before the notification of award.
THE NAINITAL BANK LTD. reserves the right to request a fresh set of documents or seek clarifications on already submitted documents.

3. Section 3 – Scope of Work

As information security monitoring becomes a mission-critical component of any bank's information security strategy, the Bank is seeking a Managed Security Service Provider for Security Operations Center (SOC) services. This provider will assist the Bank in leveraging this technology through a sound implementation approach.

The Bidder is required to integrate the Bank's core infrastructure (servers and other network devices) with the proposed SIEM solution. This includes firewalls/UTM, IPS devices, web security appliances, host intrusion prevention systems, file integrity monitoring solutions, data leakage prevention solutions, web application firewalls, privileged identity management solutions (PIM/PAM), anti-APT solutions, network behavioral anomaly detection, network access control, DAM, Bank Gmail solutions, and more. Logs received from all these devices and applications must be correlated and analyzed for the detection of threats, unusual user behavior, and proactive incident analysis in real-time.

The Bank is looking for a security service provider that can offer a "second layer of eyes" approach on existing internal security controls and monitoring services, augmenting internal capabilities with advanced SOC capabilities focused on detecting advanced threats, beyond traditional rule-based SIEM capabilities. This includes MDR methodology (Managed Detection and Response), Brand Monitoring, Active Directory (AD) security, threat hunting, incident response, and breach investigation. These services will help the Bank adopt a proactive approach in identifying both known and unknown threats, thereby reducing the risk of data and system breaches. The advanced features and capabilities expected from the vendor, in addition to rule-based monitoring, include:

- Security analytics, monitoring, and feeds services
- Threat hunting services
- Managed Detection and Response (MDR)/XDR
- Brand monitoring
- Breach investigation
- AD security

3.1 Technical Specifications: Security Operation Centre (SOC)

3.1.1 A. SOC Monitoring

In addition to the technical specifications, the Bidder shall:

1. The Bidder should perform gap analysis of the SIEM implementation to ensure it meets best practices and bank's requirements.
2. Assist The Nainital Bank Limited in formalizing Standard Operating Procedures (SOPs).
3. Create, update, delete, and maintain all operational documents regarding SOC day-to-day operations.
4. Conduct rule creation and fine-tuning.
5. Manage asset integration.
6. Ensure business continuity through data and configuration backups.
7. Oversee change management, patch management, and version management.
8. Establish KPIs and KRIs to measure SOC performance.
9. Conduct cybersecurity training for Bank-nominated personnel once every six months.
10. Cover a mutually agreed-upon agenda, including products and technologies in the training program.
11. Provide quarterly/half-yearly briefings to the Bank's senior management team on benefits, security risks, and global threats facing the banking industry.
12. Offer relevant support for external and internal security audits, required by regulatory authorities from time to time.
13. Perform quarterly firewall rule base reviews using provided tools/manually, coordinating with the application owner/team.

3.2 Scalability

1. All components of the SOC must support scalability to accommodate continuous growth and meet the demands of various user departments.
2. A modular design of the SOC is an excellent strategy to address growth without major disruptions.

A scalable SOC should easily be expanded or upgraded on demand, as new computing components are constantly deployed, either to replace legacy components or to support new missions.

3.3 Project Timeline

Delivery (installation, go-live, and proposed training) should occur within two months of receipt of the purchase order. Proper training must be provided to The Nainital Bank Limited's Information Security Cell and IT Team, along with relevant HLD, LLD, and other documentation, as well as hands-on experience and video-based knowledge sharing. The Nainital Bank Limited's sign-off is required to conclude the implementation before the operational/maintenance team takes over.

3.4 Project Structure

All team resources included in the RFP should be on the payroll of the Bidder or OEM. The Bidder shall provide on-site resources at each deployment location for their respective solutions during the implementation phase, in case the Bidder cannot resolve The Nainital Bank Limited's queries or delays in implementation, or as necessitated by The Nainital Bank Limited.

3.5 Subcontracting

The Bidder is not permitted to subcontract ongoing operations (including facility management) of the SOC to other organizations.

3.6 Implementation Phase

The Bidder is required to deploy team members according to The Nainital Bank Limited's expected organizational structure for the SOC implementation phase at the defined SOC center. The Bidder is required to provide team details in line with the roles and responsibilities defined below.

3.6.1 Roles and Responsibilities:

A Senior Management member from the Bidder shall be identified as the project sponsor; her or his responsibilities are outlined below:

1. Primarily accountable for successful implementation of the project across The Nainital Bank Limited.
2. Act to remove critical project bottlenecks.
3. Identify working team members, project management office members, and team leads.
4. Serve as the single point of contact for The Nainital Bank Limited's senior management.
5. Participate in the steering committee for implementation at The Nainital Bank Limited.
6. Ensure implementation timelines are met to achieve the desired results.
7. Monitor change management activities.
8. Monitor quality and risk-related activities.
9. Identify and implement best practices across The Nainital Bank Limited.
10. Provide periodic reports to The Nainital Bank Limited on the status, issues/challenges faced, and how these are addressed.

3.6.1.1 Team Lead

1. Lead daily implementation efforts.
2. Report on progress to the PMO (Project Management Office) and The Nainital Bank Limited.
3. Identify and report any risks to the PMO and The Nainital Bank Limited.
4. Seek advice from the PMO on mitigation measures for The Nainital Bank Limited Working Team.
5. Implement all devices in scope.
6. Customize devices as per requirements.
7. Perform acceptance testing for each device/solution.
8. Ensure customization is in line with The Nainital Bank Limited's requirements.

3.7 Operations Phase

1. Bidders should mention the number of resources required for managing the SOC in the Resource Plan Matrix format for The Nainital Bank Limited.
2. This deployment should ensure a 24/7 operational SOC with DR capabilities.
3. The cost of the resources as provided in the final commercial bill of materials shall be considered fixed for the term of the project.
4. Any change in manpower requires The Nainital Bank Limited's strict approval.

3.8 Manpower Support working days' schedule (onsite/off site)

Sr.No.	Job Profile	Place	Working days
1	SOC Operators L1	SOC Centre	365
2	SOC Analysts L2	SOC Centre	Monday to Sunday
3	SOC Manager L3	SOC Centre	Monday to Sunday

3.9 Manpower at The Nainital Bank Limited

Sr.No.	Job Profile	Place (Remote)	Working days
1	SOC Operators L1	Information Security Cell (Nainital Bank)	6:00 AM to 3:00 PM
2	SOC Operators L1	Information Security Cell (Nainital Bank)	1:00 PM to 10:00 PM
3	SOC Analysts L1	Information Security Cell (Nainital Bank)	9:30 AM to 6:30 PM

Important Note: - Bidder should ensure to submit separate quotations for One (1) L1, Two (2) L1 & One (1) L1 & One (1) L2 for onsite Location.

3.10 Security Device Management / Support

1. Provide 24x7 security device management and incident mitigation services (Hybrid option: 6 AM to 10 PM onsite, with offsite (remote) support during remaining hours and holidays preferred). An onsite resource may be required during off-hours or critical activities, based on prior intimation.
2. The proposed solution should support 24x7 phone/email fault reporting by a designated customer administrator, with escalation to principal vendors.
3. Regular sessions should be held to discuss improvements in SOC performance.
4. The Bidder should provide an escalation hierarchy matrix as an annexure as per Appendix – A
5. Qualification of L1 and L2 will be reviewed after final selection of bidder.

3.11 Security Advisory Services/ Security Incident and Crisis Management Services

1. Track and advise on new global security threats and vulnerabilities.
2. Provide proactive IOCs and recommendations for remediation.
3. Issue alerts on critical outbreaks, global risks, and critical patches applicable to the systems and technologies.
4. Deliver Information Security awareness mailer content for various domains (e.g., phishing, web security, physical security) on a monthly basis.
5. Align the Security Incident Management Plan with NTBL's Cyber Crisis Management Plan (CCMP) and Cyber Security Policy. (The Cyber Crisis Management Plan (CCMP) and Cyber Security Policy will be provided to shortlisted bidders.)
6. Incident and cyber crisis management support should be primarily offsite, with onsite support being mandatory in emergencies.
7. Provide a detailed process for managing cyber incidents, describing each phase: prepare, identify, contain, eradicate, recover, and learn from incidents.
8. Develop a response plan/strategy that prioritizes incidents based on organizational impact.
9. Establish processes for identifying, preventing, detecting, analyzing, and reporting all Information Security incidents according to best practices, with revisions as necessary.
10. Conduct incident and problem management, resolution, root cause analysis, and reporting within required time limits.
11. Describe the incident response process, including roles, responsibilities, and scope of action in line with CCMP.
12. Perform root cause analysis for security incidents and recommend controls to prevent recurrence.
13. Provide on-demand timely support, including investigation and forensic analysis of logs, ensuring necessary analysis is performed and required data is provided promptly.
14. Enhance incident response by replacing purely ad-hoc activities with advanced playbooks, analytical tools, incident management tools, and reporting, allowing security analysts to focus more on analysis.
15. Offer backend professional incident management team support in case of severe incidents.

3.12 Pert Chart

Description	W1	W2	W3	W4	W5	W6	W7
Project Plan							
Build & Provision							
Onboarding of Log Sources							
Training for the Bank							
Alerts, Configure Reports SOP's							
Business as usual							

4. Section 4 – Eligibility Criteria

4.1 Eligibility Criteria

The Eligibility Criteria has been furnished below:

A. Start-ups:

Criteria	Justification
Company Type	The bidder should be incorporated as a Private Limited Company, a Registered Partnership Firm or a Limited Liability Partnership and should have the Certificate issued by Department for Promotion of Industry and Internal Trade (DPIIT) or in the process of applying the same and shall be submitted before a formal engagement with" The Nainital Bank Limited.
Annual Turnover	Should have an annual turnover not exceeding Rs. 100 crore for any of the financial years since its Incorporation.
Company Age	Period of existence and operation should not exceed 10 years from the Date of Incorporation.
Original Entity	Entity should not have been formed by splitting up or reconstructing an already existing business
Blacklisting Status	Neither the OEM nor the Bidder should have been currently blacklisted by any Bank or institution in India.
Innovative & Scalable	Should work towards development or improvement of a product, process or service and/or have scalable business model with high potential for creation of wealth & employment
Other Criteria	The bidder should be authorized to quote and support for OEM products and services. The bidder shall not get associated with the distribution channel once in any other capacity once he is eligible for price discussion.

B. Other than start-ups:

#	Eligibility Criteria	MSME	Other than MSME
1	**Registration and incorporation**	The bidder is a Company/ LLP registered in India under the Companies Act or Partnership under Partnership Act for at least since last 3 years. a. In case the bidder is the result of a merger or acquisition, at least one of the merging companies should have been in operation for at least 3 years as on date of submission of the bid. b. In case the bidder is the result of a demerger or hiving off, at least one of the demerged company or resulting company should have been in operation for at least 2 years as on the date of submission of bid.	The bidder is a Company/ LLP registered in India under the Companies Act or Partnership under Partnership Act for at least since last 5 years. a. In case the bidder is the result of a merger or acquisition, at least one of the merging companies should have been in operation for at least 5 years as on date of submission of the bid. b. In case the bidder is the result of a demerger or hiving off, at least one of the demerged company or resulting company should have been in operation for at least 5 years as on the date of submission of bid.
2	**Turnover & profitability**	The bidder should have reported a minimum annual turnover of Rs. 20 crores and should have reported profits (profit after tax) as per audited financial statements in at least 2 out of last 3 financial years (FY 2021-22, 2022-23, 2023-24). In case audited financial statements for most recent financial year are not ready, then CA/management certified financial statement shall be considered. In case the bidder is the result of a merger or acquisition or demerger or hive off, due consideration shall be given to the	The bidder should have reported a minimum annual turnover of Rs. 30 crores and should have reported profits (profit after tax) as per audited financial statements in at least 2 out of last 3 financial years(FY 2021-22, 2022-23, 2023-24). In case audited financial statements for most recent financial year are not ready, then management certified financial statement shall be considered. In case the bidder is the result of a merger or acquisition or a merger or hive off, due consideration shall be given to the past

		past financial results of the merging entity or demerged entity to determine the minimum annual turnover to meet the eligibility criteria; should the bidder be in operation for a period of less than 2 financial years. For this purpose, the decision of bid opening Committee of the "The Nainital Bank Limited" will be treated as final and no further correspondence will be entertained on this.	financial results of the merging entity or demerged entity as the case may be to the minimum annual turnover to meet the eligibility criteria; should the bidder be in operation for a period of less than 2 financial years. For this purpose, the decision of bid opening Committee of the "The Nainital Bank Limited" will be treated as final and no further correspondence will be entertained on this.
3	**Governance – Statutory obligations**	There shall be no continuing statutory default as on date of submitting the response to the tender. Necessary self-declaration along with extract of auditors' report.	There shall be no continuing statutory default as on date of submitting the response to the tender. Necessary self-declaration along with extract of auditors' report.

C. Other Eligibility Criteria

Sr. No.	Clause	Documents Required
1.	The bidder's organization should be ISO 27001 certified.	Certified copy of Certificate issued by competent authority
2.	Blacklisting: Neither the OEM nor the bidder should have been currently blacklisted by any Bank or institution in India or abroad.	Self-certification certificate duly signed by authorized signatory on Bidder's letter head.
3	The bidder should be authorized to quote and support OEM products and services. The bidder shall not get associated with the distribution channel once in any other capacity once he is eligible for price discussion. The bidder must be authorized partner of quoted OEM.	OEM Authorization Letter from all OEMs whose products are being proposed and MAF (Manufacturer's Authorization Form) to be submitted.
4	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. **(*Visit of SOC may be conducted by the Bank.)**	Self-Declaration certificate, giving location details of the SOC owned by them in India along with details of the proposed location for Bank and DR facility.
5	Bidder must have been providing Managed Detection and response services to minimum two (2) BFSI customers during last 3 years in India. The bidder should be providing SOC Service to at least 1 Govt./ PSU/ BFSI customer from more than 1 year. Deployed solutions license may or may not be on Bidder's name. The bidder's experience in providing Managed Security Services (MSS) to run Security Operations Centre (SOC) services with Managed Detection and Response (MDR) capabilities in India.	The bidder must submit Purchase Order/Satisfactory Certificate from the organization as supporting documents for the same.
6	Implementation References-Minimum 2 The bidder should have reference of currently providing Managed Security Services for clients in India.	Annexture for the same is include in the RFP
7	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. (mandatory)

8	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. (mandatory)
8	Knowledge, skills, and experience of the Team Leader and Technical Engineer on SIEM and SOC solutions and services implementation and support. The bidder must have skilled OEM-certified staff at various levels (L1/L2/L3) for MSSP services.	Certificate from bidder's HR along with OEM certificate copy
9	Bidder should have certified / skilled resources for SOC / Incident response services. Minimum 5 OSCP / CHFI / CISA / CSA / CISM / CISSP & 10 CEH resources on their payroll.	Certificate of relevant resources
9	MSSP should have a remote SOC which is certified in major industry certifications including: 1. ISO- 27001:2013 (ISMS) – M 2. ISO-20000-1:2011 (ITSM) – O 3. ISO-9001:2015 (QMS) – O 4. ISO 22301:2012 (BCMS) – O 5. PCI-DSS v3.2.1 – O 6. CERT-In Empanelment – O 7. Service Organization Control (SOC) 2 – O 8. SOC 3 – O 9. Any other	Certified copy of Certificate issued by competent authority (2 M- Mandatory) Bidders has to submit maximum certification as it preference will be given for vendor having major industry certifications including:
10	Bidder should have handled Minimum 5 Incident handling and minimum 2 in BFSI involving fraudulent activities like money transfer, ATM etc. Ransomware / Virus incidents will not be considered.	Purchase order or equivalent document to be submitted.
11	Should have a running licensed commercial SIEM tool in environment. Deployed tool should be in Leader Quadrant in Gartner MQ for last 3 Years	Required snapshot/ document to be submitted

5. Section 5 - Bid Opening

Bids will be opened in 2 stages:
Stage 1 – In the first stage the Eligibility bid i.e. Envelope 'A' and Technical Bid i .e. Envelope 'B' will be opened.
Stage 2 – Commercial bids i.e. Envelope 'C' will be opened for technically qualified bidders for finalizing the prices by Nainital Bank's management.

5.1 Opening of Eligibility and Technical Bids Envelope A and Envelope B

Nainital Bank will open Eligibility bids (Envelope 'A') and technical bid (Envelope 'B') on the date, time and address mentioned in Section 1 or as amended by Nainital Bank from time to time.

5.2 Opening of Commercial Bids Envelope C

Those Bidders who meet the eligibility criteria and technical criteria will be intimated by email, the date, time and address for opening of the Commercial Bids. The bank may ask for the bidders' representative. If called for the Bid opening, the representatives of the Bidder have to produce an authorization letter from the Bidders by way of letter or email to represent them at the time of opening of bids. Only one representative will be allowed to represent each Bidder.

In case the Bidder's representatives are not present at the time of opening of Bids, the Bids will still be opened at the scheduled time at the sole discretion of the Nainital Bank Limited.

The Bidder's representatives who are present shall sign the register evidencing their attendance.

6. Section 6 - Bid Evaluation

Competitive bids shall be submitted in three stages:

6.1 Stage 1 – Evaluation of Eligibility Criteria

1. Whether the required information has been provided as outlined in the bid document.
2. Whether the documents have been properly signed and whether the bids are generally in order.
3. Eligibility and compliance with all forms and annexures will be the first level of evaluation.
4. The Bank may waive any minor informality, non-conformity, or irregularity in a bid that does not constitute a material deviation, provided such waiver does not prejudice or affect the relative ranking of any bidder.
5. If a bid is not substantially responsive, it will be rejected by the Bank and may not subsequently be made responsive by the bidder through correction of the non-conformity.

6.2 Stage 2 – Evaluation of Technical Criteria

1. Only those bidders who qualify all pre-qualification/eligibility criteria requirements will be eligible for technical bid evaluation.
2. A technical presentation will be part of the evaluation process for the bids.
3. The Bank reserves the right to reject a product/solution/service if it believes the offered product/service does not meet the technical requirements/objectives specified in the Technical Bid – Bank's Requirements.
4. The technical bid will first be reviewed to determine compliance with the tender terms and conditions, minimum/mandatory technical requirements, and the scope of work as defined in this tender.
5. Any bid found to be non-compliant with the mandatory technical requirements, tender terms and conditions, and the scope of work shall be rejected and will not be considered for further evaluation.
6. Bids that are technically compliant will only be considered for commercial evaluation.
7. Bidders should submit the Technical Specification Compliance Sheet as part of the technical bid.
8. If the bidder is found to be non-compliant with any of the mandatory technical specifications, the respective bid will be summarily rejected without assigning any score.
9. Bidders are required to submit all supporting documents as per the criteria mentioned in the RFP. The Bank reserves the right to summarily reject any bid that does not contain all mandatory supporting documents or may ask the bidder to resubmit documents. The decision of the Bank will be final and binding in this regard.

The Technical Evaluation will be based on the following broad parameters:

Technical Scoring Matrix

Sr No	Criteria	Max Marks
1	Eligibility criteria	20
2	In the last 3 years, Bidders Experience captive SOC/Managed SOC implementations in government/BFSI/PSU in India and Bank. And current running Soc solutions.	10
3	The bidder's experience in providing Managed Security Services (MSS) to run Security Operations Centre (SOC) services with Managed Detection and Response (MDR) capabilities in India.	5
4	The bidder's experience in providing Incident Response (IR) / Digital Forensics and Incident Response (DFIR) services to BFSI customers for cases involving financial impact.	5
5	Architecture & SIEM solution	10
6	Technical Evaluation of SOC	20
7	Bidder's technical presentation for proposed Solution & SOC visits (if feasible)	30

6.3 Stage 3 – Evaluation of Commercial Bids

6.3.1. Commercial Bid Format - SOC Services

S.No.	Services	Months/Hours	Amount (GST Extra)
1	Managed Security Services to run the Bank's Security Operations Centre (SOC/SIEM) with Managed Detection and Response (MDR), along with Brand Monitoring, Active Directory security, and Threat Hunting capabilities.	36 Months	
2	Incident Response and Breach Investigation (as per requirement)	30 days	
	Total (Taxes Extra)		

Approximate EPS Count is around 6000/-

The device count for calculation Managed Security Services to run the Bank's Security Operations Centre (SOC/SIEM) will be provided to Bidder Only after NDA with the bank in the format, if necessary.

6.3. Rate Discovery for Resident Engineer

#	Rate Discovery	Qty	Price excl taxes - Yearly
1	Onsite Engineer -L1 resource	1	
2	Onsite Engineer -L1 resource	2	
3	Onsite Engineer -L2 resource	1	
4	Onsite Engineer L1 resource and L2 resource	1 each	

All bids shall be evaluated by different Bid Evaluation Committees/Subcommittees set up for this purpose by the Bank. The evaluation will be based on Eligibility Criteria, Technical Evaluation Criteria, and Evaluation of Commercial Bids. Bidders must pass the Eligibility Criteria to be considered for Technical Evaluation. The marks obtained in Technical Evaluation will carry a 70% weightage when comparing the Commercial Bids.
The resultant score will be calculated for all qualified bidders using the following formula:
Score (S) = [(C1 / C) x 0.3] + [(T / TMax) x 0.7]
Where:

- S: Resultant Score
- C1: Lowest Commercial Bid
- C: Commercial Bid of the bidder
- T: Technical Score of the bidder
- TMax: Highest Technical Score

Illustrative Example:

Sr. No.	Bidder	Technical Evaluation Marks (T)	Commercial Bid (C)	[(C1 / C) x 0.3]	[(T / TMax) x 0.7]	Score (S)
1	ABC	95	80	(95 / 95) x 0.3 = 0.3	(95 / 95) x 0.7 = 0.7	0.925
2	PQR	80	70	(60 / 70) x 0.3 = 0.257	(80 / 95) x 0.7 = 0.589	0.846
3	XYZ	75	60	(60 / 60) x 0.3 = 0.3	(75 / 95) x 0.7 = 0.553	0.853

Scores will be considered up to two decimal places. In this example, bidder ABC, with the highest score, becomes the successful bidder. The eligibility criteria, technical evaluation criteria, and commercial bid formats are provided in the annexures. Bidders must provide information in the prescribed formats only; any deviation from these formats may lead to disqualification.

7 Section 7 - Terms and Conditions

7.1 Bank's Right to Vary Scope of Contract at the Time of Award

The Bank may, at any time, issue a written order to the Bidder to 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 be accordingly amended. Any claims by the Bidder for adjustment under this clause must be asserted within thirty (30) days from the date of the Bidder's receipt of the Bank's change order.

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

The Bank reserves the right to accept any bid, to annul the RFP/tender process, and to reject all bids at any time prior to the award of the Contract, without 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.

7.3 Notification of Award

Prior to the expiration of the period of bid validity (180 days after the last date of submission of bid date), 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 a Bank Guarantee favoring 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 return/release its EMD.

7.4 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 favoring The Nainital Bank Ltd. of 10% of the Work/Purchase Order Value for contract performance. The contract period will commence from the date of signing and will be valid for 3 years, which may be extended for an additional 2 years at the sole discretion of the Bank.

Keeping in view the project commitment, The Nainital Bank Ltd. reserves the right to ask the bidder 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. Bidder has to agree for honoring 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 changes to describe substantially the same system/service/process under a new name, all techno-fiscal benefits agreed upon concerning the original product shall be passed on to The Nainital Bank Ltd. The obligations with The Nainital Bank Ltd. taken by the bidder with respect to the product/works/services with the old name shall also transfer along with the renamed product/works/services.

The Security Deposit shall be in the form of a Bank Guarantee (BG) from any Scheduled Commercial Bank (except the Nainital Bank Ltd.). The Security Deposit should be valid for the entire period of 36 months and shall be renewed for extended period required. Upon satisfactory performance and completion of the contract, the Security Deposit shall be refunded to the bidder without any interest.

7.5Termination of contract:

1. The Bank shall serve the 30 days' notice of termination to the Shortlisted bidder before terminating the contract of the selected bidder.
2. The Bank will be entitled to terminate the contract, without any cost to the Bank and recover expenditure incurred by the Bank, on the happening of any one or more of the following:
    - The selected bidder commits a breach of any of the terms and conditions of the bid.
    - The selected bidder goes into liquidation voluntarily or otherwise or appointment of receiver or manager of any of the successful bidder's assets or insolvency of the successful bidder.
    - Distress, execution or other legal processes being levied on or upon any of the successful bidder's goods and/ or assets.
    - If the successful bidder assigns or attempts to assign his interest or any part thereof of the project assigned.
    - An attachment is levied or continues to be levied for a period of 7 days upon effects of the Agreement.

- The progress regarding the execution of the order accepted by the successful bidder is found to be unsatisfactory or delay in execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving 30 days' notice for the same. In this event, the successful bidder is bound to make good the additional expenditure, which the Bank may have to incur in executing the balance contract. This clause is applicable if for any reason the contract is cancelled.
- Non-satisfactory performance of the successful bidder during implementation and operation.
- An act or omission by the successful Bidder, its employees or its agents in the performance of the services provided in the contract and this RFP including delay in performance of the services beyond the specified period or any other reason which in the judgment of the Bank does warrants termination of contract
- Failure to perform services to the satisfaction of Bank.
- Material discrepancies in the Services noted by the Bank. The Bank reserves the right to procure the same or similar service from the alternate sources at the risk, cost and responsibility of the Successful bidder.
- Successful bidder is found to be indulged in frauds.
- The Bank suffers a reputation loss on account of any activity of empaneled vendor or penalty is levied by regulatory authority.
- In the event of subcontract or assignment contrary to the terms of agreement

FURTHERMORE, 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. Moreover, Bank will be informed in advance through written notice of likely event of any takeover/merger/acquisition/transfer of ownership of Bidder. If the contract is terminated by the Bank, the Bank shall also be entitled to get back the infrastructure and hardware, if any, provided by the Bank. Termination of contact by the Bank may also be accompanied by a de-facto blacklisting of the successful bidder.

7.6 Conflict of Interest

The Bank requires that bidder shall provide professional, objective, and impartial advice and at all times hold the Bank's interest paramount, strictly avoid conflicts with other Assignment(s)/ Job(s) or their own corporate interests and act without any expectations/ consideration for award of any future assignment(s) from the Bank. Bidder has an obligation to disclose any situation of actual or potential conflict in assignment/job, activities and relationships that impacts their capacity to serve the best interest of the Bank, or that may reasonably be perceived as having this effect. If the Bidder fails to disclose said situations and if the Bank comes to know about any such situation at any time, it may lead to the disqualification of the Bidder during bidding process or the termination of its Contract during execution of assignment

7.7 Placing of Purchase Orders

1. Purchase order will be placed on the vendor in hardcopy format for procurement of proposed solution / Hardware/ Software/ System / Service.
2. Objection, if any, to the Purchase Order must be reported to the Bank by the vendor within five (5) working days counted from the date of receipt of Purchase Order for modifications, otherwise it is assumed that the vendor has accepted the Purchase Order.
3. If the vendor is not able to supply/deploy/operationalize the ordered Hardware/software system/service/process/solution completely within the specified period, the penalty clause will be invoked.
4. 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.
5. Bank Guarantee for Contract Performance: Within thirty days of receiving the notification of award from the Bank, the successful Bidder shall furnish a performance security in the form of a Bank Guarantee

favoring The Nainital Bank Ltd., valid for a period of 36 months from the date of signing the Contract, in accordance with the Conditions of Contract.

6. Failure of the successful Bidder to comply with the requirements mentioned in the document shall constitute sufficient grounds for the annulment of the award and forfeiture of the EMD and Bank Guarantee/Security Deposit for contract performance. In the event of exigency, if the Bank engages another party to perform the work, the difference in cost shall be borne by the successful Bidder.

7.8 Performance Bank Guarantee Schedule:

S.No.	Item	Value
1	Instrument	One single Deposit in the form of Bank Guarantee
2	Validity of Performance Bank Guarantee	Bank Guarantee for contract performance to be submitted along with the duly stamped and signed contract and should be valid for a period of 36 months from the date of signing the Contract. In case there is an extension of contract beyond 06 months, Bidder has to provide the BG for that extended period.
3	Amount	10% of Purchase Order value.

7.9. Confidentiality and Non-Disclosure of the Document

The RFP Document submitted by the bidder is confidential. The Bidder shall ensure that no part of the RFP Document is disclosed in any manner. The document contains information that is proprietary to the Bank. Additionally, the bidder will have access to internal business information of the Bank and its associates. The bidder shall ensure that its employees maintain full confidentiality of all information. Disclosure, reproduction, or transmission of this RFP, any amendments, specifications, plans, drawings, patterns, samples, or any related information to parties not directly involved in providing the requested services may result in disqualification, premature termination of the contract, and legal action for breach of trust.

No media release, public announcement, or reference to the RFP or any related program shall be made without the Bank's written consent. Reproduction of the RFP or any other document without written consent of the Bank, through photographic, electronic, or other means, is strictly prohibited. The successful bidder will be required to sign a Confidentiality and Non-Disclosure Agreement with the Bank.

7.10. Prevention of Corrupt and fraudulent practices:

It is required that every participating bidder is required to sign a pact:

1. Every Bidders / Suppliers / Contractors/Service Providers are expected to observe the highest standard of ethics during the procurement and execution of such contracts in pursuance of the policy.
2. "Corrupt Practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of an official in the procurement process or in contract execution AND
3. "Fraudulent Practice" means a misrepresentation of facts to influence a procurement process or the execution of contract to the detriment of the Bank and includes collusive practice among Bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the Bank of the benefits of free and open competition.
4. The Bank reserves the right to reject a proposal for award if it determines that the Bidder recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.
5. The Bank reserves the right to declare a firm ineligible, either indefinitely or for a stated period of time, to be awarded a contract if at any time it determines that the firm has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

7.11. Tender Related Condition

The Bidder must confirm unconditional acceptance of full responsibility for completing the job and executing the 'Scope of Work' as detailed in 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 matters related to the Contract. The Bidder should not be involved in any major litigation or arbitration that may impact the delivery of services as required under this contract. If any suppression or falsification of such information comes to the Bank's attention during the tendering process or during the term of the Contract, the Bank shall have the right to reject the bid or terminate the contract without any compensation to the Bidder and/or claim damages before the court resulting from such rejection or termination.

7.12. Rejection Criteria

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

7.13. General Rejection Criteria

Bids submitted without or with improper EMD and/or Application Money.

1. Bids received through telex, telegraphic means, fax, or email will not be considered for evaluation.
2. Incomplete Bids, including non-submission or non-furnishing of requisite documents/ Conditional Bids / Bids not conforming to the terms and conditions stipulated in this RFP are liable for rejection by the Bank.
3. Bids that do not confirm unconditional validity as prescribed in the Tender.
4. If the information provided by the Bidder is found to be incorrect or misleading at any stage during the Tendering Process.
5. Any effort by a Bidder to influence the Bank's bid evaluation, comparison, or contract award decisions.
6. Bids received after the last date and scheduled time for receipt as prescribed by the Bank.
7. Bids lacking power of authorization and any other document providing adequate proof of the signatory's ability to bind the Bidder.

7.14. Technical Rejection Criteria

1. Technical bids containing commercial details.
2. Revelation of prices in any form or by any reason before the opening of the Commercial Bid.
3. Failure to furnish all information required by the RFP Document or submission of a bid not substantially responsive to RFP document in every respect.
4. Bidders not quoting for the complete scope of work as indicated in the RFP Document, corrigendum/ addenda (if any), and subsequent information given to bidders.
5. Bidders not complying with material technical requirements regarding functionality, specifications, and general terms and conditions as stated in the RFP Document.
6. The Bidder not confirming unconditional acceptance of full responsibility for providing services.
7. If the bid does not conform to the timelines indicated. (PERT CHART)
8. Bidders not scoring the minimum marks as mentioned in the Tender.

7.15 Commercial Rejection Criteria

1. Incomplete Commercial Bid.
2. Financial bids that do not conform to the Tender's commercial bid format.
3. Total price quoted does not clarify regarding all statutory taxes and levies applicable.
4. 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, its bid may be rejected.

7.16 Liquidated Damages

1. If the selected Bidder fails to complete the contract performance in accordance with the agreed specifications and conditions, the Bank reserves the right to recover liquidated damages (LD) at a rate of 0.5% of the total yearly order value per week, subject to a maximum of 10% of total charges for non-performance or delayed performance.
2. LD is not applicable for delays due to reasons attributable to the Bank or force majeure. However, it is the Bidder's responsibility to prove that the delay is attributable to the Bank or force majeure. The selected Bidder shall submit proof authenticated by the Service Provider and a Bank official that the delay is attributed to the Bank or force majeure along with the bills requesting payment. If the delay is due to the Bank, force majeure, or any other circumstances beyond the Service Provider's control, the Bank will continue with the contract without claiming any liquidated damages. The Bank reserves the right to adjust any penalties and liquidated damages against the Security Deposit.

7.17 Force Majeure

Bank shall not be responsible for delays or non-performance of any or all obligations, contained in this RFP or agreement thereafter, caused by war, revolution, insurrection, civil commotion, riots, mobilizations, strikes, blockade, acts of God, Plague, epidemics or pandemics, 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 the bank, which directly, materially and adversely affect the performance of any or all such obligations. However, the bidder shall continue to perform its obligations as contained in this RFP and agreement thereafter.

7.18 Arbitration

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

7.19 Jurisdiction

The jurisdiction for all disputes shall be in Nainital, Uttarakhand, India.

7.20 Safety

All safety codes and preventive measures for this type of work shall be strictly followed. All personnel and staff will remain under the authority of the bidder. In the event of any mishap causing injury, disability, or death on-site or off-site during or after the project due to negligence by the bidder's staff, the bank shall not bear any responsibility in any case. No claims in this regard shall be paid by the bank.

7.21 Statutory Laws:

The vendor shall comply with all applicable statutory rules, regulations, and notifications regarding taxes, duties, labor, and other relevant matters in force at any given time, including registration, labor laws, payments, ESIC, PF, insurance etc. The vendor shall coordinate these matters directly with the relevant authorities directly.

Service Provider shall procure and maintain all necessary licenses, permissions, approvals from the relevant authorities under the applicable laws throughout the currency of this Agreement, require for performing the Services under this Agreement

7.22 Confidential Information:

All information exchanged between the parties will remain confidential. If the implementation project requires the disclosure of, or receipt of confidential information, such actions will be made with mutual agreement and may involve a separately executed MoU or non-disclosure agreement with the vendor by the bank.

7.23 Extra Deviated Items:

Any extra items, such as variations in quantity/quality of services, must be executed only after receiving appropriate approvals and written confirmation from the bank. At the time of invoice submission, all documentary evidence of the necessary approvals for extra/deviated items or variations in quantities/ quality must be attached. Payments will not be made without proper approvals.

7.24 Term and Extension of the Contract

The term of this Contract shall commence from the date of signing contract (covering both Phases 1 – Implementation and 2). It may be extended for an additional two years at the sole discretion of the Bank. The Bank reserves the exclusive right to grant any extension to the a fore mentioned term and shall notify the Bidder in writing at least six months before the expiration, indicating whether an extension will be granted. The decision to grant or refuse the extension shall be at the Bank's discretion.

If deemed appropriate, during the extended period, the terms and conditions for the Service Level Agreement (SLA), penalties, and prices for services, Annual Maintenance Contract (AMC), and manpower shall remain the same.

Should the Bank determine that no further extension will be granted, it will notify the Bidder at least six months prior to the expiration of the term. Upon receipt of such notice, the Bidder shall continue to fulfill all obligations under the Contract until such reasonable time beyond the contract term, during which the Bank will either appoint an alternative service provider or establish its own infrastructure to operate the Services provided under this Contract. In this case, the terms and conditions for SLA, penalties, and prices for services, AMC, and manpower shall remain the same as those specified for the third year.

7.25 Prices

Prices quoted must be firm and shall not be subject to any upward revision for any reason throughout the contract period. However, any increase or decrease in taxes or duties occurring after the Notification of Award shall be passed on to The Nainital Bank Limited.

The quoted cost should include licensing and monitoring services provided through the vendor's Security Operations Center (SOC) on a 24x7x365 basis. Additionally, the cost must cover the integration of the bidder's Security Information and Event Management (SIEM) solution with the Bank's existing devices, as no separate charges will be paid for this integration.

Under no circumstances shall any additional costs be payable by the Bank for any software or tools used by the service provider in rendering the required services outlined in the tender. The bidder must arrange for such software or tools at their own expense. The responsibility for ensuring that only legal, authorized, and licensed versions of software or tools are provided and used by its employees' rests solely with the bidder. The Bank shall not be involved in any litigation arising from the use of unauthorized software or tools by the bidder or service provider.

7.26 Payment Terms

Payments will be released only upon satisfactory acceptance of the deliverables for each task, according to the following schedule (for both phases):

Sr. No.	Details
1	Payment would be done on quarterly basis at the end of the quarter upon receipt of 3 monthly invoice from vendor after the SLA verification.

All payments shall be made exclusively in Indian Rupees and will be released by the Bank against the invoices raised by the Bidder within 30 calendar days, provided that all relevant documents are submitted promptly and are complete in every respect.

The bidder request(s) for payment shall be made to "The Nainital Bank Ltd." in writing (Invoice) accompanied by Service Level Requirements compliance reports for which payment is being claimed.

All the payments to the bidder shall be subject to the report of satisfactory accomplishment of the concerned task.

Penalties, if any, on account of liquidated damages and non-compliance of Service Level Requirements, shall be deducted from the invoice value.

Payments will be released only on satisfactory acceptance of the deliverables for each Task as per the particulars mentioned in the commercial bid format.

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.
- No advance payment will be made.

8. Section 8: Service Level Agreement & Penalties

8.1 Service Levels during implementation phase

1. Time is the essence of contract.
2. The Bidder is expected to complete the responsibilities that have been assigned as per the Project timelines which is agreed by both the parties.
3. One percent of the total implementation fees would be levied as a penalty for every one-week delay as per implementation timelines per product/service. Or The bidder is required to adhere to the service level agreements as mentioned below for the Implementation phase.

8.2 Responsibility Matrix

The following table describes the responsibilities of the bidder, Bank (The Nainital Bank Limited) and original equipment manufacturer for problem management and issue resolution related to the applications and tools proposed by the bidder**.**

#	Activity	Bank	Bidder / OEM
1	SOC Solution Design	S	P
2	Installation / Configuration as per the solution design	S	P
3	Acceptance of the solution	S	P
4	SOC Operations - Ongoing	S	P
5	SOC Operations Review –Biannual) / Incident based Audit	S	-
6	SOC (SIEM use cases Review) Half-yearly	S	P
7	SLA Reports	S	P
8	Incident Management	S	P
8	"P" - Performed (Primary responsibility for executing the activity) "S" – Signed Off (Responsible for providing the go-ahead)		

Appendix-A – Escalation Matrix

Service level Category	Response/Resolution Time	Escalation thresholds			
		Escalation Level 1		Escalation.....	
		Escalation to	Escalation Mode	Escalation to	Escalation Mode
Production Support		<Name, designation contact no.>			
Service Milestones		<Name, designation contact no.>			
Infrastructure Management		<Name, designation contact no.>			
Application Development & Maintenance		<Name, designation contact no.>			
Service Desk Support		<Name, designation contact no.>			

Stipulated Time Schedule

The key milestone dates anticipated by the Bank are as follows:

Date of release of Purchase Order and project timelines, including penalties:

- Date of release of Purchase Order: T Day
- Purchase Order acceptance by successful bidder: T + 5 days

Sr.	Roadmap	Project Timelines (i.e., "T")
1.	Phase 1 1: - List of requirements to be shared with the Bank. - Bank's readiness with requirements. - Delivery, installation, configuration, and commissioning of all Managed Security Services as defined in the RFP document. Phase 2 Go Live and Operational phase	T + 10 days T + 15 days 45 days from the date of confirmation letter for the Bank's readiness

The Bidder shall perform the Services and comply fully with the critical dates. Any failure by the Bidder to meet these critical dates may lead to the imposition of obligations outlined in the Delay and Deterrent Mechanism, the levying of penalties, and/or termination of the Contract at the Bank's discretion, without prejudice to any other rights the Bank may have.

8.3 Service Level Agreement (SLA) & Targets

The SLA, as described, establishes the minimum service levels required based on performance indicators and measurements. The Vendor shall ensure the provision of all required services while continuously monitoring performance to effectively comply with these levels.

The services provided by the Vendor will be reviewed quarterly by THE NAINITAL BANK LTD., which will:

- Evaluate the Vendor's performance against the SLA over the three-month review period, considering key issues from past performance statistics, including major incidents and service trends.
- Discuss escalated problems, new issues, and outstanding matters requiring resolution.
- Review statistics related to the rectification of outstanding faults and agreed-upon changes.
- Solicit suggestions for improving service levels.

If deemed necessary, THE NAINITAL BANK LTD. may initiate an interim review to assess the Agency's performance and obligations. The Bank will conduct quarterly reviews of the services rendered by the Service Provider on mutually agreed schedules, with representatives from both the Bank and the Service Provider in attendance. The SLA may be periodically reviewed (i.e., quarterly) and revised if required.

8.4 Service Level Agreements Matrix Operations Phase

Vendors need to strictly adhere to Service Level Agreements (SLA) computed on parameters as per industry best practice. Services delivered by vendor should comply with the SLA mentioned in the table below. SLA will be calculated monthly. SLA violation will attract penalties:

8.4.1 Uptime of the solution

For purpose of calculating penalty, uptime is calculated as under:

$$\text{Uptime (\%)} = \frac{\text{Sum of total hours during Month - Sum of downtime hours during Month} * 100}{\text{Sum of total hours during the Month}}$$

Total hours during the Month = No. of working days i.e. 30 * 24 hours = 720 hours

$$\text{Uptime (\%)} = \frac{720 - \text{Sum of downtime hours during the Month} * 100}{720}$$

#	Service Area- Availability of solution	Acceptable Service Level	Penalty
1	SIEM Solution Uptime % calculated on monthly basis for SIEM. In case of any hardware problems, the Bidder should ensure that replacement devices are made available to meet the SLAs.	System Availability 99.9 % and above	NA
		98% to 99.9	2 % of monthly payment
		95% to 97.99%	10 % of monthly payment
		90% to 94.99%	20 % of monthly payment
		Below 90%	50 % of monthly payment

8.4.2 Security Incident Alerting & Reporting

#	SLA Metric	Description	Critical	High Priority	Med Priority	Low Priority
1	TTN	Time to Notify This is the acceptable time a System/analyst shall take to send out an Incident notification to the customer.	Notify events within 15 minutes of the event identification	Notify High priority events within 30 minutes of the event identification.	Notify medium priority events within 45 minutes of the event identification	Low: Update should be provided at the minimum of once in every 8 hours along with action plan/ mitigation steps till the closure of the incident.
2	TTR	Time to Triage This is the acceptable time an SOC Analyst will take to perform and conduct first responder processes as documented (run - books)	1 hours	4 hours	6 hours	12 hours
3	TTD	Time to Diagnose This is the acceptable time an SOC Analyst will take to perform a detailed analysis of the Incident, and update the customer with recommendation and response steps	Critical incidents should be closed within 4 hours	High Priority incident should be closed within 12 hours	Median Priority incident should be closed within 24 hours	Low priority incident should be closed with 84 hours
4	Penalty	Delay in attending as per defined SLA of Bank will attract penalty. Penalty for missing critical incident escalation will be as follows:				

#	Event	SLA (of Monthly Billing)	High Priority	Med Priority
1	Incident Monitoring And Response till Resolution	1-2 events: 2% 3-4 events: 5% 5-6 events: 7% 7 and above events:10%	1-3 events: 2% 4-6 events: 5% 7 & Above events: 7%	1-3 events : 1% 4-6 events : 2% 7-10 events : 3% 11 and above events: 5%
2	Escalation of Incidents	1-2 events: 2% 3-4 events: 5% 5-6 events: 7% 7 and above events:10%	1-3 events: 2% 4-6 events: 5% 7 & Above events: 7%	1-3 events : 1% 4-6 events : 2% 7-10 events : 3% 11 and above events: 5%
3	Closure of Incidents	1-2 events: 2% 3-4 events: 5% 5-6 events: 7% 7 and above events:10%	1-3 events: 2% 4-6 events: 5% 7 & Above events: 7%	1-3 events : 1% 4-6 events : 2% 7-10 events : 3% 11 and above events: 5%

Reporting and Dashboard			
1	Reporting and Dashboard compliance. Periodic reports to be provided as per requirements in SoC Deliverables.	Daily Reports: By 12:00 PM Weekly Reports: By 10:00 AM : Monday	Delay in reporting for daily report for more than 1 day shall incur a Penalty of 1% of quarterly SOC Management charges

<table>
<tr><td>2</td><td>Daily Reports: Next Working Day by 12 PM
Weekly Reports: Monday 12 PM
Monthly Reports: By 5th day of every month (n) for 1st day of (n-1) month to last day of (n-1) month
Quarterly reports by 5th day of every quarter end
Ad hoc reports : Detailed RCAs for security incidents</td><td>Monthly Reports:
By 5th of each month</td><td>Delay in reporting by more than 3 days for both weekly and monthly reports shall incur a penalty of 1% of quarterly SOC Management charges</td></tr>
<tr><td>3</td><td>Security Intelligence Advisories within 24 hours of vulnerability disclosure/global threat detection for each security device/solution</td><td>Advisories within 12 hours of new global threats & vulnerabilities disclosures.</td><td>A delay of more than Five days will incur a penalty of 1% of monthly SOC

Management charges for that month</td></tr>
<tr><td>4</td><td>Periodic Reviews</td><td>The vendor is expected to improve the operations on an on-going basis.
The vendor is expected to provide a quarterly report of the new improvements suggested, action plans, and the status of these improvements to the bank The SOC project sponsor or location delegate from the vendor is expected to conduct a quarterly review meeting with participating bank officials resulting in a report covering details about current SOC SLAs, status of operations, key threats and new threats identified, issues and challenges etc.</td><td>The quarterly meeting for next years to be conducted on the 25th (Tentatively) of each month during the operations phase.

A delay of more than One week will incur a penalty of 1% of monthly SOC Management charges for that month</td></tr>
<tr><td>5</td><td>Availability of minimum manpower as per this RFP and add changes agreed from time to time.</td><td></td><td></td></tr>
<tr><td>6</td><td>Brand Image protection

Dark Web monitoring should be available on 24x7 basis.

Anti-Malware service should scan Bank’s websites minimum once in a day and report the findings.</td><td>SLA metric is as given below:
<table><tr><th>SLA Type</th><th>Incident Nature</th><th>SLA Metric</th></tr><tr><td rowspan="6">Detection Incident Portal</td><td>Malware</td><td>>50%</td></tr><tr><td>Social Media</td><td>>80%</td></tr><tr><td>Mobile Apps</td><td>>80%</td></tr><tr><td>Detection Time to Incident creation</td><td><10 minutes</td></tr><tr><td>Incident creation to notify</td><td><5 Minutes</td></tr><tr><td>Portal Availability</td><td>100% uptime</td></tr></table></td><td>The maximum aggregate cap on account of penalty will be limited to the 10% of the contract amount.</td></tr>
</table>

Severity Categorization

Critical and High Severity: Such incidents will usually have a Critical and major effect on system operation and significant business impact requiring high level intervention or crisis management. Time sensitive issues requiring an immediate response from one or more parties to mitigate or remediate the risk or impact of a particular incident. Capable of causing significant financial impact or reputation loss of value to the company or shareholders. Other possible issues are legal or compliance impact for failure to comply or report.

Medium Severity: Includes any successful attempts to actively breach an information system security policy on one or more systems, and may result in a minor or moderate effect on system operations and/or business impact. These issues are more likely to be contained within CUSTOMER and/or have a manageable level of impact.

Low Severity: Events that produce no effect on system operations or result in significant business impact, and is comprised of identified, but Unsuccessful, attempts to actively breach an information system security policy. Non-time sensitive issues where any change made would not create an impact or increase the risk to the infrastructure or data. Capable of causing low financial impact or reputation loss of value to the company or the shareholders.

Incidents will be categorized as Critical, High, or medium priority in consultation with the selected bidder throughout the contract period.

- Response Time: This refers to the duration taken to log an incident from the moment a security breach, cyberattack, or security incident is reported.
- Resolution Time: This is the time taken to troubleshoot and resolve the problem, measured from when the incident is reported or logged in the helpdesk/ticketing tool (whichever occurs first) until the problem is fully resolved.
- Go-Live of SOC: This signifies the date when the proposed solution is fully deployed in compliance with RFP requirements, including the integration of all devices, configuration of use cases, and generation of alerts from the solution.

Parameter	Penalty Deduction
Unavailability of Facility Management Resource	• Deduction equivalent to the cost of the resource per day of absence will be levied. • Penalty of additional Rs.10,000 (Rupees Ten Thousand only) per resource (L1/L2) per day, as applicable, will be levied for each resource unavailable [if appropriate replacement of the unavailable resource is not provided].

1. All the above penalties are independent of each and are applicable separately and concurrently. The total penalty will be an aggregation of the penalties of each of the slabs of the SLA mentioned in the above table. LD is not applicable for the reasons attributable to the Bank and Force Majeure.
2. New patches are applied on a regular basis as and when available become generally available to all related technologies supplied by the vendor.
3. Security Device Management and Administration Vendor is expected to provide this service 24/7 . Management and administration of all security devices / solutions supplied under SOC.
4. Integration of security devices with AAA systems like, TACACS/ Secure ID/ PIM/ DAM / CLMS/ IRM etc. for the Administrative access framework & audit trails will be done in 2 weeks from date of implementation
5. 24 x 7 L1 Support over Email and Ticket.

Note: These SLA parameters are for indicative purposes only, further SLA Agreement will be reviewed and finalized with the selected bidder after discussion.

8.5 Deployment Models & Service Delivery Methodology

The Bank envisions a model that combines onsite and remote services provided by the Bidder. Remote services will be offered from the Bidder's own Security Operations Centre (SOC), while onsite services will include the deployment of one (1) Level 2 resource to coordinate incident management at the Bank's preferred location in the Haldwani, Nainital/ Noida during business hours (10 AM to 6 PM, Monday to Saturday) at implementation stage.

The Bidder should note that the Bank currently hosts its Data Centre in Noida and its Disaster Recovery (DR) Centre in Mumbai. However, these locations may change in the future, subject to **RFP # (NTBL/ISC/SOC/2024/11/22**) issued for the selection of a vendor for Data Centre and DR Services. Consequently, the deployment of SOC services will be structured as follows:

The vendor will deliver Security Monitoring Services through a model where a log collector is deployed at the Bank's premises. Other components, such as log storage, correlation, and monitoring, will take place at Bidder's SOC. Log storage will occur at the Bidder's SOC, alongside other components like the SIEM, rules and correlation engine, advanced detection systems, and response platforms. The Bidder must provide a declaration that the Bank's log data will be stored within Indian boundaries and will not leave the country's jurisdiction under any circumstances.

The SOC service pricing, including one-time charges, must be clearly specified in the commercial section. Management of platforms (including the other services required by the Bank), 24x7 monitoring, and incident analysis will be performed from the vendor's SOC. The Bank will not be responsible for procuring any SIEM licenses required for setup.

The Bidder should consider both near and far DR requirements in the proposed design, as monitoring services are needed for devices installed at the Bank's near and far DR sites. Bidders must clearly specify the types of technologies that will be used to create the SOC setup for the Bank, including SIEM and other related technologies.

Any interfaces or custom connectors required for integration must be developed by the Bidder for the successful implementation of the SOC, at no additional cost to the Bank. The vendor will also provide support to the Bank's team in integrating the in-scope devices and identifying the correct log baselines and configuration changes needed for effective correlation and monitoring.

The overall scope includes ensuring full coverage of 24x7x365 log monitoring for various security solutions, devices, and applications, such as firewalls, network intrusion prevention systems, web application firewalls (WAF), database activity monitoring (DAM), privileged identity management (PIM), data loss prevention (DLP), anti-DDoS, anti-APT, and deception technologies. This encompasses critical network security devices located at the Data Centres, DR sites (both near and far), branches, and other locations identified by Nainital Bank. The scope also involves onboarding these devices to the monitoring platform and transitioning them to new devices, all at no additional cost to the Bank.

Additionally, the development and implementation of processes for managing and operating the SOC will include (but not be limited to) the following:

- Ticketing of the Alerts by the Ticking tool provided by the bidder
- Configuration and Change Management
- Incident Triage and Escalation Management Processes
- Daily Standard Operating Procedures
- Training Procedures and Materials
- Reporting Metrics and Continuous Improvement Procedures
- Data Retention and Disposal Procedures
- Business Continuity Planning (BCP) and Disaster Recovery (DR) Plans and Procedures for the SOC

8.6 Business Continuity

The bidder shall be responsible for defining a Disaster Recovery (DR) and Business Continuity Plan (BCP) for the Security Operations Center (SOC) operations. Additionally, the bidder must ensure that periodic tests are conducted according to the agreed testing calendar or regulatory requirements set by the bank. This is to confirm that all deliverables and Service Level Agreements (SLAs) are met if SOC operations need to be switched to an alternate site (DR-SOC). The proposed DR site must be located within India.

Annexure 2

Technical Specifications: Security Operation Centre (SOC)

Compliance: C – Fully compliant, P – Partially Compliant, N – Not compliant
Category: M – Mandatory, O – Optional

Key Requirements: SOC Implementation (SIEM)

S.No	Specifications	Category	Compliance	Remarks
1	**Security Monitoring Requirements**			
1.1	The Bidder should configure SIEM to monitor security logs to detect malicious or abnormal events and raise the alerts for any suspicious events that may lead to security breach.	M		
1.2	The Bidder should develop, update, and maintain log baselines for all security related platforms at The Nainital bank Limited that are required to be monitored. Bidder should also coordinate with different team to implement and maintain the log baselines on all the Bank's systems.	M		
1.3	The Bidder should configure SIEM to collect logs from most of the standard platforms like Windows, Linux, Firewall, Network and other security devices or solutions, etc. (Integration of logs of all the IT devices (Servers, Network devices etc.) hosted out for The Nainital bank Limited DC/DR/NDR and other places)	M		
1.4	The Vendor should configure SIEM to collect logs from most of the standard network, security devices, Databases, Web servers and cloud services (Aws/Azure), SAAS Solutions, O365, GC Workspace and DLP & DAM solutions etc.	M		
1.5	The Vendor should configure SIEM to monitor, detect and manage incidents for the following minimum set of database security events. This is an indicative list and is not a comprehensive/complete set of events. Vendors should indicate their event list in proposal response. Monitor Access to Sensitive Data (e.g. PII data). Database access includes logins, client IP, server IP and source program information. Track and audit administrative & high-risk commands	M		
1.6	The Vendor should carry out correlations amongst the logs from multiple sources to detect multi-vector attacks.	M		
1.7	The Vendor should have capability to integrate log from nonstandard application and devices and service provider platform should be able to process them for generating alerts and reports. This should be accomplished through standard or custom parsers as applicable.	M		
1.8	SIEM reports in compliance with industry best practices and international standards like ISO 27001, PCI-DSS, SOC1, SOC2 etc.	M		
1.9	The SIEM solution will collect the following items, at a minimum: • Registry access – adds, changes, and deletions • User account changes • administrator equivalent permissions • Permission changes to groups • Login failures and successes	M		

	• System events – success and failure • Application failure, start, or shutdown • Intrusion detection logs • Anti-virus logs • Interfaces for high TCP and UDP traffic • DNS changes • HTTP "404" errors • FTP server access and file transfers • Permission and access changes to files, folders, and objects • Password change attempts – success and failure • All actions by privileged accounts • Object access – success and failure • Process tracking – success • Policy change – success and failure • Account management – success • Directory service access – success and failure			
1.10	The Bidder should define rules on event logs captured from various sources to detect suspicious activities not limited to the following Examples: • Failed login attempts • Successful Login attempts from suspicious locations or unusual systems • Authorization attempts outside of approved list • Vendor logins from unauthorized subnets • Vertical & Horizontal port scans • Traffic from blacklisted IP's • Login attempts at unusual timings	M		
1. 11	The Bidder should provide solutions and should be able to provide charts for the top attacks & attackers, OWASP based threat analysis, Trending threats, attack demographics etc. by utilizing the WAF solution deployed in the Bank.	O		
1.12	The SIEM shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.	M		
1.13	Any failures of the event collection infrastructure must be detected, and operations personnel must be notified.	M		
1.14	The SIEM should be configured to support enrichment of data with contextual information like Geo Data, malicious IPs, Domains, URLs, Threat Intel and custom specified tags and annotations.	O		
1.15	SIEM should detect both internal and external attacks. In addition to security attacks on IT infrastructure, Vendor should configure the SIEM to monitor for security events on critical business applications, databases and identify network behavior, user behavior anomalies, and servers.	M		
1.16	The SIEM should monitor, detect, and manage incidents for the following minimum set of IT infrastructure security events and send alerts. This is an indicative minimum list and is not a comprehensive /complete set of events. • Buffer Overflow attacks • Port and vulnerability Scans • Password cracking	M		

	• Worm/virus outbreak • File access failures • Unauthorized service restarts • Unauthorized service/process creation • Unauthorized changes to firewall rules • Unauthorized access to systems • SQL injection • Cross site scripting All layer 7 web attacks via internet / intranet			
1.17	The SIEM should be configured to monitor, detect and manage incidents for the following minimum set of business application security events and send alerts. This is an indicative list and is not a comprehensive /complete set of events. Attempted segregation of duties violations • Attempted access violations • Critical user additions, deletions • Creation, deletion, and modification of critical application roles/groups • Changes to permissions or authorizations for critical application roles/groups • Changes to account and password policies in the application • Changes to critical application parameters • Changes to audit parameters	M		
1.18	Vendor should configure centralized incident management to prioritize and manage security incidents.	M		
1.19	The solution should enable investigation of triaged alert/custom alerts.	M		
1.20	Solutions should support MITRE attack framework	O		
1.21	The SIEM Solution should have a clear physical or logical separation of the collection module, logging module and co-relation module.	M		
1.22	The proposed product should be able to handle 10,000 Events Per Second (EPS), which should be scalable to 50,000 or Higher	M		
1.23	The solution should be able to conduct agentless collection of logs except for those which cannot publish native audit logs.	M		
1.24	The solution should have connectors to support the listed devices/applications/ new log sources, wherever required the vendor should develop customized connectors at no extra cost.	M		
1.25	The Vendor Should carry out Root Cause Analysis of the security incident/breach reported and submit RCA report/s. Any support required in this regard will be facilitated by Nainital Bank Team.	M		
1.26	The entire solution shall be implemented as per the best practices recommended by the OEM. The Bidder Shall ensure that the proposed solution is upgraded, as and when the OEM releases patches/bug fixes. Preferably at-least once in a quarter.	M		
1.27	The solution must support the auto discovery of assets that are being protected or monitored and make them available in an asset database within the system.	M		

1.28	The solution must support user extended taxonomy of events and fields. The user must be able to add their own unique event names (i.e., the ability to add in new fields that are not part of the vendors out of the box schema such as a field called "SpecialID from my Custom Application").	O		
1.29	The bidder Shall provide demonstration of all the features of the solution (including the use cases configured) deployed as part of acceptance testing.	M		
1.30	The Solution should offer a global threat feed which must allow the analyst to perform search across various parameters like IPv4, IPv6, URL, vulnerability, Applications name, Malware and Spam etc.	M		
1.31	The Solution should allow analysts to perform manual ad-hoc check to determine if it is infected with any Zero-day attack.	O		
1.32	The solution must provide more advanced event drill down when required.	M		
1.33	The solution must provide a real-time streaming view that supports full filtering capabilities	M		
1.34	The solution must provide a mechanism to capture all relevant aspects of a security incident in a single logical view. This view should include relevant events, network activity data, correlated alerts, etc..	M		
1.35	There should be provision available to create complex searches by means of GUI, to support advance investigation on the data available in the platform.	O		
1.36	The platform should Query-less search experience which guides analysts in defining what they want to search for with ability to change condition, operator, time frame, column display, and values	O		
1.37	Service provider to assist the organization to ensure the log retention is as per local regulatory requirement like RBI, CERT and NCIIPC , etc. – 3 Months Online and 2 Years Offline	M		
1.38	Proactive monitoring of www.nainitalbank.co.in for any Cyber-attacks. (Anti-Trojans, and Anti-Rogue Services). However, the Bank reserves the right to add any number of additional URLs registered in its name. Bidder should be able to proactively monitor, detect and handle the following incidents (Trojans/ Brand abuse cases)	M		
1.39	As part of Breach Assessment, bidders shall provide investigation services in case of any compromise/breach due to any attack. The bidder shall perform analysis on the compromised system/s and submit their analysis report. The report should also include the steps that need to be taken proactively to prevent such attack/ compromise/breach in future.	M		
1.40	The vendor should Provide Latest Security threat advisories from threat intel sources including CERTIN, NCIIPC. Threat advisories shall be integrated with the solution. Department will facilitate to get the threat intel feed from CERTIN, NCIIPC. However, it is the responsibility of the bidder to integrate these feeds into the SOC solution.	O		

2	**Log Collection and Management**	**Category**		
2.1	All logs should be Authenticated (time-stamped) encrypted and compressed before transmission.	M		
2.2	The solution should be able to continue to collect log data during database backup, de-fragmentation, and other management scenarios, without any disruption to service.	M		
2.3	The solution should support log collection from all operating systems and their versions including but not limited to Windows, AIX, Unix, Linux, servers, etc.	M		
2.4	In case the connectivity with SIEM management system is lost, the collector should be able to store the data in its own repository. The retention, deletion, synchronization with SIEM database should be automatic but it should be possible to control the same manually.	M		
2.5	The solution shall allow bandwidth management, rate limiting, at the log collector level.	**O**		
2.6	The solution should ensure that the overall load on the network bandwidth at DC/DR/NDR, WAN level is minimal.	M		
2.7	The solution must provide time-based store and forward feature at each log collection point.	M		
2.8	The solution should have the capability to compress the logs for storage optimization.	M		
2.9	Solution must have a log collection and archive architecture that supports both short-term (online) and long-term (offline) event storage	M		
2.10	It should be possible to store the event data in its original format in the central log storage.	M		
2.9	The data archival should be configured to store information in a secure format and should comply with all the relevant regulations.	M		
2.10	The system shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.	M		
2.11	The Proposed Solution Should support the following log collection protocols: Syslog over UDP/TCP, Syslog NG, SDEE, SNMP Version 2 & 3, ODBC, FTP, Windows Event Logging Protocol, NetFlow at a minimum.	M		
2.12	Log collection software should support protocols like syslog, JDBC, API, WMI, SFTP, FTP, SCP, SNMP, MQ etc. on single software/hardware appliance.	O		
2.13	The solution must support industry log collection methods (syslog, WMI, JDBC, SNMP, Opsec etc.). Solution can read and interpret events from more than 300 log sources.	O		
2.14	The system should be able analyze logs with different event formats e.g. well-structured logs, natural language logs, multi-line logs etc.	M		
2.15	The solution must provide a common taxonomy of events.	O		
2.16	The solution must provide the ability to normalize and aggregate event fields that are not represented by the out-of-the-box normalized fields	O		
2.17	The SIEM must provide searching & data/log management, including free form search.	M		

2.18	The vendor to ensure logs are transmitted using strong encryption & no PII data is moved out of Bank's Environment.	M		
3	**Correlation & Alerting**	**Category**		
3.1	The SIEM must allow the creation of an unlimited number of new correlation Rules.	M		
3.2	The 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.	O		
3.3	The system/solution should have the ability to correlate all the fields in a Log.	M		
3.4	The Solution must be able to store logs in a separate system which would not be required to perform any real time correlation thereby minimizing the load on the Real time analysis.	O		
3.5	The solution should be able to parse and correlate multi line logs.	M		
3.6	They should have the ability to gather information on real time threats and zero-day attacks issued by antivirus or IDS/ IPS vendors or audit logs and add this information as intelligence feed into the SIEM solution via patches or live feeds.	M		
3.7	The solution should allow a wizard-based interface for rule creation. The solution should support logical operations and nested rules for creation of complex rules. For e.g. the output of one correlation rule should be used as an input to the other correlation rule.	O		
3.8	The central correlation engine database should be updated with real-time security intelligence updates from OEM.	M		
3.9	The correlation engine should support identification of "low and slow" attacks by providing capabilities of data mining historical incidents and generating on screen patterns which can then be translated into correlation rules for future detection and analysis	M		
3.10	The solution must provide alerting based on observed security threats from monitored devices and network activity	M		
3.11	The solution must support a distributed model for correlation such that counters, sequences, identity lookups, etc. are shared across all collectors. (i.e., 'X' login failures from the same username followed by a single successful login for that same username, where events seen by a single collector do not exceed the threshold of 'X', but across multiple collectors would exceed the threshold) (X would be fixed by the bank.).	M		
3.12	Proposed solution should provide capability to add the following systems for effective incident detection and correlation post completion of the SIEM deployment. 1. Flow based threat Detection 2. User Behavior analysis 3. Threat Intelligence	M		
3.13	The solution must chain alerts into one single incident record, so when different rules are triggered and these activities are related to one single offense, then these triggers will generate only one incident record to avoid overloading the security operation team.	M		

3.14	The solution must provide alerting based upon established policy. (e.g., IM traffic is not allowed.)	M		
3.15	The solution must be able to detect when strange users access a specific host, learn what users connect with specific assets such as a point-of-sale terminal and then alert when new users login.	M		
3.16	The solution must generate and be alert when a new service appears on the network or when new assets appear where they shouldn't or are not planned.	M		
3.17	The system must manage user activity by host overtime even when usernames don't present in the immediate event data.	M		
3.18	The solution must provide the ability to transmit alerts using multiple protocols and mechanisms to other management solutions	M		
3.19	The solution must provide UI based wizards and capabilities to minimize false positives and deliver accurate results.	M		
3.20	The solution must limit the presentation of multiple similar alerts. Describe the solutions ability to minimize duplicate alarms.	M		
3.21	The solution must monitor and alert when there is a disruption in log collection from a device. In other words, if logs are not seen from a server in X minutes, then generate an alert.	M		
3.22	The solution must provide an out-of-the-box mechanism to discover and classify assets by system type (i.e. mail servers vs. database servers) to minimize false positives associated with poor asset classification.	M		
3.23	The solution must support correlation for a missing sequence. Example service stopped not followed by the service restarting within 10 minutes.	M		
3.24	The solution must support correlation for additive values over time. For example, alert when any SRC IP sends more than threshold data to a single port on a single DST IP in a one-hour period.	M		
3.25	The solution must provide a mechanism to optimize rule tuning, which allows for the grouping of similar input values of a correlation rule that can be used by multiple rules. This grouping mechanism should allow for both static groups and groups that are dynamically created by other correlation rules. For example, the user of the system can define a group of banned ports/protocols that should be used across multiple correlation rules that monitor for inappropriate network activity.	M		
3.26	The solution must support historical correlation so users can re-run past events and flows on historical data, so new rules can be tested more precisely.	M		
3.27	The solution must be able to be updated regularly, to stay aware of the latest threat information and research available.	M		
3.28	The solution must be able to analyze user activity to detect malicious insiders and determine if a user's credentials have been compromised.	M		
3.29	The Platform Shall create a baseline model that contains information about the flows and flow attributes that currently exist on the system.	M		

3.30	The platform should analyze the flow records to determine normal traffic patterns, while comparing all incoming flows to the baseline models. Flow should be assigned an outlier score based on the flow attribute values and frequency of communication is observed on the network.	M		
3.31	the platform should Visualize offenses, network data, threats, malicious user behavior, and cloud environments from around the world in geographical maps, and auto updating charts.	M		
3.32	The platform should allow to Import and export dashboards or share dashboard links with colleagues.	M		
3.33	The platform should allow users to create dashboard items that use the full power of native language, dynamic search, offense and the generic APIs.	M		
3.34	The platform should allow users to fine-tune there with complete flexibility in dashboard layout and dashboard item refresh rates	M		
3.35	The platform should allow users to Assign thresholds to Big Number, Time Series, Tabular, and Geographical charts.	M		
3.36	The platform should offer an interface to help user in browsing the existing rule mapping across MITRE Framework & enabling them to map their custom rules to MITRE ATT&CK tactics and techniques.	M		
3.37	The platform should offer users to tune their environment with the help of built-in analysis capability.	M		
3.38	The Platform should allow user to Use new insights to prioritize the rollout of new use cases and apps to effectively strengthen your security posture.	M		
4	**Dashboard and Reporting**	**Category**		
4.1	The dashboard 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.	M		
4.2	Events should be presented in a manner that is independent of device specific syntax and easy to understand for all users.	O		
4.3	The dashboard should show the status of all the tools deployed as part of the SOC, including availability, bandwidth consumed, system resources consumed (including database usage).	M		
4.4	It should be possible to categorize events while archiving, for example, events for network devices, antivirus, servers etc.	M		
4.5	Any failures of the event collection infrastructure must be detected, and operations personnel must be notified as per SLA. The device Health monitoring must include the ability to validate that original event sources are still sending events.	**M**		
4.6	The solution should generate the following reports (but not restricted to): User activity reports, Configuration change reports, Incident tracking report, Attack source reports etc. In addition, the solution should have a reporting writing tool for development of any ad-hoc reports.	M		
4.7	The Dashboard design for the solution should be editable on an ad hoc basis as per the individual user's need.	O		

4.8	The system should display all real time events. The solution should have drill down functionality to view individual events from the dashboard.	M		
4.9	The solution should allow for qualification of security events and incidents for reporting purposes. The solution should be able to generate periodic reports (weekly, monthly basis) for such qualified security events/incident.	M		
4.10	The platform shall support provision for dashboard specific to a single offense, which can offer various widgets, provision for sharing notes, representation of data in a graphical manner over a certain period and various rules triggered, rules model responsible in triggering of the offense.	M		
4.11	The solution should not limit the number of non-critical events that need to be collected for compliance reasons and doesn't require correlation till the maximum capacity of hardware/storage.	M		
4.12	The solution should not require additional license to deploy additional nodes for collection & processing & HA license for these nodes	M		
4.13	For storage calculation, the bidder should consider 700 bytes as the average raw payload size of the logs.	O		
5	**Other Technical Specifications SIEM**	**Category**		
5.1	Solutions should be proposed in high availability in both DC and DR	M		
5.2	SIEM shall support Connector Development tool/SDK /API availability for developing collection mechanism for home-grown or any other unsupported devices/applications. The respective tool should be provided.	M		
5.3	Communication is encrypted within SIEM components. With external components it purely depends on compatibility.	M		
5.4	The solution must integrate with 3rd party directory systems as an authentication method. Solution should be integrated with LDAP or Active Directory solution for access provisioning to the SIEM system.	M		
5.5	The proposed solution should be horizontally scalable to support increase in EPS and should have global correlation capability on raw or metadata/normalized events (i.e. correlation of events if processed on multiple hardware/appliances)	M		
5.6	SIEM solution should support High Availability across all components within the system e.g. log collection, log correlation, management console etc.	M		
5.7	The solution must support high availability requirements in an embedded fashion at all layers including collection, normalization, correlation and management and without the need for additional 3rd party software.	M		
5.8	High Availability should use cluster set-up so that data can be shared between the nodes.	M		
5.9	SIEM solution should support Disaster Recovery	M		
5.10	The solution must support a web-based GUI for management, analysis and reporting. There should be no plug-ins, Java, Flash, or thick-client requirements for operating the solution.	M		

5.11	The solution must support the one "master console" approach in case of having multiple SIEM instances.	M		
5.12	The solution should be able to define purging and retention rules for log storage.	M		
5.13	The solution must provide an open API mechanism	M		

Bank may add SOAR capabilities in near future basis requirement with the shortlisted vendor

S.No	Technical Specifications - User Behavior Analytics (UBA)	Category	Compliance	Remarks
A	**User Behavior Analytics (UBA)**			
1	UBA shall be an inbuilt capability of offered SIEM solution. UBA should be part of the SIEM solution & SI should not require any additional/ Third party component to complete the UBA solution.	M		
2	UBA UI/panel should be integrated in SIEM dashboard. Thus, which will help in monitor desired elements of users' behaviors, risks and trends from a single screen	M		
3	The solution should provide UBA dashboard based on various UBA models' outcome. • UBA Dashboard should highlight risky users based on objective scoring of users based on composite risk score comprising all behavior anomalies of the user • Organization should be able to define risk thresholds based on their risk appetite	M		
4	Detect malicious/illegal activities performed by users	M		
5	Solution to have capabilities to collect user data from a variety of sources like Directory Services, IAM, VPN, Proxy, O365, etc	M		
6	Service providers should submit a monthly threat hunting based on the threat hunting performed on the logs generated.	O		
7	Access high-value assets such as User starts accessing and downloading high-value assets with increased frequency.	O		
8	Usage changes over time such as User activity deviates from normal over a short period of time or a gradual change over an extended period of time.	O		
9	Assessing frequency of assets such as User's volume of activity suddenly spikes or access to number of assets increases rapidly.	O		
10	Usage deviates from peer group such as User pattern of activity starts deviating from the peer group	O		
11	Change in account privileges such as User attempts to change privileges on existing accounts or open new accounts on other systems.	O		
12	Application misuse by sequence of actions: User performs a sequence of actions which no other user is performing.	O		
13	Sensitive data leakage such as User manipulates http request / response parameter to download sensitive data.	O		
14	Application misuse by malware or bots such as A bot or malware attacks an application or access sensitive data.	O		
15	Dynamic adjustment of risk scores such as Dynamically adjusting the risk score of rules when triggered against user or users.	O		
16	UBA should activate a rule for a set of users until a specified condition or specified time window.	O		
17	Solution should leverage Machine learning to perform analytics to gain additional insight into user behavior with predictive modelling.	O		

18	UBA should perform the above-mentioned scenarios as well.	O		
19	UBA ML model (User Behavior Analytics (UBA) app with Machine Learning) must cover Individual user models (by numbers or observed): Like Access Activity, user's general activity by time, Authentication Activity, data that is downloaded or uploaded by user, Lateral Movement, process usage etc. Peer Group Analysis: like Activity distribution, defined peer group, learned peer group etc. Custom Models: like Application Events, Source IP, Destination Port, Office File Access, AWS Access, Process, Website, Risky IP	O		
20	ML Based UBA Use cases must include 1. Access activity 2. Aggregated activity 3. Authentication activity 4. Data uploaded to remote networks 5. Data downloaded 6. DML events 7. DDL events 8. Large HTTP transfers 9. Outbound transfer attempts 10. Risk posture 11. Suspicious activity 12. Successful access and authentication activity 13. Activity distribution 14. Defined peer group 15. Learned peer group 16. Lateral Movement: Internal Destination Port Activity 17. Lateral Movement: Network Zone Access 18. Lateral Movement: Internal Asset Usage 19. Process Usage	O		
21	Use Case for UBA: 1. Accounting more high value assets than normal 2. More data being transferred than a normal to and from servers and / or external location 3. Privileged account accessing high-value servers from a new location for the first time 4. Account used for the first time in a long time 5. Rare privilege escalation 6. Accounts being used from peculiar locations 7. User involved in previously malicious or threatening behavior User an outlier within their peer group.	O		
22	Exfiltration: 1. Data Exfiltration by Print 2. Data Exfiltration by Removable Media 3. Data Loss Possible 4. Initial Access Followed by Suspicious Activity 5. Large Outbound Transfer by High-Risk User Multiple Blocked File Transfers Followed by a File Transfer	O		
23	Browsing behavior: 1. Browsed Entertainment Website 2. Browsed to Gambling Website 3. Browsed to Information Technology Website 8. Browsed to Mixed Content/Potentially Adult Website	O		
24	Network Traffic and Attacks	O		

	1. D/DoS Attack Detected 2. Honey token Activity 6. Capture, Monitoring and Analysis Program Usage			
25	DNS Analysis 1. Potential Access to Blacklist Domain 2. Potential Access to DGA Domain 3. Potential Access to Squatting Domain 4. Potential Access to Tunneling Domain	O		
26	Geography Based 1. Anomalous Account Created from New Location 2. User Access from Multiple Locations 3. User Geography Change 3. User Geography, Access from Unusual Locations	O		

S.No	Specifications	Category	Compliance	Remarks
B.	**MDR –Managed Detection and Response Services**			
	Technical Specifications -MDR			
1	The Endpoint Security Solution setup must have the capability to manage 2500 endpoints at Central Console, which may be implemented in a phased manner.	M		
2	The proposed solution should support either SaaS based platform or on-premises deployment.	M		
3	If the proposed solution is cloud based, it must be deployed in Indian Data Centre and data should not move out of India.	M		
4	In the case of on-prim solution bidder will provide requisites hosting hardware & all necessary software within the quoted price**.**	O		
5	The solution must be capable of managing minimum 1500 endpoints to start with and must be scalable to manage up to 10 thousand End Points. The bidder must ensure that hardware/software required at the central console can scale to additional endpoints onboard at any time.	M		
6	Solutions features must be fully compatible over IPv4/IPv6 network such as hardware, software, and application software etc.	M		
7	The solution should have management infrastructure, operational monitoring, upgrades, reporting, notifications & 24x7 support.	M		
	Management Console			
8	The solution should provide a unified web-based console for all functionalities and should allow administrators to access the management interface to any authorized user, without installing additional software.	M		
9	The solution should support multi-site configuration and multiple tenants within the same organization.	M		
10	The solution should provide the flexibility to have individual rules/policies for every group. The solution should also support policy inheritance from Account to Site to Group with the ability to break inheritance if required.	M		
11	The proposed solution must have the option to create role-based access/ view(s) of the management console.	M		
12	The solution should provide API with access to all management capabilities and access to data. API should be well documented and available without any additional cost and application and hardware. The solution should have the ability	M		

	to quickly run APIs on the console data set without any limitations.			
13	The solution must provide multi-factor authentication and single sign on solutions for the management console and sensitive functions such as remote shell.	M		
14	The solution must provide non-repudiable Centralized auditing and logging of activity through the management console. Management activity must be logged and audited with the ability to send logs to an external source without restrictions.	M		
	Endpoint Agent Capabilities			
15	Endpoint Agent must provide Endpoint Protection (EPP) and Endpoint Detection & Response (EDR) capabilities available in a single agent without requiring multiple software packages to be installed. Besides this all the other security features of the solution, i.e. Host Firewall, threat intel, Device Control, real-time analysis & threat hunting must be available via a single agent.	M		
16	Endpoint Agent must provide strong anti-tamper capabilities, to ensure that an end user cannot remove, disable or modify the product in any way.	M		
17	Endpoint Agent must support ability to on-demand scans (from console and/or endpoint) to look for malware or ensure a threat has been remediated.	M		
18	The proposed solution must have the capability to schedule agent upgrades from the management console.	M		
19	Endpoint Agent must have ability to temporarily disable agent via the management console for temporary troubleshooting or testing.	M		
20	License should not restrict features of the solution, in case of license count exceeding in emergent/unintended circumstances.	M		
21	The solution should have a feature of automatically decommissioning old agents if they haven't communicated to the management server for a configurable period. As and when connection to the system is established the agent must be auto populated in the console.	M		
22	Endpoint Agent must be lightweight with minimal system resource utilization for standard system usage (<3% CPU, <350 MB of memory).	M		
22	Agent must support remote uninstallation from the management console.	M		
23	Agent must support display of customized alert messages on managed endpoints.	M		
24	Deployed agents must be able to communicate with the central management server via a web proxy.	M		
	Operating System Support			
26	The solution must support all versions of Windows Operating Systems starting from windows 7 SP1 for endpoints and Windows server 2008 onwards servers.	M		
27	Solution should support all the latest virtual environments.	M		
28	Agent supports all MAC OSs starting from macOS Mojave (10.14).	M		
29	Solution should support all the latest Linux environments Amazon, CentOS (6.4+ and above), Debian (8 and above), Fedora, Oracle, Red Hat Enterprise Linux (6.4 - 6.10 and	M		

	above),SUSE Linux Enterprise Server(12.X and above) Ubuntu (18.04, 16.04, 14.04 and above with LTS)			
30	The solution must support all windows OS for a minimum period of 12 months after the OS version is end of sale/life. Similarly, Solution must support all MAC OS for a minimum period of 36 months after the OS version is end of sale/life.	M		
31	The solution should support all the new OS Updates/Versions within 60 days of release.	M		
32	The solution must support Windows agent run in kernel space to ensure highest level of anti-tamper.	M		
33	Mac agent should support Kextless architectures.	O		
37	Linux agent must run solely in user space to avoid kernel panics and tainted kernels that invalidate support.	M		
	Threat Prevention			
34	The proposed solution should provide context-aware endpoint investigation and response (EDR), recording and detailed reporting of system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack. The solution must have features for Custom detection, intelligence, and controls.	M		
35	EDR Solution must provide prevention across all major Operating Systems – Windows, MacOS and Linux.	M		
36	EDR Solution must have the capability to protect the system against known and unknown malwares.	M		
37	EDR solution should ensure that files are checked for any infection on write and execute operations.	M		
38	The solution should be effective against sophisticated attacks by analyzing Behaviors on an endpoint.	M		
39	The solution should have a mechanism to protect the endpoint against malware, even when the system is not connected to the network. The agent needs to be fully autonomous meaning it does not need have any dependency on Management Server or Cloud or any resources external from the Agent to detect and respond appropriately to sophisticated threats (Zero Day, File-less, Ram-based, Zero Day exploits, Ransomware, Miners, Lateral movement, APT) in real time as the threats are detected.	M		
40	EDR solution should leverage Artificial Intelligence or Machine Learning to analyze files pre-execution as well as analyze behaviors while a file is running.	M		
41	The solution should have the capability to detect dormant threats as well.	M		
42	The EDR solution should support equivalent protection capabilities across Windows, Mac, Linux, and Kubernetes.	M		
43	The solution should protect endpoints from malicious documents and scripts.	M		
44	The solution should monitor and protect the system from lateral movements & insider threats.	M		
45	The EDR solution should monitor and protect from exploits and file-less attacks.	M		
46	The EDR solution should identify and block potentially unwanted programs on MAC based systems.	M		
47	The solution should provide flexibility to safely download malicious or convicted file from the management console.	M		

48	Threat alerts should be correlated together automatically across enterprise if related to the same attack.	M		
	Response & Remediation Capabilities			
49	The proposed solution shall allow ingestion of IOCs (Indicators of compromise) like domains, file-hashes and shall also allow blocking of the files/file-hashes/domains/URLs identified by the IOCs.	M		
50	The proposed solution should perform multi-level search across endpoints using rich-search criteria And User-defined criteria like Username, File - Name, File - Hash (SHA1 and SHA2) IP address, Hostname, Registry Key, Registry Value Name & Registry Value Data	M		
51	The proposed solution should be able to create multi-stage detailed kill-chain for performing the root cause analysis of an incident. Kill chain also provide reputation of the files from the global threat intelligence as well	M		
52	The proposed solution is to provide the advance response capabilities as mentioned below 1. Kill process 2. Isolate device 3. Block process	M		
53	The solution should support a fully remote shell for all OS (Mac, Windows, Linux) and not limit or restrict set of commands.	M		
54	The solution should track all remote shell commands and logged during a remote shell session.	M		
55	Solution should alert both suspicious and malicious threat behavior.	M		
56	Solution should have ability to kill and quarantine an offending process.	M		
57	Solution should be able to un-quarantine a file from the management interface or API.	M		
58	The solution should have the ability to remediate all operating system changes and perform corrective action. Tools should also be able to undo any system level changes related to the attack (Registry edits, configuration changes etc.)	M		
59	Solution should have options to reverse destructive data events including but not limited to ransomware. The tool should also recover files that were deleted or encrypted as part of an attack and restore files to their pre-attack state.	M		
60	The solution should provide the option to network quarantine a device and provide flexibility to configure the select allow list during quarantine	M		
61	Threat response capabilities offered by the solution should be automated.	M		
62	The solution should provide a mechanism to take remedial actions on multiple systems at once.	M		
63	Solutions should have options to add notes or set the status of an issue or event (i.e. resolved, in progress, unresolved).	M		
	Policy & Installation			
64	Tool should provide Ability to support policy inheritance across an account, site or group of devices.	M		
65	Tool should have the option to provide dynamic policy assignment based on device attributes	M		
66	Devices should be installed and placed directly into a specific device group at the time of installation.	M		

67	The policy context should provide the option to turn ON or OFF unique engines or by Type of engine (Pre-Execution and Run-Time Engines).	M		
68	The product should have a predefined list of known or recommended exclusions.	M		
69	Should the Tool provide the option for the administrators to make policy exclusions of the console at multiple levels? (Account, Site, Group).	M		
70	Provide option for exclusions be deployed in a highly granular way to make the smallest exception possible while still supporting interoperability.	M		
71	Provide an option for Administrators to configure exclusions to independently suppress alerts related to file-based machine learning and/or behavioral engines	M		
72	Exclusions to be configured by the administrator to handle interoperability issues down to specific paths or single executables by reducing monitoring of parent processes and/or parent processes and all their spawned child processes	M		
73	Exclusions should be configurable by the administrator to handle performance issues down to specific paths or single executables by disabling monitoring of parent processes and/or parent processes and all their spawned child processes.	M		
74	Tools to provide options for exclusions are made by administrators of the console for the following parameters. (Hash, Path, Certificate or Signer ID, File Type)	M		
	Device Control and Application Visibility			
75	Tool to have the capability to control external USB media and fine tune Block policy to allow only 'Read only' access to the USB media including mobile.	M		
76	Tools should have the capability to control external Bluetooth devices including mobile	M		
77	The proposed solution should have granular device control capability which can be applied to a Class, Serial Number Product ID, or Type of Device.	M		
78	Device control capabilities should be available on Mac and Windows.	M		
79	The proposed solution must provide a software/application inventory for the environment and identify unpatched 3rd party software apps that may have vulnerabilities.	M		
80	The proposed solution should report all known vulnerabilities in programs installed on an endpoint, along with export option.	M		
	Host Based Firewall Control			
81	The solution should provide Firewall Control for Windows, MAC & Linux. It must not be limited to Windows only. The firewall control policy should provide context unique to each group of Endpoints. Firewall and should support FQDN's, IP, CIDR, Range.	M		
82	The proposed solution should have Firewall rules be built to apply to a specific group of devices (leveraging tagging or policy groups)	M		
83	Firewall rules should be location aware to apply different policies when on or off network	M		
	Device & Network Discovery			
84	Solution must have capability to implement policies for rogue devices to reduce the potential attack surface and Actions	M		

	could include isolate (prevent communication from rogue devices) or installing an agent.			
85	The proposed solution must have the capability to manage the Live global asset inventory, Advanced ML device fingerprinting with flexible active + passive scanning and isolating suspicious and malicious devices.	M		
87	The solution should automatically discover IoT devices in a network without the need to deploy sensors, sniffers, or other hardware.	M		
88	The solution should provide flexibility to ensure discovery is only occurring on desired networks	M		
89	The solution should have the ability to actively scan for and fingerprint unmanaged and IoT devices. The solution should provide the means to search for devices based on device class (Video, Mobile, Printer, Infrastructure, Server, Workstation, IP-Phone, Storage, Virtual Machine)	M		
	Integrations			
90	The solution must have capability to Integrate with Active Directory.	M		
91	The solution should have native integrations with SIEM solutions such as Splunk & Qradar etc.	M		
92	The product should stream EDR data in real-time to own internal data lake.	M		
93	EDR solution should natively send event logs via Syslog. The solution must support the following syslog formats: CEF, CEF2, RFC-5424, STIX and IOC. It should support sbid X.509 certificates for syslog transport encryption and authentication.	M		
94	The solution must have the capability to API integration	M		
	Dashboards & Reporting			
95	The proposed solution must identify rogue devices discovery capability to reduce the potential attack surface, with Network exclusion capability	M		
96	The proposed solution has the option to export data into 3rd party reporting tools.	M		
97	The proposed solution must have inbuilt and customizable dashboards and reporting capability per Site /Group and user.	M		
98	The Solution should have the capability to report all known vulnerabilities in programs installed at an endpoint, along with export option.	M		

Compliance Capability: C – Fully Capable P – Partially Capable N – Not Capable
Category: M – Mandatory, O - Optional

S. No.	**Technical Specifications - Incident Response**	**Category**	**Compliance Capability**	**Remarks**
C.	**Incident Response**			
1	The breach investigation services shall be On-Demand basis.	M		
2	Bidder will provide Man Day Rate for Breach Investigation Services and quote for 30 Days.	M		
3	The Nainital Bank Limited may suspect/face a security attack/System Compromise/data breach in its network/ Infrastructure and may require expert assistance to rapidly detect, triage, investigate, and minimize the impact of attacks.	M		

4	The Nainital Bank Limited shall specifically intimate the vendor in such cases and the vendor shall depute an expert team within 24 hours to contain and resolve the incident and help Nainital Bank in restarting normal operations.	M		
5	The support team will also give a post incident report to The Nainital Bank Limited for future guidance in similar circumstances.	M		
6	The expert team shall focus on: • Finding the hack quickly and preventing further damage • Itemizing security issues Nainital Bank needs to resolve (and how to resolve them) • Reducing the window of vulnerability • Helping preempt damage to Nainital Bank brand • Helping Nainital Bank recover rapidly from cyber attacks • Documenting the process and preserving the evidence to allow sharing for legal/regulatory requirements	M		
7	The scope of breach investigation services shall include: • Determining the scope of the breach • Performing incident forensics to determine the type of infection and its extent • Containing the breach and elimination of source of breach • Determining the root cause of the breach - what happened, how it happened and why System recovery • Providing evidence to help in legal requirements • Suggesting actions and measures to prevent recurrence • Finding if any more threats are remaining which needs to be plugged • Incident Reporting and providing a detailed post incident report documenting the attack anatomy, timelines, vulnerabilities, impact, scope, and recommendations	M		
8	The incident forensics under the breach investigation services shall include: • Forensic analysis of computers, mobile devices, and other IT systems/devices. • Forensic analysis of memory and hard drives • Analysis of network traffic and operating system • Malware analysis—static and dynamic analysis • All the above activities shall be done after preservation of original media. • File system examination and analysis • User accounts and access analysis • Windows Registry analysis • Event logs - System, Security and Application logs analysis • Anti-virus and other security software logs analysis • Network Connections, Wireshark, Open Shares, RDP and other connection analysis • Disk Analysis • Text view analysis of files • Application Component Analysis • Database analysis • Keyloggers analysis • Deleted files recovery and analysis • Corrupted Executable analysis	M		

	• Collection of evidence in a manner that protects the chain of custody should include the following but not limited: 1.1 Retrieval of Deleted artefacts 1.2 Timeline analysis of installed applications 1.3 USB Device analysis – attached USB devices 1.4 USB devices to correlate files 1.5 Remote Connections analysis 1.6 Malware Analysis 1.7 Timeline analysis of emails Provide technical support for containment, mitigation, and recovery activities such as reimaging, rule changes in security products, patch and configuration changes in assets, deactivating accounts etc.			
9	Licenses – Bidder shall use its own licenses (log analysis, scaling, Investigation at scale and disk analysis) and tools as part of this RFP. During incident management, if a need arises for any specific hardware/ software license (like Threat Hunting, Mobile forensics, and disk Imaging-Write Blocker). Bidder and Nainital Bank will mutually discuss the same and procure the same separately. Bidder shall not be responsible for updating or creating policy and procedure documentation unless engaged for the same.	M		
10	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 the first compromise was. • Maintain artifacts & IOCs of an incident.	M		
11	Bidder to describe how it performs a strong Incident Response Mechanism in providing Bank with comprehensive information about a potential incident, assembling the appropriate context, investigating as make recommendations so that Bank starts containment & remediation activities.	M		
12	Vendor to help Bank's team in performing the post incident analysis & RCAs which shall help in improving the Incident Management process & learning.	M		
13	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	M		

S.No.	Requirement	Category	Compliance	Remarks
C.	**Brand Monitoring**			
	Technical Specifications – Brand Monitoring			
1.	Real time intelligence into online threats and provides a seamless 24x7x365 Global Incident Response.	M		
2.	The Solution should identify and mitigate compromised accounts in real time.	M		

3.	The Solution should identify end users and transactions compromised by malware.	M		
4.	The Solution should be web-based portal with alerts and reports	M		
5.	The Solution should be 24x7x365 Global security Incident Response	M		
6.	Whitelist Management – Solution should have central management system offering a secure mechanism to manage portfolio of Brands, Domains, Social presence and Mobile Apps across different OS, brands and versions.	M		
7.	Monitoring and Detection - Real time monitoring and pre-attack detection across the channels. Multiple independent services need to be correlated and provided as one integrated solution.	M		
8.	Solutions should detect sources of phishing, malware and abuse targeting the organization, if any.	M		
9.	Service should be available where client SPAM or data can be sent to a dedicated server for real time analysis to detect any threats targeting the client and other brands.	M		
10.	Solution should monitor domain names like– New Domain Registrations, domain names where registration details have recently changed, such as Registrant/Registry contacts, and domain names that have recently expired or have entered Redemption period. Monitoring should also include International Domain Names (IDN) that use non-ASCII characters such as Arabic, Greek, Chinese, Russian, etc.	M		
11.	The solution should have a secure mechanism to analyze web logs, web server referral logs and provide proactive brand protection.	M		
12.	Social Media sites should be monitored using specific keywords and images for brand abuse, malware and rogue apps that may be distributed across the social spectrum. Blogs and forums need to be monitored for client trademarks and copyright content	M		
13.	Solution should monitor all the 'trusted" App stores, unofficial App stores, telco stores, vendor stores, social media, third party stores to prevent brand abuse	M		
14.	Solution should be able to monitor specific points of presence such as local ISP, DNS, App stores or social media, blogs or forums	M		
15.	Solution should be able to detect or recover following type of files: Stolen / Compromised Login Credentials and Bank Account Information; Compromised Credit Card Details; Personal Identifiable Information (PII) (Customer / Employee data); Private / Sensitive Documents relating to the business; Hacking documents/tools specifically targeting client; Leaked Source Code; Copyright / Trademark infringement; Technical Information / Data that could be used to target corporate systems.	M		
16.	Executive monitoring capability should be available but not limited to Duplicate and fake Social Media accounts, blog and forum content; Identification of PII posted online and dark web; Prevent Cyberstalking, online bullying, hacktivism, and defamation;	M		
17.	Digital Asset Discovery – Solution should discover all websites, public facing web apps, subdomains, subnets, IPs,	M		

	nameservers, certificates, ports, protocols and application configurations, Identify Rogue/ Shadow IT and more.			
18.	Solution should detect any changes in public facing content above set threshold parameters. Detect unauthorized content by internal users, third parties and malicious actors.	M		
19.	Solutions should monitor for a range of threats, malware, defacement across the public surface web apps.	M		
20.	Web Defacement - real time monitoring of websites for hacking, defacement, malicious code.	M		
21.	Infrastructure Monitoring - monitoring of exposed network surface services including network and Open VAS, TCP/UDP/SSL/OS Configuration status and checks.	M		
22.	Incident Management - real-time alerts, sandbox analysis, verification, reporting and recommendations for remediation.	M		
23.	Website Reputation - checking websites, apps, domains against global blacklists to report on reputation status.	M		
24.	Real Time and Monthly Executive Summary Reports. Real-time Incident and Analysis reports as well as Executive Summary reports. All master data should be downloadable in .csv format	M		
25.	The solution should be able to: Discover and evaluate the ransomware and malware components, provide forensic analysis to respond and mitigate against the malicious content, discover if, where and how data is being transmitted to a third party; Identify third party sites for Response and Enforcement	M		
26.	Customers should be notified of Incident Creation, Incident Updates, Analysis Reporting and Intelligence, Recovered Forensics, Incident Closure and when any relevant event occurs during the response process	M		
27.	Threat Category - moderate to critical threat level incidents shall be actioned automatically without any client intervention. Categorization of Low or Moderate shall generate an alert to the customer and customer response will be required	M		
28.	Unlimited Takedowns should be available in the solution. In the case of a phishing site, immediate Site Take Down shall be automatically initiated. In cases of malware incidents or malicious mobile apps a site takes down on malware back-end malware infrastructure such as Update Points, Control and Command Servers, and Credential Drop Sites, shall occur.	M		

Sr. No.	**Requirement**	**Category**	**Compliance**	**Remarks**
D.	**Threat Intelligence & Analytic**			
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.	M		
2.	Service Provider should anticipate likely threats to the Bank both from outside (global intelligence) as well as arising from bank's internal infrastructure.	O		
3.	Service Provider should support integration of machine-readable threat intelligence from different open and commercial sources. It should support providing weightage	O		

	against sources and support algorithms to reduce noise & false positives in threat intelligence feeds.			
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.	M		
5.	Service providers 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	M		
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.	M		
	Threat Hunting	**Category**	**Compliance**	**Remarks**
7.	Services 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.	M		
8.	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	M		
9.	Service to detect access to anomalies e.g. Detection of deviation in the interaction of one server with another to detect attacks such as lateral movements.	M		
10.	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.	M		
	Advanced Alert Analytics & Attack Detection Capabilities	**Category**	**Compliance**	**Remarks**
11.	The solution should have capabilities to detect any compromises by linking related alerts collected over a period.	M		
12.	Solution should have capabilities to correlate alerts between sources & destination IPs to find similar or colluding threat signals.	M		
13.	Solution should have a knowledge base on methods used by attackers in various past breaches globally to create models to detect such attacks.	M		
14.	Solution should utilize data science techniques to identify kill chains for attacks such as lateral movements e.g. If a	M		

	destination IP of one alert later becomes a source IP of another alert this suggests existence of a sequence.			
15.	The solution should have detection models to find out threat's sources are linked to the same attacker by grouping alerts with common characteristics like time, day location, target asset profiles etc.	M		
	Rule Based Detection (Traditional SIEM Capabilities)	**Category**	**Compliance**	**Remarks**
16.	In addition to the advanced analytics capabilities like MDR, solutions 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	M		
	Incident Analysis	**Category**	**Compliance**	**Remarks**
17.	Solution should support auto-triaging of alerts from a number of security products including Firewalls, PIM, DLP, IPS, WAF, Anti-APT, HIPS, AV etc.	M		
18.	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.	M		

The solution should provide comprehensive Active Directory protection covering the following:

Sr. No.	Features	Category	Compliance	Remarks
E.	**AD Security**			
1.	The proposed solution should provide Visibility to AD security hygiene issues and actionable alerting to key exposures at the domain, computer, and identity level.	M		
2.	The proposed solution should provide Real-time provide detection of AD privilege escalation and granularly restricting access to AD information without impacting business operations.	M		
3.	The proposed solution should provide Continuous visibility into identities and service account risks related to credentials, shadow administrators, stale accounts, shared credentials, and identity attack paths.	M		
4.	The proposed solution should provide detection exposures that lead to Credentials harvesting from Sysvol & Netlogon Share" with "Default permissions changes on Schema Partition".	O		
5.	The proposed solution should provide Perform a Domain Dominance Assessment provide detection weak policies that could lead to Golden Ticket" with "Default permissions changes on Domain Partition"	O		
6.	The proposed solution should provide detection presence of Dangerous trust relationship \ Enable SID Filtering" with "Skeleton Key Vulnerability Assessment."	O		

7.	The proposed solution should provide detection policies for use of Anonymous & Unsigned LDAP protocol" with "Trust accounts passwords that have not changed"	O		
8.	The proposed solution should provide detection if the Default Administrator account has been hardened" with "Domain using a dangerous backward-compatibility configuration".	M		
9.	The proposed solution should provide detection if Unprivileged Users exist in Admin Holder ACL" with "Computers Accounts with password not changed recently".	M		
10.	The proposed solution should "provide detection Accounts with Pre-Authentication disabled" with "Unusual Accounts with Replication Permissions (DCSync)"	M		
11.	The proposed solution should "provide detection if Unprivileged users listed as DNS Admins" with "AdminCount attribute set on standard users	M		
12.	The proposed solution should "provide detection dangerous computer accounts delegations" with "Servers with passwords unchanged for more than 60 days"	M		
13.	The proposed solution should provide detection Brute force attacks – mass account lockouts.	M		
14.	The proposed solution should provide detection Brute force attacks – mass account disabling.	M		
15.	The proposed solution should provide detection of suspicious password change on service accounts.	M		
16.	The proposed solution should provide detection suspicious password changes for sensitive accounts.	M		
17.	The proposed solution should provide detection Suspicious Service Creation on Domain Controller.	M		
18.	The proposed solution should provide detection Brute force attacks – provide detection mass password reset / changes.	M		
19.	The proposed solution should provide detection brute force attacks – Password Spray attack.	M		
20.	The proposed solution should provide detection Reactivation of Disabled Privileged Accounts Provide detection suspicious service creation on domain controller.	M		
21.	The proposed solution should provide detection and detection DC Shadow attacks.	M		
22.	The proposed solution should provide detection Shadow Admins in Privileged groups.	M		
23.	The proposed solution should provide detection Service Accounts that have shadow Admin privileges.	M		
24.	The proposed solution should provide detection Non-Use of Managed Service Accounts.	M		
25.	The proposed solution should provide detection Guest account is enabled.	M		
26.	The proposed solution should Check for enabled Wdigest that could lead to credentials theft	M		
27.	The proposed solution should provide detection LAPS Solution not enabled on Domain.	M		

28.	The proposed solution should provide detection Group Policy Objects - Unlinked, disabled or orphan.	M		
29.	The proposed solution should provide detection Credentials harvesting from Domain Shares.	M		
30.	The proposed solution should provide detection Protected Users group not created or not used.	M		
31.	The proposed solution should provide detection High-Risk Trust relationships	M		
32.	The proposed solution should provide detection Domain with Advanced Audit Policy disabled.	M		
33.	The proposed solution should provide detection. Regular users can add new computers into the AD domain.	M		
34.	The proposed solution should provide detection Multiple issues in the password policy.	M		
35.	The proposed solution should provide detection Rogue domain controllers.	M		
36.	The proposed solution should provide detection Dangerous access rights delegation on critical objects.	M		
37.	The proposed solution supports the detection of Active Directory targeted attacks by intercepting attack queries without applying any changes on production active directory servers.	M		
38.	The proposed solution should support intercepting AD queries/responses of privileged accounts (Domain Admins, Administrators, Enterprise Admins, Schema Admins, Group Policy Creator Owners), hide real accounts and add deceptive accounts to misdirect the attacker to decoys AD and servers.	M		
39.	The proposed solution should prevent compromise of Privileged Credentials.	M		
40.	The proposed solution should prevent a compromise of Service Accounts.	M		
41.	The proposed solution should prevent compromise of Shadow Admin Accounts or Delegated Admins.	M		
42.	The proposed solution should prevent the compromise of Domain Controllers.	M		
43.	The proposed solution should prevent attacks that target network sessions with privileged accounts.	M		
44.	The proposed solution should prevent theft of Kerberos tickets with privileged accounts to be used for Pass-the-ticket attacks. It must also mis-direct an attacker thereby disrupting the attack.	M		
45.	The proposed should ensure comprehensive assessment and attack detection, providing coverage across domain, user, and computer levels.	M		
46.	The proposed solution should detect and prevent all Pass-the-ticket attacks (Golden and Silver Ticket Attacks)	M		
47.	SOC setup/infrastructure may be subjected to audit from third party and/or regulatory body. It shall be the responsibility of the Vendor to co-operate and provide necessary information and support to the auditors. The Vendor must ensure that the audit observations are closed on top priority and to the satisfaction of regulatory body and its appointed	O		

	auditors. Extreme Due care should be taken by the Vendor to ensure that the observations do not get repeated in subsequent Audits.			
48.	SLA's and implementation timelines for the various activities would be mutually agreed while signing a contract with the selected SP. However, the service Provider is expected to give an overall implementation and roll out plan as part of this proposal with templates of SLA, Project Plan, Governance meeting templates etc.	O		
49.	Analytical reports on Daily, weekly and Monthly basis and Ad-hoc reports as and when to be provided by service provider	O		
50.	During the exit of the contract or services the vendor should provide logs as per retention period from their end to The Nainital Bank Limited without any Price	O		

F.	**CCMP (One Time)**	Frequency		
1	Security Incident and Crisis Management services Plan formulation – This would need to be provided as a one-time service at the start of the contact.	One Time		
2	Alignment of Security Incident management plan in line with Banks Cyber Crisis Management Plan (CCMP)to be provided by the solution provider and Cyber Security Policy and review of both the policies.	One Time		
3	The Incident and Cyber crisis management support shall be (preferred online and, in case of emergency, online support is mandatory) provided by MSSP	One Time		
4	MSSP will provide a detailed process for managing cyber incidents - describing each phase of the process – prepare, identify, contain, eradicate, recover and learn from the incidents	One Time		
5	Develop response plan/ strategy which will describe the prioritization of incidents based on the organizational impact	One Time		
6	security event and generate alerts & establishing process for identifying, preventing, detecting, analysing & reporting all Information Security incidents as per the best practices, this may revise from time to time as per the requirements	One Time		
7	Incident and problem Management, resolution, root cause analysis, and reporting within time limit as per the requirement	One Time		
8	Describe the incident response process including the roles and responsibilities and scope of action in line with CCMP	One Time		
9	MSSP must provide on demand timely support by performing investigation and forensic analysis on the logs by doing the necessary analysis on the logs by doing the necessary analysis and log review and providing required data in a timely fashion	One Time		
10	MSSP shall provide backend professional incident management team support in case of severe incident occurs	One Time		

Annexure 2 B

Technical Specifications: Information Security Cell

Security Controls: In addition to the eligibility criteria defined in Appendix-2 A, Bidder(s) are also required to comply with the following points and submit their compliance on the same on their letterhead. In case of non-compliance of any of the requirements, bid would be rejected

S. No.	Required Controls	Compliance (Yes/No)
1	Whether Bidder has information security policy in place with periodic review	
2	Whether Bidder has operational processes with periodic review in following areas: a) Business continuity management b) Backup Management c) Desktop/ system/ server/ network device hardening with baseline controls d) Patch management e) Port management f) Media movement g) Log management h) Personnel security i) Physical security j) Internal security assessment processes k) Asset Management l) Change Management	
3	Whether Bidder has implemented physical controls to allow access to computing facilities only to authorized users? If yes, whether the sufficiency and effectiveness of physical controls is assessed by independent security auditors?	
4	Whether Bidder has proper documented policy and process of incident management/ response	
5	Whether Bidder's IT environment is suitably protected from external threats by way of firewall, WAF, IDS/IPS, AD, AV, NAC, DLP etc.	
6	Whether Bidder's IT environment is suitably protected from external threats by way of firewall, WAF, IDS/IPS, AD, AV, NAC, DLP etc.	
7	Whether Bidder monitors firewall rule position regularly for presence of any vulnerable open port or any-any rule.	
8	Whether Bidder has captive SOC or managed service SOC for monitoring their system and operations.	
9	Whether Bidder's environment is segregated into militarized zone (MZ) and demilitarized zone (DMZ) separated by firewall, where any access from an external entity is permitted through DMZ only.	
10	Whether Bidder has deployed secure production, disaster recovery and testing environment for their application.	
11	Whether quarterly/Half yearly vulnerability assessment and penetration testing is being done by the Bidder for its IT infrastructure.	
12	While sharing the data, whether Bidder is agreeable to encrypt the same as per industry best standards with robust key management.	
13	Whether Bidder is agreeable to store the data with encryption (Data at rest encryption), if storing is permitted in RFP.	
14	Bidder to confirm that it will not share the NTBL's data to any other party for any purpose without prior permission of the NTBL.	
16	Bidder to confirm that it will not take any crucial decisions on behalf of the NTBL without written approval from the NTBL	

17	Whether Bidder is willing to purge the post archival data regularly and report the same to the NTBL	
18	Whether Bidder is willing to purge the post archival data regularly and report the same to the NTBL.	
19	Whether bidder is having system in place for proper log generation, storage, management and analysis?	
18	Whether bidder is maintaining all Web, Application, DB, Configuration and User access logs for forensic readiness?	
19	Whether bidder is maintaining logs for privileged access to their critical systems?	
20	Bidder must comply to all RBI/CERT-in and other frameworks & circulars existing & new.	

Documents forms to be put in Envelop A

1. Annexure A1 - Bidder's Letter for Application Money & EMD Details

To,
The Chief Operating Officer
Nainital Bank Ltd
Head Office
Mallital, Nainital -263001 (Uttarakhand)

Subject: **RFP # NTBL/ISC/SOC/2024/11/22** dated **06-11-2024** for "Request for proposal for engaging a Managed Security Service Provider for Security Operations Centre (SOC) Services with Managed, Detection and Response (MDR) Along with Brand Monitoring, Breach Investigation, AD Security and Threat Hunting Capabilities.

a. We have enclosed an Application Money in the form of a DD/PO/NEFT - UTR No_____issued by the branch of the_____Bank, for the sum of Rs_____(Rupees_____). This Application money is as required by clause 2.11 of the Instructions to Bidders of the above referred RFP.
b. We have enclosed an EMD in the form of a DD/PO/NEFT/RTGS - UTR No_____issued by the branch of the_____Bank, for the sum of Rs_____(Rupees_____). This EMD is as required by clause 2.11 of the Instructions to Bidders of the above referred RFP.

Thanking you,

Yours faithfully,

(Signature of the Bidder)
Name:
Designation:
Seal:
Date:
Business Address:

2. Annexure A2 - Bid Security (Bank Guarantee)

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

Date:
[Bank's Name, and Address of Issuing Branch or Office]

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 a Managed Security Service Provider for Security Operations Centre (SOC) Services with Managed, Detection and Response (MDR) Along with Brand Monitoring, Breach Investigation, AD Security and Threat Hunting Capabilities for three years for The Nainital Bank Limited (hereinafter called "the Purchaser") in response to Request for Proposal **RFP# NTBL/ISC/SOC/2024/11/22** (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. 7,00,000/- (Rupee Seven 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:
   - 2.1 fails or refuses to execute the Contract; or
   - 2.2 fails or refuses to furnish the Security Deposit/ Bank Guarantee for contract performance.

We undertake to pay the Purchaser up to 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 two conditions, specifying the occurred condition or conditions.
This Guarantee will remain in force up to and including _____months i.e. up to _____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 up to _____ 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 the Bank under this Guarantee shall be limited to INR Rs. 7,00,000/- (Rupee Seven lakh only).

Place :

SEAL Code No. Signature

NOTE:
1.Bidder should ensure that the Seal & Code no of the signatory is put by the bankers, before submission of BG.
2.Stamp paper is required for the BG issued by the scheduled commercial banks in some states.

3. Annexure A3 - Bid Security

(PERFORMANCE BANK GUARANTEE FORMAT)

To,
The _____
The Nainital Bank Limited
_____
_____

In consideration of The Nainital Bank Limited, having its Registered office at G.B. Pant Road, Nainital (hereinafter referred to as NTB) (which expression shall unless repugnant to the context or meaning thereof shall include its successors, representatives and assignees) having awarded in favour of _____ a Company registered under the Companies Act, 1956 (now the Companies Act 2013) and having its registered Office at _____ (hereinafter referred to as "Service Provider") a Purchase Order No. _____ dated _____, hereinafter referred to as contract/agreement for the _____ at Bank Branches/Offices With _____ on terms and conditions set out in contract aforesaid, which is valued at Rs._____ (Rupees _____ Only) and the same having been unequivocally accepted by the Service Provider and the Service Provider having agreed to provide a Contract Performance Guarantee for due, satisfactory and faithful performance of entire 'Contract' including the warranty obligations/liabilities under the said contract equivalent to _____ of the said value of the contract to the NTB amount to Rs._____(Rupees _____ Only) as Contract Security in form of a Bank Guarantee (hereinafter called as 'the Performance Guarantee').
AND WHEREAS the Service Provider has approached us, _____, a body corporate in terms of the Banking Companies Acquisition and Transfer of Undertakings Act,1970/1980 having it's registered office at _____ and amongst other places, a branch at _____ (hereinafter referred to as the Bank) for providing the Performance Guarantee to NTB,

AND WHEREAS in consideration of the fact that the Service Provider is our valued constituent and the fact that they have entered into the Agreement with NTB, we_____, a body corporate in terms of the Banking Companies Acquisition and Transfer of Undertakings Act,1970/1980 having it's registered office at _____ and amongst other places, a branch at _____ have agreed to issue the Performance Guarantee,

THEREFORE, we the Bank through our Registered office at _____and amongst other places, a branch at _____ India furnish you, the NTB, the Performance Guarantee in manner hereinafter contained and agree with NTB as follows:

We _____(Bank name) do hereby expressly, irrevocably and unconditionally guarantee and undertake to pay NTB, on demand any and all money payable under this Guarantee without any demur, merely on demand from you and undertake to indemnify you and keep you indemnified from time to time and at all times to the extent o of Rs._____ (Rupees _____ Only) an amount equivalent to 10% of the Total Purchase Order Value excluding tax if any against any loss or damage caused to or suffered by or that may be caused to or suffered by NTB on account of any material breach or breaches on the part of the Service Provider of any of the terms and conditions contained in the Agreement and in the event of the Service Provider default or defaults in carrying out any of the work or discharging any obligation in relation thereto under the Agreement or otherwise in the observance and performance of any of the terms and conditions relating thereto in accordance with the true intent and meaning thereof we shall forthwith on demand pay to NTB such sum or sums not exceeding the sum of Rs._____ (Rupees _____Only) claimed by NTB on account of breach on the part of the Service Provider of their obligations in terms of the Agreement.

Notwithstanding anything to the contrary herein or elsewhere, we agree that NTB's decision as to whether the Service Provider has made any such breach/default or defaults and the amount or amounts to which the NTB is are entitled by reasons thereof will be binding on us and we shall not be entitled to ask the NTB to establish NTB's claim or claims under Performance Guarantee but will pay the same forthwith on NTB's demand without any

protest or demur. Any such demand made by NTB shall be conclusive as regards the amount due and payable by us to you.

This Performance Bank Guarantee shall continue and hold good until it is released by you on the application by the Vendor after expiry of the relative guarantee period provided always that the guarantee shall in no event remain in force after..... (date) without prejudice to your claim or claims arisen and demanded from or otherwise notified to us in writing before the expiry of the said date which will be enforceable against us notwithstanding that the same is or are enforced after the said date.

Should it be necessary to extend Performance Guarantee on account of any reason whatsoever, we may extend the period of Performance Guarantee at our sole discretion only on a request from the Service Provider till such time as may be required by NTB.

NTB will have the fullest liberty without affecting Performance Guarantee from time to time to vary any of the terms and conditions of the Agreement or extend the time of performance of the agreement/Contract or to postpone any time or from time to time any of its rights or powers against the Service Provider and either to enforce or forbear to enforce any of the terms and conditions of the Agreement and we shall not be released from our liability under Performance Guarantee by the exercise of NTB's liberty with reference to matters aforesaid or by reason of any time being given to the Service Provider or any other forbearance, act, or omission on its part or any indulgence by it to the Service Provider or by any variation or modification of the Agreement or any other act, matter or things whatsoever which under law relating to sureties, would but for the provisions hereof have the effect of so releasing us from our liability hereunder provided always that nothing herein contained will enlarge our liability hereunder beyond the limit of Rs._____(Rupees _____ Only) as aforesaid or extend the period of the guarantee beyond the said day of _____ unless expressly agreed to by us in writing.

The Performance Guarantee shall not in any way be affected by your taking or giving up any security from service provider or any other person, firm or company on its behalf or by the winding up, dissolution, insolvency or death as the case may be of the Service Provider or due to any disputes raised or pending before any Court, Tribunal, Arbitration or any other authority.

We agree that the guarantee herein contained shall continue to be enforceable till this sum due to the NTB is fully paid and claim is satisfied or till the Service Provider disagrees the obligations contained in the said Agreement or until _____whichever is earlier.

In order to give full effect to the guarantee herein contained, NTB is entitled to act as if we were its principal debtors in respect of all its claims against the Service Provider hereby guaranteed by us as aforesaid and we hereby expressly waive all our rights of suretyship and other rights, if any, which are in any way inconsistent with any of the provisions of Bank Guarantee and notwithstanding any other Security or guarantee that we may have in relation to the Service Provider liabilities.

Subject to the maximum limit of our liability as aforesaid, Performance Guarantee will cover all claim or claims of NTB against the Service Provider from time to time arising out of or in relation to the Agreement and in respect of which its claim in writing is lodged on us from the date of claim expiry of Performance Guarantee.

Any notice by way of written demand or otherwise hereunder may be sent by special courier, registered post to our local address as aforesaid and if sent by post it shall be deemed to have been served on the date of it being received by us duly acknowledged shall mean delivery to the Branch.

The Performance Guarantee and the powers and provisions herein contained are in addition to and not by way of limitation of or substitution for any other guarantee or guarantees heretofore given to NTB by us (whether jointly with others or alone) and now existing un-cancelled and that Performance Guarantee is not intended to and shall not revoke or limit such guarantee or guarantees.

The Performance Guarantee shall not be affected by any change in the constitution of the Service Provider or us nor shall it be affected by any change in NTB's constitution or by any merger, amalgamation or absorption thereof or therewith, but will endure to the benefit of and be available to and be enforceable by the absorbing or amalgamated company or concern.

The Performance Guarantee shall come into force from the date of its execution and shall not be revoked by us any time during its currency without your previous consent in writing.

We further agree and undertake to pay to NTB the amount demanded by it in writing irrespective of any dispute or controversy between you and the Service Provider in any suit or proceedings pending before any court or tribunal including arbitration relating thereto, our liability under this present being absolute and unequivocal. The payments so made by us shall be valid discharge of our liability for payment hereunder and the Service Provider shall have no claim against us for making such payment.

Notwithstanding anything contrary contained in any law for the time being in force or banking practice, this guarantee shall not be an assignable or transferable by the beneficiary. Notice or invocation by any person such as assignee, transferee or agent of the beneficiary shall not be entertained by the bank. Any invocation of guarantee can be made only by the beneficiary directly.

Notwithstanding anything contained herein

i. Our liability under this guarantee shall not exceed Rs._____ (Rupees _____Only).
ii. This guarantee shall be valid and remain in force upto and including the date _____ and,
iii. The beneficiary's right as well the Bank's liability under this Guarantee shall stand extinguished unless a written claim or demand is made under this Guarantee on or before completion of one year from expiry date i.e. _____.

We have the power to issue this Bank Guarantee in your favour under the Memorandum and Articles of Association of our Bank and the undersigned has full power to execute this Bank Guarantee under the Power of Attorney issued by the Bank.

Dated this _____(month)___202_____

For and on behalf of

_____ Bank

Seal and Address

NOTE:

1. Vendor should ensure that the seal & code no. of the signatory is put by the bankers, before submission of BG
2. Stamp paper is required for the BG issued by the banks located in _____
3. Bank guarantee if submitted, should be accompanied with copy of the SFMS transmitted at the time of issue of bank guarantee. As per IBA notification no. PS&BT/Govt/2305 dated 16-mar-2016 along with ministry of finance, government of India circular f.no.7/112/2011-boa dated 08-mar-2016 with respect to sending bank guarantee advices through structured financial messaging system (SFMS), it is necessary to confirm the authenticity of the bank guarantees (BG) by SFMS message. The SFMS should be sent to following branch: _____IFSC code:
4. Vendor should ensure that the bank guarantee should contain all terms & conditions as per this format. Bank guarantee submitted with any rider or deviation to the stipulated terms & conditions will not be accepted

4. Annexure B - Bid Offer Form (without Price)

(Bidder's Letter Head)
OFFER LETTER

Date:

To,
The Chief Operating Officer
Nainital Bank Ltd
Head Office
Mallital, Nainital -263001 (Uttarakhand)

Dear Sir,
Subject: RFP # NTBL/ISC/SOC/2024/11/22 dated 06-11-2024 for "Request for proposal for engaging a Managed Security Service Provider for Security Operations Centre (SOC) Services with Managed, Detection and Response (MDR) Along with Brand Monitoring, Breach Investigation, AD Security and Threat Hunting Capabilities.

We have examined the above-mentioned RFP document. As per the terms and conditions specified in the RFP document, responses to the pre-bid queries and in accordance with the schedule of prices indicated in the commercial bid and made part of this offer.
We acknowledge having received the following addenda / corrigenda/ pre-bid responses to the RFP document.

Addendum No. / Corrigendum No/Pre-bid responses	**Dated**

While submitting this bid, we certify that:
1. All the Prices have been quoted in INR.
2. The prices in the bid have not been disclosed and will not be disclosed to any other bidder of this RFP.
3.We have not induced nor attempted to induce any other bidder to submit or not submit a bid for restricting competition.
4. We agree that the rates / quotes, terms, and conditions furnished in this RFP are for The Nainital Bank Limited. If our offer is accepted, we undertake to start the assignment under the scope immediately after receipt of your order. We have taken note of Penalty clauses in the RFP and agree to abide by the same. We also note that The Nainital Bank Limited reserves the right to cancel the order. We understand that for delays not attributable to us or on account of uncontrollable circumstances, penalties will not be levied and that the decision of The Nainital Bank Limited will be final and binding on us.
We agree to abide by this offer till 180 days after the last date of submission of bid date stipulated by The Nainital Bank Limited for submission of bid, and our offer shall remain binding upon us and may be accepted by The Nainital Bank Limited any time before the expiry of that period.
Until a formal contract is prepared and executed with the selected bidder, this offer will be binding on us. We also certify that the information/data/particulars furnished in our bid are factually correct. We also accept that in the event of any information / data / particulars are found to be incorrect, The Nainital Bank Limited will have the right to disqualify /blacklist us and forfeit bid security.
We undertake to comply with the terms and conditions of the bid document. We understand that The Nainital Bank Limited may reject any or all the offers without assigning any reason whatsoever.
As security (EMD) for the due performance and observance of the undertaking and obligation of the bid we submit herewith RTGS/BG bearing no. ----------dated----------drawn in favor of "The Nainital Bank Limited" or Bank Guarantee valid for----------days for an amount of Rs. ---------- (Rs.--------- only) payable at Nainital.

Yours sincerely,
Authorized Signature
[In full and initials]:
Name and Title of Signatory:
Name of Company/Firm:
Address

5. Annexure C - Bidder Information

(Bidder's Letter Head)
Bidder Profile

To,
The Chief Operating Officer
Nainital Bank Ltd
Head Office
Mallital, Nainital -263001 (Uttarakhand)

Sub: Request for proposal (RFP) for RFP # NTBL/ISC/SOC/2024/11/22 dated 06-11-2024.

Having examined the Tender Documents including all Annexures and Appendices, the receipt of which is hereby duly acknowledged, we, the undersigned offer to supply, deliver, implement and commission ALL the items/activities mentioned in the 'Request for Proposal' and the other schedules of requirements and services for your bank in conformity with the said Tender Documents in accordance with the schedule of Prices indicated in the Price Bid and made part of this Tender.

We also submit the required information along with documentary evidence in the following format:

Sr.	Particulars	Details
1.	Name of the Bidder	
2.	Address of the Bidder	
3.	Status of the Company (Public Ltd/ Pvt. Ltd)/Firm/LLP etc.	
4.	Details of Incorporation of the Company/Firm	
5.	Details of Commencement of Business	Date: Ref
6.	GSTIN Number HSN Number	
7.	Permanent Account Number (PAN)	
8.	Name & Designation of the authorized contact person to whom all references correspondence shall be made regarding this tender Including (Contact no and Email id:)	
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.	Details of NEFT/RTGS transaction details (if Application Money, Fees for proposed solution features, and EMD are credited to Bank through electronic mode).	
14.	Details of accounts wherein the EMD amount is to be returned if the EMD is sent through NEFT / RTGS.	The following details are to be submitted: Account Name – Account Number – IFSC Code – Bank Name - Branch Name -
Financial Details (as per audited Balance Sheets) (in Cr)		

	Year	2020-2021	2021-2022	2022-2023	2023-24
15	Net worth				
16	Turn Over				
17	Profit After Tax (PAT)				

If our Bid is accepted, we undertake to comply with the delivery schedule as mentioned in the Tender Document.

3. We agree to abide by this Tender Offer for 180 days after the last date of submission of bid date and our Offer shall remain binding on us and may be accepted by the Bank any time before expiry of the offer.

4. This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

5. We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".

6. We agree that the Bank is not bound to accept the lowest or any Bid the Bank may receive.

7. We certify that we have provided all the information requested by the bank in the format requested for.

We also understand that the bank has the exclusive right to reject this offer in case the bank is of the opinion that the required information is not provided or is provided in a different format.

Dated this……..by …….2024

Yours faithfully,
Authorized Signatory
Name:
Designation:
Bidder's Corporate Name
Address
Email and Phone #

6. Annexure D - Declaration for Clean Track Record

Declaration for non-blacklisting
(Bidder's Letter Head)

To,
The Chief Operating Officer
Nainital Bank Ltd
Head Office
Mallital, Nainital -263001 (Uttarakhand)

Dear Sir,

Subject: RFP # NTBL/ISC/SOC/2024/11/22 dated 06-11-2024 for "Request for proposal for engaging a Managed Security Service Provider for Security Operations Centre (SOC) Services with Managed, Detection and Response (MDR) Along with Brand Monitoring, Breach Investigation, AD Security and Threat Hunting Capabilities.

I have carefully gone through the Terms & Conditions contained in the NTBL/ISC/SOC/2024/11/22 dated 06-11-2024.
I hereby declare that my company has not currently been debarred/blacklisted by any Government / Semi Government / Private organizations in India / abroad. I further certify that I am a competent officer and duly authorized by my company to make this declaration.

Yours faithfully,

(Signature of the Bidder)
Printed Name
Designation
Seal Date:
Business Address:

7. Annexure E - Declaration for Acceptance of RFP Terms and Conditions

(**Bidder's Letter Head)**

To,
The Chief Operating Officer
Nainital Bank Ltd
Head Office
Mallital, Nainital -263001 (Uttarakhand)

Dear Sir,

Subject: RFP # NTBL/ISC/SOC/2024/11/22 dated 06-11-2024 for "Request for proposal for engaging a Managed Security Service Provider for Security Operations Centre (SOC) Services with Managed, Detection and Response (MDR) Along with Brand Monitoring, Breach Investigation, AD Security and Threat Hunting Capabilities.

I/WE have carefully gone through the terms & conditions contained in the NTBL/ISC/SOC/2024/11/22 dated 06-11-2024.
I/WE declare that all the provisions of this RFP/Tender Document are acceptable to my company. I/WE further certify that _____ is the authorized signatory of my company and, therefore, competent to make this declaration.

Yours faithfully,

(Signature of the Bidder)
Printed Name
Designation
Seal Date:
Business Address:

8. Annexure F - Declaration for Acceptance of Scope of Work

(Bidder's Letter Head)

To,
The Chief Operating Officer
Nainital Bank Ltd
Head Office
Mallital, Nainital -263001 (Uttarakhand)

Dear Sir,

Subject: RFP # NTBL/ISC/SOC/2024/11/22 dated 06-11-2024 for "Request for proposal for engaging a Managed Security Service Provider for Security Operations Centre (SOC) Services with Managed, Detection and Response (MDR) Along with Brand Monitoring, Breach Investigation, AD Security and Threat Hunting Capabilities.

I/WE have carefully gone through the scope of work (including the scope of work mentioned in responses to pre-bid queries/Corrigendum/Corrigenda) contained in the NTBL/ISC/SOC/2024/11/22 dated 06-11-2024.

I/WE declare that all the provisions of this RFP / Tender Document are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours faithfully,

(Signature of the Bidder)
Printed Name
Designation
Seal Date:
Business Address:

9. Annexure G - Format Power of Attorney

(On Stamp paper of relevant value)

Know all men by the present, we ----------(name of the company and address of the registered office) do hereby appoint and authorize ---------- (full name and residential address) who is presently employed with us holding the position of----------as our attorney, to do in our name and on our behalf, deed and things necessary in connection with or incidental to our proposal for---------- in response to the NTBL/ISC/SOC/2024/11/22 dated 06-11-2024 for "Request for proposal for engaging a Managed Security Service Provider for Security Operations Centre (SOC) Services with Managed, Detection and Response (MDR) Along with Brand Monitoring, Breach Investigation, AD Security and Threat Hunting Capabilities., including signing and submission of all the documents and providing information/responses to The Nainital Bank Limited in all the matter in connection with our bid. We hereby agree to ratify all deeds and things lawfully done by our said attorney pursuant to this Power of Attorney and that all deeds and things done by our aforesaid attorney shall always be deemed to have been done by us.

Dated this ----------day of_____ 2024.
For ---------- .

(Signature)

(Name Designation and Address)

Accepted

(Signature)
(Name Designation) Date:
Business Address:

10. Annexure H1 - Eligibility Criteria Compliance

(Bidder's Letter Head)

Sr. No	Eligibility Criteria	Compliance (Yes/No)	Documentary proof to be attached
1	The bidder should be incorporated or registered in India under Companies Act/Partnership Act / Indian Trust Act (Annual filling with ROC) and should have the Certificate issued by Department for Promotion of Industry and Internal Trade (DPIIT) or in the process of applying the same and shall be submitted before a formal engagement with THE NAINITAL BANK LIMITED.		1. Certificate of incorporation 2. MSME registration certificate (if applicable) 3. DPIIT (for startups)
2	The bidder's annual turnover should be less than Rs. 100 crores as per audited financial statements in each of the financial years from the date of registration/ incorporation subject to compliance to Sr. No. 3		1. Standalone audited financial statements for last 3 years a. Balance sheets b. Profit /loss statement c. Signed Statutory Auditor's Report d. Notes to Accounts and Schedules forming part of accounts to be submitted. • Complete financial statements duly signed/ approved by Auditor. 2. CA certificate in case more than 3 years for previous years
3	The date of incorporation of the bidder should be anywhere between 1 to 10 financial years		Certificate of incorporation/ registration
4	Neither the OEM nor the Bidder should have been currently blacklisted by any Bank or institution in India or abroad.		Declaration letter from the Bidder and OEM as per Annexure D
5	The bidder should be authorized to quote and support for OEM products and services. The bidder shall not get associated with the distribution channel once in any other capacity once he is eligible for price discussion.		Authorization from OEM. Self-declaration of not being part of distribution channel
6	The Bidder has paid or submitted along with the bid submission required Application Money as mentioned in the RFP.		Remittance proof of RTGS in favor of The Nainital Bank Limited **Annexure- A1**
7	The Bidder has paid or submitted along with the bid submission required EMD as mentioned in the RFP.		Remittance proof of RTGS/ BG in favor of The Nainital Bank Limited **Annexure- A1 or AnnexureA-2.**

11. Annexure H2 – Other Than Start Ups.

Sr. No.	MSME	Other than MSME	Compliance Yes/No	Documentary proof to be attached
1.	The bidder is a Company registered under the Companies Act/ Partnership / LLP at least since last three (3) years. In case the bidder is the result of a merger / acquisition, at least one of the merging companies should have been in operation for at least two (2) years as on date of submission of the bid. In case the bidder is the result of a demerger / hiving off, at least one of the demerged company or resulting company should have been in operation for at least two (2) years as on the date of submission of bid.	The bidder is a Company registered under the Companies Act/ Partnership / LLP at least since last five (5) years. In case the bidder is the result of a merger / acquisition, at least one of the merging companies should have been in operation for at least five (5) years as on date of submission of the bid. In case the bidder is the result of a demerger / hiving off, at least one of the demerged company or resulting company should have been in operation for at least five (5) years as on the date of submission of bid.		1. Certificate of incorporation 2. MSME registration certificate (if applicable)
2.	The bidder should have reported minimum annual turnover of Rs. 20 crores and should have reported profits (profit after tax) as per audited financial statements in at least 2 out of last 3 financial years (FY 2021-22, 2022-23, 2023-24). In case audited financial statements for most recent financial year are not ready, then management certified financial statement shall be considered. In case the bidder is the result of a merger or acquisition or demerger or hive off, due consideration shall be given to the past financial results of the merging entity or demerged entity as the case may be for the purpose of determining the minimum annual turnover for the purpose of meeting the eligibility criteria; should the bidder be in operation for a period of less than 2 financial years. For this purpose, the decision of THE NAINITAL BANK LIMITED will be treated as final and no further correspondence will be entertained on this.	The bidder should have reported minimum annual turnover of Rs. 30 crores and should have reported profits (profit after tax) as per audited financial statements in 2 out of last 3 financial years (FY 2021-22, 2022-23, 2023-24). In case audited financial statements for most recent financial year are not ready, then management certified financial statement shall be considered. In case the bidder is the result of a merger or acquisition or demerger or hive off, due consideration shall be given to the past financial results of the merging entity or demerged entity as the case may be for the purpose of determining the minimum annual turnover for the purpose of meeting the eligibility criteria; should the bidder be in operation for a period of less than 2 financial years. For this purpose, the decision of THE NAINITAL BANK LIMITED will be treated as final and no further correspondence will be entertained on this.		Standalone financial audited financial statements 1. Balance sheets 2. Profit/ loss statement 3. Signed Statutory Auditor's Report 4. Notes to Accounts and Schedules forming part of accounts to be submitted.

3	There shall be no continuing statutory default as on date of submitting the response to the tender. Necessary self-declaration along with extract of auditors' report.	There shall be no continuing statutory default as on date of submitting the response to the tender. Necessary self-declaration along with extract of auditors' report.		Self-declaration to be provided by Bidder
4	Neither the OEM nor the Bidder should have been currently blacklisted by any Bank or institution in India or abroad	Neither the OEM nor the Bidder should have been currently blacklisted by any Bank or institution in India or abroad		Declaration from OEM as per **Annexure D** on company letter head Declaration from Bidder as per **Annexure D** on company letter head
5.	The bidder should be authorized to quote and support for OEM products and services. The bidder shall not get associated with the distribution channel once in any other capacity once he is eligible for price discussion.	The bidder should be authorized to quote and support for OEM products and services. The bidder shall not get associated with the distribution channel once in any other capacity once he is eligible for price discussion.		Declaration from OEM Self-declaration by bidder of not being part of distribution channel
6.	The bidder has paid the bid cost as given in the RFP at the time of purchasing the bid document or has paid or submitted along with the bid submission	The bidder has paid the bid cost as given in the RFP at the time of purchasing the bid document or has paid or submitted along with the bid submission		Remittance proof of Electronic Transfer in favor of The Nainital Bank Limited
7.	The Bidder has paid or submitted along with the bid submission required EMD as mentioned in the RFP.	The Bidder has paid or submitted along with the bid submission required EMD as mentioned in the RFP.		Remittance proof of Electronic Transfer/ BG in favor of The Nainital Bank Limited

Other Eligibility Criteria		
Sr. No.	**Clause**	**Documents Required**
1.	The bidder's organization should be ISO 27001 certified.	Certified copy of Certificate issued by competent authority
3	The bidder should be authorized to quote and support OEM products and services. The bidder shall not get associated with the distribution channel once in any other capacity once he is eligible for price discussion. The bidder must be authorized partner of quoted OEM.	OEM Authorization Letter/Declaration from Bidder from all OEMs MAF (Manufacturer's Authorization Form) to be submitted as per point

4	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.
5	Bidders SOC Capability: Bidder shall provide the details of the SOC owned by them in India and other details	Self-Declaration certificate, giving location details of the SOC owned by them in India along with details of the proposed location for Bank and DR facility.
6	Bidder must have been providing Managed Detection and response services to minimum two (2) BFSI customers during last 3 years in India. The bidder should be providing soc service to atleast 1 Govt./ PSU/ BFSI customer from more than 1 year. Deployed solutions license may or may not be on Bidder's name. The bidder's experience in providing Managed Security Services (MSS) to run Security Operations Centre (SOC) services with Managed Detection and Response (MDR) capabilities in India.	The bidder must submit Purchase Order/Satisfactory Certificate from the organization as supporting documents for the same.
7	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 the bidder.
8	Bidder to provide the declaration that any of its subsidiaries 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 the bidder.
9	Bidder should have certified / skilled resources for SOC / Incident response services. Minimum 5 OSCP / CHFI / CISA / CISM / CISSP & 10 CEH resources on their payroll.	Certificate of relevant resources
10	Bidder should have handled Minimum 5 Incident handling and minimum 2 in BFSI involving fraudulent activities like money transfer, ATM etc. Ransomware / Virus incidents will not be considered.	Purchase order or equivalent document to be submitted
11	Should have a running licensed commercial SIEM tool in environment. Deployed tool should be in Leader Quadrant in Gartner MQ for last 3 Years	Required snapshot/ document to be submitted

Dated this…… Day of 2024
(Signature)
(Name) (In the capacity of)
Duly authorized to sign Bid for and on behalf of

12. Annexure H3 Turnover Certificate

[To be provided by Statutory Auditor/Chartered Accountant on their Letterhead]

NTBL/ISC/SOC/2024/11/22 dated 06-11-2024 for "Request for proposal for engaging a Managed Security Service Provider for Security Operations Centre (SOC) Services with Managed, Detection and Response (MDR) Along with Brand Monitoring, Breach Investigation, AD Security and Threat Hunting Capabilities.

This is to certify that M/s _____, a company incorporated under the Companies Act, 1956 with its headquarters at, _____ has the following Turnover, Net Profit/Loss, and Net worth from its Indian Operations. This information is based on the Audited Financial Statements for FY2021-22, FY2022-23 and FY2023-24.

Financial Year (for Three Consecutive FY)	Annual Turnover (in Rs.)	Net Profit/Loss (in Rs.)	Net Worth (in Rs.)
2021-22			
2022-23			
2023-24			

I/WE declare that all the provisions of this RFP / Tender Document are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours faithfully,

(Signature of the Bidder)
Designation
Seal Date:
Business Address:

13. Annexure I - Requirement of manpower skillset

Details of skill set required for the engagement of engineers but not limited to following:

Position	Skill Set
Level-1 (L1)	Educational qualifications: Graduation in CS / IT / EC or Information Security / Cyber Security / MCA At least one Mandatory certification from: CEH / CSA/CCNA / ISO 27001 / ITIL or Certifications as per Level 2 or Level 3 • Experience: Previous experience in CSOC of 2-5 year.
Level-2 (L2)	• Educational qualifications: Graduation in CS / IT / EC or Information Security / Cyber Security / MCA / MTech • Atleast one Mandatory certification from: CEH / CSA/CISA / CISM / CSXP / CISSP / OSCP / OSCE • Experience of above 3 years and up to 5 years • Previous experience in CSOC of 4-6 years

14. Annexure J - Client Details

(To be included in Envelope B- Technical Bid Envelope)

Sr.No	Particulars	Details
A.	Organization Details	
1.	Name of the Organization	
2.	Address	
3.	Contact Person Name and Designation	
4.	Phone Number of the Contact person	
5.	Email Address of the Contact person	
B.	Project Details	
1.	Name of the Project	
2.	Start Date	
3.	End Date	
4.	Current Status (In Progress / Completed)	
C.	Size of Project	
1.	Value of Work Order (In Lakh) (only single work order)	

(Signature)

(Name) (In the capacity of)

Performance Certificate
(Email confirmation from the issuing company)

[RFP Ref. No. NTBL/ISC/SOC/2024/11/22 dated 06-11-2024**]**

To,
The Chief Operating Officer
Nainital Bank Ltd
Head Office
Mallital, Nainital -263001 (Uttarakhand)

This is to certify that M/s _____ has supplied/implemented the below listed devices.

Name and Full Address of the Purchaser	Purchase Order Number and Date	Name of OEM of the Product and Model Service Offered	Specifications (in brief)	Date of GO LIVE/ Sign Off

The services provided by the M/s _____ for the specified solutions are:

a) Satisfactory
b) Good
c) Very Good — [Select and tick only one]
d) Excellent

and working fine since the date of go-live/ sign-off till date.

The certificate has been issued on the specific request of the company.

Date: _____

Place: _____

[Signature of Authorized Signatory]

Name of Signatory:
Designation:
Email ID:

15. Annexure K - Manufacturer's (OEM) Authorisation Form

To be provided on the Letter head of the OEM duly signed & stamped by their Authorized Signatory

To,
The Chief Operating Officer
Nainital Bank Ltd
Head Office
Mallital, Nainital -263001 (Uttarakhand)

Dear Sir,

Subject: RFP # NTBL/ISC/SOC/2024/11/22 dated 06-11-2024 for "Request for proposal for engaging a Managed Security Service Provider for Security Operations Centre (SOC) Services with Managed, Detection and Response (MDR) Along with Brand Monitoring, Breach Investigation, AD Security and Threat Hunting Capabilities.

We hereby submit the following: -

1. We, M/s_____ are the OEM of the following components/devices/solution being offered to The Nainital Bank Limited through M/s _____ (Bidder's Name), who is our authorized Partner/representative in India for supply of this Product/Solution.

S.No.	Component/ Device/ Solution Name	Model No.	Components/ devices/ solutions conform to all the technical specifications and requirements mentioned in this RFP

2. We agree to provide the device/solution/component being supplied as per the scope of work and technical specifications of this RFP through our partner M/s _____
3. With reference to all the components/parts/assemble/software used inside the company products being quoted by us vide your tender cited above, we hereby undertake that all the components / parts / assembly used inside the company products/software shall be original new components / parts / assembly / software only, from respective OEMs of the products and that no refurbished / duplicate / second hand components / parts / assembly are being used or shall be used.
4. In the case of default/unable to comply with the above at the time of delivery or during implementation, for the IT asset including software already billed, we agree to take back the supplied items without demur, if already supplied and replace the same with new one.

I/WE declare that all the provisions of this RFP / Tender Document are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours faithfully,

(Signature of the Bidder)
Printed Name
Designation
Seal Date:
Business Address:

16. Annexure L – Hardware Requirement

Bidder needs to factor required hardware/ software/ OS/ DB licenses to run the services

17. Annexure M - Commercial Bid Form

(Bidder's Letter Head)

(To be included in Commercial Bid Envelope)

To The Nainital Bank Limited

Dear Sir,

Re: NTBL/ISC/SOC/2024/11/22 dated 06-11-2024 - Request for Proposal engaging a Managed Security Service partner

Having examined the Bidding Documents placed along with RFP, we, the undersigned, offer to provide the required infrastructure in conformity with the said Bidding documents for the sum of Rs (Rupees) (exclusive of taxes) or such other sums as may be ascertained in accordance

with the Schedule of Prices attached herewith and made part of this Bid.

We undertake, if our Bid is accepted, to provide External Cyber Threat Intelligence Solutions within the stipulated time schedule. We agree to abide by the Bid and the rates quoted therein for the orders awarded by NTBL up to the period prescribed in the Bid which shall remain binding upon us. Until a formal contract is prepared and executed, this Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India.

We have complied with all the terms and conditions of the RFP. We understand that you are not bound to accept the lowest or any Bid you may receive.

Dated this…… Day of 2024

(Signature)

(Name) (In the capacity of)

Duly authorized to sign Bid for and on behalf of

18. Annexure N- Commercial Bid

(Bidder's Letter Head)

A- Commercial Bid Format - SOC Services

S.No.	Services	Months/Hours	Amount (GST Extra)
1	Managed Security Services to run the Bank's Security Operations Centre (SOC/SIEM) with Managed Detection and Response (MDR), along with Brand Monitoring, Active Directory security, and Threat Hunting capabilities.	36 Months	
2	Incident Response and Breach Investigation (as per requirement)	30 days	
	Total (Taxes Extra)		

B-Details as under

	Particular	Under line Method	Amount
1	Managed SOC Solution		
1.1	SIEM/SOC-EPS	Total EPS and Range wise Cost 6000-7000 7000-8000 8000-10000	
1.2	Brand Monitoring	Domain-www.nainitalbank.co.in CXO-1	
1.3	Managed XDR	Number of end points (1400)	
1.4	AD Security	Number of users (1000)	
1.5	Resource Onsite*	Onsite at Haldwani (1L1)	
		Onsite at Haldwani (1L2)	
2	Incident Response	30 days	
TOTAL (excluding GST) for 3 Years			

*If the Bidder needs Device count for the EPS, Bank will execute NDA before sharing the Device details

C- Rate Discovery for Onsite Engineer

	Rate Discovery	Qty	Price excluding taxes - Yearly
1	Onsite Engineer -L1 resource		
2	Onsite Engineer -L2 resource		

Important Note: - Bidder should ensure to submit separate quotations for One (1) L1, Two (2) L1 & One (1) L1 & One (1) L2 for onsite Location.

This Price remain valid during the entire contract period of three years.

D-Rate Discovery for Incremental Devices / EPS during the contract period (for 3+2 Years)

#	Rate Discovery	EPS/ Device count	Price excluding taxes - Yearly
1	Managed SOC services for additional 1000 EPS over and above usages of Subscribed EPS	1000 EPS unit	
2	20 AD users and 100 XDR end points		

E-Rate Cart for Executive monitoring capability

#	Rate Discovery	Qty	Price excluding taxes
1	Single CXO		

19. Annexure O - Declaration for Undertaking of Information Security

(Bidder's Letter Head)

To,
The Chief Operating Officer
Nainital Bank Ltd
Head Office
Mallital, Nainital -263001 (Uttarakhand)

Dear Sir,

Subject: RFP # NTBL/ISC/SOC/2024/11/22 dated 06-11-2024 for "Request for proposal for engaging a Managed Security Service Provider for Security Operations Centre (SOC) Services with Managed, Detection and Response (MDR) Along with Brand Monitoring, Breach Investigation, AD Security and Threat Hunting Capabilities.

We hereby undertake that the proposed hardware/ software/firmware to be supplied will be free of malware, free of any bugs/vulnerabilities and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/modifications done) which may lead to any data leakage/compromise of the server/solution or any cyber security incident in future.

We also undertake that: -

a) The Solution and Software being offered, as part of the contract, does not contain Embedded Malicious code that would activate procedures to:

1. Inhibit the desires and designed function of the equipment.
2. Cause physical damage to the user or equipment during the exploitation.
3. Tap information resident or transient in the equipment/network.

b) The firm will be considered to be in breach of the procurement contract, in case physical damage, loss of information or infringements related to copyright and Intellectual Property Right (IPRs) are caused due to activation of any such malicious code in embedded software and any loss occurring due to the above may be recovered from the existing contracts.

I/WE declare that all the provisions of this RFP / Tender Document are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours faithfully,

(Signature of the Bidder)
Printed Name
Designation
Seal Date:
Business Address:

20. Annexure P: Non-Disclosure Agreement

(To be submitted by all Bidders for Managed Security Service Provider for Security Operations Centre (SOC) Services with Managed, Detection and Response (MDR) Along with Brand Monitoring, Breach Investigation, AD Security and Threat Hunting Capabilities for a period of 3 Years)

(TO BE STAMPED AS AN AGREEMENT AS APPLICABLE TO STATE OF UTTARAKHAND)
This NON-DISCLOSURE AGREEMENT **("NDA")** is made at Nainital this _____ day of _____ 2024
BY AND BETWEEN
THE NAINITAL BANK LTD, a public limited Banking Company incorporated under the Companies Act, 1956 (now the Companies Act, 2013) having its Registered Office at G.B. Pant Road, Nainital and its Head Office at Seven Oaks Building, Mallital, Nainital (CIN No. U65923UR1922PLC000234) (hereinafter referred to as the "**Bank**" which expression shall mean and include its legal representatives, successors-in-interest and permitted assigns) and represented herein by its authorized signatory, of the **ONE PART**.
AND
_____ a company within the meaning of Section 2(20) of the Indian Companies Act 2013, having its registered office at_____ ___, INDIA (hereinafter referred to as the "Bidder" which expression shall mean and include its legal representatives, successors-in-interest and permitted assigns) and represented herein by its authorized signatory, of the **OTHER PART**; Bank and Bidder are hereinafter individually referred to as the "Party" and collectively as the "Parties", as the context may require in this Agreement.

RECITALS

WHEREAS:
Bank pursuant to its working relationship which has been or may be established, with the Bidder, anticipate that it may have to disclose or deliver certain documents, components, parts, information, drawings, data, sketches, plans programs, specifications, techniques, processes, software, inventions and other materials, both written and oral, of a secret, confidential or proprietary nature, including without limitation any and all information relating to marketing, finance, forecasts, invention, research, design or development of information system and any supportive or incidental sub-systems, (collectively, "Proprietary Information"); and which may be accessible / available to the Bidder.
WHEREAS, Bank desires to ensure that the confidentiality of any Proprietary Information is maintained, during the tenure of the NDA (contract) and thereafter;
NOW, THEREFORE, in consideration of the foregoing premises, and the mutual covenants contained herein, both the parties intending to be legally bound, Bank and Bidder hereby agree as follows:

1-CONFIDENTIAL INFORMATION

1. All Bank's product and process details, documents, data, applications, software, systems, papers, statements and business / customer information which may be communicated to or come to the knowledge of the Bidder or its employees during the course of discharging their obligations shall be treated as absolutely confidential and the Bidder irrevocably agrees and undertakes and ensures that the Bidder and its employees shall keep the same secret and confidential and not disclose the same, in whole or in part to any third party without the prior written permission of Bank nor shall use or allow to be used any information other than as may be necessary for the due performance by the Bidder of its obligations.
2. The Bidder shall not make or retain any copies or record of any Confidential Information submitted by Bank other than as may be required for the performance of the Bidder.
3. The Bidder shall notify Bank promptly of any unauthorized or improper use or disclosure of the Confidential Information.
4. The Bidder shall return all the Confidential Information that is in its custody, upon termination / expiry of this Agreement. Also so far as it is practicable the Bidder shall immediately expunge any Confidential Information relating to the projects from any computer, word processor or other device in possession or in the custody and control by Bidder or its affiliates.
5. Bidder shall extent practicable, immediately furnish a certificate signed by its director or other responsible representative confirming that to the best of his/her knowledge, information and belief, having made all proper enquiries the requirements of this paragraph have been fully complied with.
6. The Bidder hereby unconditionally agrees and undertakes that it and its employees shall not disclose the terms and conditions of any oral or written information which may contain, hold or bear confidential information or disclose the information submitted by Bank under any other Agreement to any third part unless such disclosure is mandatorily required by law or if it is required necessarily to be disclosed to any other agency/subcontractor or the like for the purpose of performing any of its obligations under the contract.
7. Bidder shall not disclose the name of the Bank, or the existence, nature or substance of any agreement, relationship and/or negotiations between Bank and the Bidder, in any publicity material or other communications to any third parties without the prior permission of Bank.

8. However, the Confidential Information will not be limited to the information mentioned above but not include the following as Confidential Information:
    - Without breach of these presents, has already become or becomes and/or hereinafter will become part of the public domain;
    - Prior to the disclosure by Bank was known to or in the possession of the Bidder at the time of disclosure;
    - Was disclosed or parted with the prior consent of Bank;
    - Was acquired by the Bidder from any third party under the conditions such that it does not know or have reason to know that such third party acquired directly or indirectly from Bank.
9. The Bidder agrees to take all necessary action to protect the Confidential Information against misuse, loss, destruction, deletion and/or alteration. It shall neither misuse or permit misuse directly or indirectly, nor commercially exploit the Confidential Information for economic or other benefit.
10. In any dispute over whether information or matter is Proprietary Information or not mentioned herein, it shall be the burden of Bidder to show that such contested information or matter is not Proprietary Information within the meaning of this Agreement, and that it does not constitute violation under any laws for the time being enforce in India.

2-PROPRIETARY RIGHTS

Title to all documents, process details, any other information which is having intellectual property rights received by Bidder from Bank, including all Proprietary Information, shall remain at all times the sole property of Bank, and this Agreement shall not be construed to grant to Bidder any patents, licenses or similar rights to such property and Proprietary Information disclosed to Bidder hereunder.

3-INDEMNITY

3.1 The Bidder hereby agrees to indemnify and keep Bank indemnified safe and harmless at all times against all or any consequences arising out of any breach of this confidentiality undertaking by the Bidder and /or its employees and shall immediately reimburse and pay to Bank on demand all damages, loss, cost, expenses or any charges that Bank may sustain suffer, incur or pay in connection therewith.

3.2 The Bidder acknowledges that a breach of its obligations under this Agreement could cause irreparable harm to the Bank for which monetary damages may be difficult to ascertain or an inadequate remedy. The Bidder therefore agrees that the Bank will have the right, in addition to its other rights and remedies, to seek injunctive relief and damages for any violation of this Agreement.

3.3 In event, the Bank arrives to the conclusion that the bidder has disclosed the confidential information in breach of NDA, the Bank will appropriate the EMD deposited by the bidder along with the RFP apart from other available remedies of seeking compensation from the bidder.

4-TERMINATION AND SURVIVAL

4.1 The terms of this Agreement shall be for twelve months unless terminated by Bank with thirty days' prior written notice to Bidder, however, this Agreement's provisions will survive as to Confidential Information that is disclosed before termination.

4.2 Unless Bank otherwise agree in writing, Bidder duty to protect Confidential Information expires one year from termination / expiry of this Agreement, provided the information which is by its nature required to keep confidential or under any applicable laws required to protect forever such information shall remain confidential forever or until such time when the Bidder no longer has access to the Confidential Information or has returned or destroyed all Confidential Information having in its possession.

5-GOVERNING LAW AND JURISDICTION:

The provisions of this Agreement shall be governed by the laws of India. If any disputes or differences shall arise between the Parties hereto as to the interpretation or the performance of this Agreement the same shall be referred to sole arbitrator to be appointed by Bank. The arbitration proceeding shall be governed by the Arbitration and Conciliation Act 1996 and rules / amendments there under.

The place of Arbitration shall be at Nainital. The language of arbitration shall be English and the courts at Nainital shall have the exclusive jurisdiction to try any matters arising from this Agreement.

6-SEVERABILITY

If any provision of this Agreement is invalid or unenforceable, then such provision shall be construed and limited to the extent necessary, or severed if necessary, in order to eliminate such invalidity or unenforceability, and the other provisions of this Agreement shall not be affected thereby.

7-NO LIABILITY

Bidder understands and agrees that neither Bank nor any of its directors, officers, employees, agents, advisors or representatives (i) have made or make any representation or warranty, expressed or implied, as to the accuracy or completeness of the Confidential Information or (ii) shall have any liability whatsoever to Bidder or its Affiliates relating to or resulting from the use of the Confidential Information or any errors therein or omissions therefrom.

8-MISCELLANEOUS

8.1 No delay or omission by either party in exercising any rights under this Agreement will operate as a waiver of that or any other right. A waiver or consent given by either Party on any one occasion is effective only in that instance and will not be construed as a bar to or waiver of any right on any other occasion.

8.2 This Agreement is in addition to any prior written agreement between Bank and Bidder relating to the subject matter of this Agreement; in the event of any disparity or conflict between the provision of such agreements, the provision which is more protective of Proprietary Information shall control.

8.3 This Agreement may not be modified, in whole or in part, except by an agreement in writing signed by Bank and bidder.

IN WITNESS WHEREOF, the Parties hereto have set the hands of the respective authorized officials on the day and year first hereinabove written.

Signed by, for & on Behalf of the Nainital Bank Ltd through	Signed by, for & on Behalf of Bidder
Designation:	Designation:
In presence of	In presence of
Designation:	Designation:
Date: Place:	

---End of Document---