Tender No 1/2023/FBL/ISD

RFP for procurement of SIEM Solution and engaging an agency for Security Operations Center (SOC) services.

30 October 2023

The Federal Bank Ltd
Integrated Risk Management Department
Corporate Office
Federal Towers PB No 103,
Aluva-683101, Kerala, India
Email: isd@federalbank.co.in
Website: www.federalbank.co.in

Table of Contents

Disclaimer 5
1. About Federal Bank 6
2. Purpose 6
3. Scope of Work 7
3.1 Security Incident & Event Management (SIEM) 7
3.1.1 SIEM tool and related components 7
3.1.2 Log collection 8
3.1.3 Log aggregation and normalization 8
3.1.4 Log archival 9
3.1.5 Log correlation 9
3.1.6 Alert generation 9
3.1.7 Event viewer/dashboard/reports/incident management 9
3.1.8 Incident management 10
3.1.9 Integration with in-scope monitored devices. 10
3.1.10 Development of connectors for customized applications/ devices 10
3.2 Resources 11
3.2.1 Implementation 11
3.2.2 Administration 12
3.2.3 SOC Analysts 12
3.3 Training 13
4. Warranty and Support 14
5. Annual Maintenance Contract (AMC) 14
6. ESCROW ARRANGEMENT FOR SOFTWARE 15
7. Subcontracting 15
8. Delivery and installation schedule 15
9. Expectations From OEM 17
10. Expectations From Bidders 18
11. Service Level Agreement (SLA) 19
11.1 Implementation 19
11.2 Operations 20
12. Amendment Of the RFP Document 23
13. Requests For Proposal 24

14. Minimum Eligibility Criteria 25
15. Instruction to Bidders 26
15.1 Clarification of bids 26
15.2 Amendment to the bidding document 26
15.3 Language of bid 27
15.4 Documents comprising the bid 27
15.5 Signing, sealing and marking of bids 28
16. Bid currency 29
17. Period of validity of bids 29
18. Deadline for submission of bids 29
19. Late bids 30
20. Modification and/ or withdrawal of bids: 30
21. Opening of bids by the Bank 30
22. Evaluation Methodology 30
22.1 Preliminary examination 30
22.2 Technical evaluation 31
22.3 Commercial evaluation 32
22.4 Arithmetic errors correction 32
22.5 No commitment to accept the lowest or any offer 32
22.6 Conditional bids 33
22.7 Contacting the Bank 33
22.8 Issuance of contract 33
23. General Terms and Conditions 33
23.1 Term of implementation 33
23.2 Adherence to terms and conditions 34
23.3 Termination 34
23.4 Issuance of purchase order 34
23.5 Software/Hardware requirements 34
23.6 Professionalism 35
23.7 Adherence to safety procedures, rules regulations and restriction 35
23.8 Expenses 35
23.9 Payment terms 36
23.9.1 Payments of hardware and software items 36

23.9.2 Payment for the SOC Operations....36
23.9.3 Payment for the other services....36
23.10 Contract performance guarantee....36
23.11 Single point of contact....37
23.12 Applicable law and jurisdiction of court....37
23.13 Liquidated damages (LD)....37
23.14 Force majeure....38
23.15 Authorized signatory....38
23.16 Due Diligence....38
23.17 Indemnity....38
23.18 Agreements....39
23.19 Non Payment of agreed price....39
23.20 Assignment....39
23.21 Confidentiality....39
23.22 Use Of Name/Logo of the Bank....40
23.23 Non-solicitation....40
23.24 No employer-employee relationship....40
23.25 Subcontracting....40
23.26 Cancellation of contract and compensation....41
23.27 Dispute resolution....41
23.28 Ownership of documents....42
Annexure A: Bid Forwarding Letter (Submitted on Bidder's letter head)....43
Annexure B: Minimum Eligibility Criteria....44
Annexure C: Technical Bid Format....47
Annexure D: Technical Specification....49
Annexure E: Profile of onsite manpower at Cochin / Aluva....82
Annexure F: Commercial Bid Format....88
Annexure G: Compliance Certificate (On company's letterhead)....91
Annexure H: Manufacturer Authorization Format (On OEM's letter head)....93
Annexure I: Undertaking of authenticity (to be signed by authority not lower than the Company Secretary of the Bidder)....94
Annexure J: Power of Attorney (Executed on a non-judicial stamp paper)....96
Annexure K: MUTUAL NON-DISCLOSURE AGREEMENT (On a Stamp paper)....98

Disclaimer

The information contained in this Request for Proposal (RFP) document or formation provided subsequently to bidder(s) or applicants whether verbally or in documentary form by or on behalf of Federal Bank Limited ("Bank"), is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP document is not an agreement and is not an offer by Bank. This RFP is to invite proposals from the applicants who are qualified to submit the bids ("bidders"). The purpose of this RFP is to provide the bidder(s) with information to assist them in formulation of their proposals. This RFP does not claim to contain all the information each bidder may require. Each bidder may conduct its own independent investigations and analysis and is free to check the accuracy, reliability and completeness of the information in this RFP. Bank makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. The information contained in the RFP document is selective and is subject to updation, expansion, revision and amendment. It does not purport to contain all the information that a Bidder may require. Bank does not undertake to provide any Bidder with access to any additional information or to update the information in the RFP document or to correct any inaccuracies therein, which may become apparent. Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP. Bank reserves the right of discretion to change, modify, add to or alter any or all of the provisions of this RFP and/or the bidding process, without assigning any reasons whatsoever. Such change will be intimated to all Bidders. Any information contained in this document will be superseded by any later written information on the same subject made available to all recipients by Bank.

Bank reserves the right to reject any or all proposals received in response to this RFP document at any stage without assigning any reason whatsoever. The decision of Bank shall be final, conclusive and binding on all the parties

.

1. About Federal Bank

The Federal Bank Limited ("Federal Bank") is a Banking company incorporated in India under Companies Act 1956 and having its registered office at "Federal Towers", Bank Junction, Aluva 683101, Kerala, India and having branches / offices all over India. Federal Bank is also a scheduled commercial Bank as notified by the Reserve Bank of India under the Reserve Bank of India Act, 1934 which categorizes Federal Bank under the group of "private sector Banks". Federal Bank has engaged in wholesale Banking, retail Banking, treasury operations and other Banking operations.

2. Purpose

The Bank already has a captive Security Operations Centre (SOC) with SIEM and Incident Management tool deployed. Considering the increased threats from emerging technologies like AI/ML, block chain, crypto-currencies, bots etc and regulatory requirements, Bank has decided to setup state of the art NextGen Cyber Security Operations Centre which can process logs / data at extremely high concurrency operating on 24x7x365 basis. The proposed security monitoring technologies should support deep learning analytics powered by Artificial Intelligence / Machine learning (AI/ML) and ingested with threat intelligence to proactively monitor, report, manage and predict cyber-attacks (internal and external).

Bank proposes to implement and maintain NextGen Security Operation Centre (SOC) for its Information Technology setup comprising critical locations such as DC, DR, Cloud, Near DR and other IT locations which may come up in future. The Bank intends to issue this bid document to the bidders to participate in the competitive bidding for procurement, implementation, and maintenance of SIEM Solution, Security Operation Centre and other services on captive SOC model.

Bank has state of the art Data Center at Aluva (Own Premises) with DR site at Bengaluru and a Near DR in Aluva. All the applications are hosted at DC, DR, Near DR and multiple Cloud. The selected Bidder shall deploy the SIEM Solutions at DC and DR in HA mode and should deliver SOC services including but not limited to performance monitoring, performance tuning, optimization, and maintenance of SIEM & security tools, also SIEM log backup, troubleshooting, security monitoring, security product management and administration.

The Bidder should note that:

a) The purpose behind issuing this RFP is to invite pre-qualification, technical and commercial bids

from the eligible bidders and selection of bidder (s)..

b) Bidder should provide proposal for procurement and support of SIEM solutions, Administration of SIEM solution and SOC operations.

c) Successful Bidder and OEM should provide a SPOC to coordinate the project initially which includes implementation period and thereafter stabilization period of 3 months.

d) The technical specifications specified in Annexure-D are the minimum specifications for the SIEM solutions.

e) The selection process consists of the following three phases:

1) Pre-Qualification/Minimum Eligibility Criteria

2) Technical Evaluation

3) Commercial Evaluation

3. Scope of Work

Following is a broad scope of work.

3.1 Security Incident & Event Management (SIEM)

3.1.1 SIEM tool and related components

- Bidder should quote a SIEM Sustained EPS / Volume 50,000 EPS or equivalent TB/day whichever is higher in DC & DR separately from day one. The solution, including hardware, should be scalable to support 1 lakh EPS or equivalent TB/day whichever is higher in DC & DR separately during contract period.
- The solution should have a High Availability feature built in. There should be an automated switch over to secondary collectors/Agent server in case of failure on the primary collector/Agent Server.
- The SIEM tool can be either software based, or appliance based. In case of Software based SIEM solutions, bidder shall bundle necessary hardware. OEM must certify that the hardware proposed by the bidder is sufficient to cater to the RFP requirement. Hardware proposed in both cases should be rack mountable with dual power supply and should comply with Data Center Standards.
- Onsite implementation of the SIEM solution, Integration of phase I event sources, creation of use cases/reports/dashboards is to be done directly by OEM and this includes implementation of a similar setup at both DC and DR.

- Log should be retained for a period of 6 months online, 1 year offline and shall be available for querying. Logs to be retained for additional 7 years in network storage.
- The bidder should provide 24X7 monitoring & Security Analysis of the infrastructure through SIEM solution.
- The bidder should patch the SIEM systems and related components as and when required in case new updates are available and new vulnerabilities are identified. Security updates/Vulnerabilities should be patched as per Bank's patch management policy.
- The bidder should administer the SIEM tool and ensure that an uptime of 99.95% is available for the SIEM tool and related components.
- The bidder should ensure that End of Life and End of Security patch Support of the SIEM tool and related components is available for next seven years.
- Technologies proposed to be deployed by bidder and OEMs should leverage self-learning, analytics models powered by Artificial Intelligence / Machine Learning (AI/ML) and should be capable of handling extremely high IOPS without latency.

3.1.2 Log collection

Logs from all the in-scope devices located at the geographically dispersed location should be collected. Bidder should develop the baseline for the level of logs to be enabled from different components of IT infrastructure assets. The log baseline should be in line with global best practices. In case the systems/applications are writing logs to the local hard disks, solution should be capable to pull the logs from these devices through secure transfer. Only in case where remote log collection is not feasible, Bidder should install agent on the servers and applications for collection of logs. Raw logs should be made available in case of legal requirement. The detailed requirements are mentioned in Annexure – D – Log Collection and Retention.

3.1.3 Log aggregation and normalization

Logs collected from all the devices should be aggregated as per the user configured parameters. Logs from multiple disparate sources should be normalized in a common format for event analysis and correlation.

3.1.4 Log archival

Logs collected from all the devices should be stored in a non-tamperable format on the archival device in the compressed form. Collection of Logs and storage should comply with the Regulatory requirement and should maintain a chain of custody to provide the same in the court of law, in case the need arises.

Retrieval of archived logs should not require any proprietary tools/protocol and should be retrievable using open standards/protocols or else the retrieval tool should be provided to the Bank at no extra cost.

Storage of logs should be encrypted using highest level encryption such as AES256 or equivalent or above and compressed on a minimum of 1:8 or more.

3.1.5 Log correlation.

Collected Logs should be correlated according to various predefined criteria for generation of alert and identification of the incident. The correlation rules should be predefined and also user configurable. Correlation rules should be customized by bidder on regular basis to reduce false positives. False negatives will not be permitted, in case of detection of any such incident, correlation rules must be customized immediately to capture such incidents.

For correlation and report generation purpose, past -6- months log data should be available online.

3.1.6 Alert generation

Solution should be capable to generate alerts, register and send the same through message formats like SMTP, SMS, Syslog, SNMP, instant messengers as per user configurable parameters.

3.1.7 Event viewer/dashboard/reports/incident management

SIEM Solution should provide web based facility to view security events and security posture of the Bank's Network and register incidents for all event sources. Solution should have drill down capability to view deep inside the attack and analyze the attack pattern.

Dashboard should have filtering capability to view events based on various criteria like geographical

location, device type, attack type etc. Dashboard should have Role based as well as Discretionary access control facility to restrict access to incidents based on user security clearance level. Solution should provide various reports based on user configurable parameters and standard compliance reports like PCI-DSS, ISO27001, SOX, IT Act and regulatory reports.

Selected Bidder will customize incident management/dashboard/reports for the Bank and will modify the same as per the changing requirement of the Bank.

3.1.8 Incident management

Solution should be able to register any security event and generate trouble ticket. Solution should provide complete life cycle management (work flow) of trouble tickets from incident generation till closure of the incident. Solution should provide the logging facility to different levels of users to monitor and manage the incidents generated for closure of the same as per the defined workflow. Incident management should include escalation as per the escalation matrix. Solution should be able to send the incident report in various forms like e-mail, SMS, instant messages etc. Solution shall have the in-built capability to map the incidents to standard frameworks such as MITRE ATT&CK framework, Cyber kill chain, etc.

3.1.9 Integration with in-scope monitored devices.

Bidder in coordination with OEM should integrate the event sources to SIEM, as per Bank's requirement. The Bidder is responsible for integrating all in scope devices with the SIEM solution for log monitoring and correlation, and on ongoing basis.

3.1.10 Development of connectors for customized applications/ devices

Connectors for all the standard applications and devices should be readily available in the collector and Log management devices, connector for in-house/custom built applications should be developed by Bidder in coordination with OEM. It is the responsibility of the Bidder to develop connector applications for the custom-built applications specifically developed for Bank.

3.2 Resources

Resources shall be provided for administration & maintenance of the tools and for SOC Operations.

It is mandatory for the Bidder to provide the dedicated onsite resources having the minimum detailed skill sets and experience as per Annexure E. All the resources from Bidder and OEM should be OEM certified. Evidence on educational qualifications and certifications should be submitted at the time of reporting at the Bank failing which, the Bank will reject the resource. Bank reserves the right to reject any resource profile without any reason. Refer Resource requirement details as per Annexure E

The bidder SOC team should regularly track and advise the Bank about new global security threats and vulnerabilities. The advisories should be customized to suit the Bank's security infrastructure. Bidder should advise the Bank for upgrades /changes in the security infrastructure of the Bank against evolving threats and responsibilities.

For Reporting and Timings, the following should be ensured.

- The onsite team should report to Bank personnel / Bank authorized representative.
- The Team should operate from the Bank's premises during the hours assigned to engineers as per the shifts.
- In case of exigencies even during off business hours / Bank holidays, the resources may be required to be present onsite.
- A replacement must be given in case the resource proceeds for leave.
- The Bidder personnel deployed in the Bank premises shall comply with the Bank's Information Security Requirements.

For calculations, Per Man day charges (for the purpose of deduction on account of absence) = Charges per man year/(12X Number of days in a month)

3.2.1 Implementation

Onsite implementation of the SIEM solution and its components is to be done by the OEM directly. OEM engineer shall be present at Bank's premise till completion of the entire phase I implementation. Competent bidder resource shall be present during the entire implementation phase together with the OEM resource and will be responsible for remaining integrations as detailed in scope of work, in coordination with OEM.

3.2.2 Administration

SOC administration team should be present from the date of phase I implementation and coordinate with Bank's team for the implementation activities.

All the resources provided for administration of the solution should be OEM trained and certified. Certificates should be submitted at the time of reporting. Refer Resource requirement details as per Annexure E.

Manpower Support work schedule.

S.No.	Job Profile	No of Shifts per day	Working days
1	SIEM Administrator	2	Banks working days and whenever required by the Bank during any activity

Shift: 8 Hours a day.

In case of exigencies, the Administrator should be available 24*7 as well.

In the absence of the resource, suitable replacement is to be provided on immediate basis. In case of absolute absence (when no replacement is provided), no payment will be done and in addition to that penalty would be deducted @0.5% of the monthly operations cost, for each day, up to a maximum of 10% of the monthly operations cost.

3.2.3 SOC Analysts

SOC Analyst has to perform all the functionalities in SOC not limited to handling the incidents and alerts created at the SOC. The scope of activity includes the proposed SIEM solution and the other monitoring solutions implemented by the Bank. The detailed description of Job profile and the qualifications is given in Annexure E.

Manpower Support work schedule.

S.No.	Job Profile	No of Shifts per day	Working days
1	L1	3	365
2	L2	3	365

3	L3	1	10 am to 6 pm on Banks working days and whenever required by the Bank during any activity.

Shift window considered above is 8 Hours a day.

In case of exigencies, L3 should be available on 24*7 as well. In the absence of L3, senior L2 resource shall be available.

In the absence of the engineer during shift or less no. of support engineers (as asked by the Bank) during any point of time of contract, suitable replacement is to be provided on immediate basis. In case of absolute absence (when no replacement is provided),

- If a lower-level person does not report on duty, then higher level person will be expected to perform the job of lower level person and payment will be made as per the payment structure of lower level person only.
- In the absence of the L3 engineer, suitable replacement is to be provided on immediate basis. In case of absolute absence (when no replacement is provided), no payment will be done and in addition to that penalty would be deducted @0.5% of the monthly operations cost, for each day, up to a maximum of 10% of the monthly operations cost.

3.3 Training

Selected bidder shall provide the training to the Bank's personnel as described below:

i. The training should include the architecture, hardware, software, administration, integration, and customization, use case management, policy installation, troubleshooting, reporting and other aspects of the solution.

ii. SIEM Training - This faculty should be solution certified up to advance level and should provide courseware with adequate lab facility as well. The training should be provided by the OEM employee and should be of minimum five days, 8 hours a day. Pre implementation training must be provided before project implementation and post implementation training

must be provided after successful implementation. At the end of training, participants shall be given certificate of successful completion by the OEM. Bidder should submit detailed course content and provisional agenda along with the Bid.

iii. Refresher training - Post acceptance test, selected bidder shall conduct more refresher trainings for the SOC team (Bank personnel and Outsourced) on quarterly basis. The participants of these programs may or may not be same. The course duration will be of 1 day.

iv. Bidder shall ensure that regular cyber security/OEM trainings and knowledge sharing sessions are provided to resources deployed at Bank's premises. Training shall be done at minimum of half yearly basis and certificates are to be shared with Bank.

4. Warranty and Support

All the hardware, software products supplied should carry warranty and on-site, comprehensive, back-to-back support from Original Equipment Manufacturer (OEM) for a period of 3 years from the completion of phase I implementation. The warranty also includes all software subscriptions (critical hot fixes, service packs, and major upgrades).

OEM shall replace the failed hardware within 24hrs from the time call is lodged. The penalties for any non-compliances is defined under section SOC operations in SLA.

Bank shall not return defective/used storage component to OEM when a replacement has been sent under a parts exchange request and Return Material Authorization.

5. Annual Maintenance Contract (AMC)

The AMC shall be:

- On-site, comprehensive, back-to-back from OEM for all hardware and software products as a part of RFP for a period of 4 years from the date of expiry of warranty.
- Software updates and upgrades at no cost to the Bank
- L2 and above support from OEM

- Replacement of failed hardware within 24hrs from the time call is lodged. The penalties for any non-compliances defined under Section SLA
- Comprehensive on-site support from bidder for day to day operational issues as and when arises.

6. ESCROW ARRANGEMENT FOR SOFTWARE

The Bidder should agree for Escrow arrangement in following manner:

- The bidder shall provide, at its own cost, escrow mechanism for the software used (all components) for rendering the services in order to protect the Bank's interest in an unexpected eventuality. The software should be periodically tested and latest version to be kept under Escrow.

-For the third-party licensed software used by the bidder for rendering the required services, the Bidder should have an Escrow agreement with the licenser for the software used (all components), in order to protect the Bank's interest in an eventual situation.

7. Subcontracting

The selected Bidder shall not subcontract or permit anyone other than its personnel or the OEM supplier to perform any of the work, service or other performance required of the Bidder under the contract without the prior written consent of the Bank.

8. Delivery and installation schedule

a) The Bidder should deliver and implement the hardware and software under the scope within 2 months from the date of purchase order. Training to the Identified users must be provided prior to supplying the solutions to the Bank.

b) Delivery of the goods shall be made by the Supplier in accordance with the terms of the purchase contract. The bidder should take responsibility of the goods till it reaches the delivery destination as informed by Bank, transport to such place of destination in India, including insurance and storage, as specified in the contract, shall be arranged by the supplier. Bidder shall arrange the road permits, or any other document wherever required. Any letter required for this will be given by the Bank.

c) The Bank will not be in a position to supply Form-C or Form-D and bidder will have to arrange for Form 31 or 32 or any other road permit, if required, on behalf of Bank

d) SOC operations team should be operational once the implementation of SIEM solution is completed or within two months from the date of purchase order whichever is earlier.

e) Integration of the devices for collection of logs will be done in a phased manners as given below.

Phase 1: All servers associated with Critical Applications , internet facing applications, payment applications, network and security devices including but not limited to WAF, Firewall, IPS, Router, Switches at DC & DR. This should be completed within three (3) months of issuance of the purchase order. Warrantee will start after successful completion of phase 1

Phase 2: All standard application and remaining devices/servers within 4 months of issuance of the Purchase Order.

Phase 3: All custom-built applications involving development of connection application should be completed within 6 months of issuance of the Purchase Order.

Installation will be treated as incomplete in one/all of the following situations:

- Non-delivery of any hardware or other components viz. accessories, documentation, software/ drivers media mentioned in the order.
- Non-delivery of supporting documentation.
- Delivery, but no installation of the components and/or software.
- System operational, but unsatisfactory to the Bank.

f) After completion of installation the bidder should obtain sign-off on the Installation-cum-Acceptance certificate from the Bank official at respective locations. Bank will carry out acceptance of hardware as per acceptance test plan.

g) The Bank will consider the inability of the Bidder to deliver or install the equipment within the specified time limit, as a breach of contract and would entail the payment of Liquidation Damages on the part of the Bidder.

h) The liquidation damages represent an estimate of the loss or damage that the Bank may have suffered due to delay in performance of the obligations (relating to delivery, installation, operationalization, implementation, training, acceptance, warranty, maintenance etc. of the deliverables) by the Bidder.

i) The Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum as specified in General Terms and Conditions.

j) Products shall be supplied in a ready to use condition in the latest stable firmware version along with all Cables, Connectors, Software Drivers, Manuals and Media etc.

9. Expectations From OEM.

a) The OEM should be committed to the success of the project during actual implementation by being involved in Solution design of the project till its completion.

b) The OEMs should do the overall design, architecture, implementation, post implementation audit, yearly review etc.

c) The OEMs must give the certificate to Bank post implementation, confirming the implementation of their products with best industry practices and the standards and no zero-day threats or malware in the installed device or appliance.

d) The following are the tentative expectations with respect to OEM involvement during the contract period, however Bank reserves the right to change the scope:

- Validation of solution design and architecture.
- Implementation of the SIEM solution and its components.
- OEM to integrate the event sources related to critical applications and create parsers/data models for logs received and generate use cases required by Bank.
- Mandatory Yearly health check-up and review of implemented solution by the Bidder. Bank can further ask to review the implemented setup at any point of time during contract.
- OEM should release the parsers immediately after upgradation/change in version of any application/Operating system etc.
- OEM shall release updated integration guides within 30 days of upgradation of any supported/unsupported applications/databases/devices.

e) In case the bidder is not able to support, then the OEM should directly or through another Security Integrator get the solution supported to the satisfactory level of Bank as per RFP terms & conditions.

f) Bidder is responsible to arranging/conducting yearly review from respective OEM's and payments will be processed after submitting the OEM's reports to Bank.

10. Expectations From Bidders

g) Bidder is expected to examine all instructions, forms, terms and specifications in this RFP and study the RFP document carefully. Bid shall be deemed to have been submitted after careful study and examination of this RFP with full understanding of its implications.

h) The bid should be precise, complete and in the prescribed format as per the requirement of this RFP.

i) Failure to furnish all information required by this RFP or submission of a Bid not responsive to this RFP in each and every respect will be at the Bidder's own risk and may result in rejection of the Bid and for which Bank shall not be held responsible.

j) The Bidder shall bear all costs and expenses associated with the preparation and submission of its Bid and Bank shall in no case be held responsible or liable for these costs, regardless of the conduct or outcome of the bidding process including cancellation or abandonment or annulment of the bidding process.

k) No binding legal relationship will exist between any of the respondents and Bank until execution of a contractual agreement.

l) The recipient must conduct its own investigation and analysis regarding any information contained in the RFP document and the meaning and impact of that information.

m) Each recipient should notify Bank of any error, omission, or discrepancy found in this RFP document.

n) A recipient will, by responding to Bank for the RFP, be deemed to have accepted the terms of this RFP.

11. Service Level Agreement (SLA)

The Bidder shall abide to the Service Level Agreements for SOC mentioned in the RFP as below:

11.1 Implementation

S. No	Service Area	Service Level	Penalty
1	Delivery of Hardware/Software	Delay in delivery and Installation of the hardware beyond 2 months from date of purchase order.	1% of the purchase order value per week after the stipulated time period, will be levied, subject to maximum of 10% in 4 months. In case the delay in delivery and installation exceeds more than 4 months, Bank reserves the right to cancel the order and no payment will be made to the Bidder.
2	Implementation	Delay in Implementation of SIEM tool and its components beyond 3 months from the date of purchase order	1% of the purchase order value per week after the stipulated time period, will be levied, subject to maximum of 10% in 6 months from purchase order. In case the delay in implementation exceeds more than 6 months, Bank reserves the right to cancel the order and no payment will be made to the Bidder.
3	Integration of event sources, parsers and creation of associated use cases	Phase I Completion	1% of the purchase order value per week after the stipulated time period will be levied, subject to maximum of 10%
		Phase II Completion	1% of the purchase order value per week after the stipulated time period will be levied, subject to maximum of 10%
		Phase III Completion	1% of the purchase order value per week after the stipulated time period will be levied, subject to maximum of 10%

Penalty as in 1, 2, 3a, 3b, 3c can be levied simultaneously. Maximum deducted penalty of one type will not affect any other type of penalty i.e. All the three types of penalties can be levied up to their maximum limit simultaneously. Maximum penalty will deduct 15 % of purchase order value.

11.2 Operations

S. No	Service Area	Service Level	Penalty
1	Device (Hardware/Software) component Failure	Problem should be resolved within 24 hours	Nil for first failure and 10% of monthly SOC operations charges for each repeat failure.
		Problem resolved between 24 to 48 hours.	5% of monthly SOC operations charges for 1st failure and 10% for each repeat failure.
		Problem resolved between 48 to 72 hours.	10% of monthly SOC operations charges for 1st failure and 20% for each repeat failure.
		Problem resolved between 3 days to 5 days.	20% of monthly SOC operations charges for 1st failure and 40% for each repeat failure.
		Problem resolved between 5 days to 10 days.	50% of monthly SOC operations charges for 1st failure and 100% for each repeat failure.
		Problem resolved beyond 10 days.	100% of monthly SOC operations charges.
2	Set of Devices (Hardware/Software) component failure leading to the complete disruption of the objective performed by the said devices. (Both DC and DR down at the same time)		10% of monthly SOC operations charges on each occasion. 100% of monthly SOC operations charges if problem not resolved within 48 Hours.
3	Solution Uptime. (Individual systems at DC / DR)	Uptime % calculated on monthly basis	
		99.95 % and above	NA
		99% to 99.95%	5% of monthly SOC operations charges
		97% to 98.99%	8% of monthly SOC operations charges
		90% to 96.99%	15% of monthly SOC operations charges
		80% to 89.99%	30% of monthly SOC

S. No	Service Area	Service Level	Penalty
			operations charges
		70% to 79.99%	50% of monthly SOC operations charges
		Less than 70%	100% of monthly SOC operations charges
4	Incident Resolution	For the devices / solutions managed and administrated by the Bidder a. Critical incidents within 60 minutes of the event identification. b. High priority incidents within 90 minutes of the event identification. c. Medium priority incidents within 120 minutes of the event identification.	Critical Incidents 10% of monthly SOC operations charges Medium Priority Incidents: 5% of monthly SOC operations charges Low Priority/ Operational incidents need to be logged and maintained for reference. These need to be included in the daily reports
5	Monitoring& Log Analysis Services	24x7 monitoring of all in-scope devices Categorization of events into Critical, High, Medium and Low priority shall be carried out in consultation with the selected bidder during the contracting period. All Critical, High and Medium priority events should be logged as incident tickets and responded as per SLA Events along with action plan/ mitigation steps should be alerted to designated Bank personnel as per the below SLA: a. Critical events within 15 minutes of the event identification. b. High priority events within 30 minutes of the event identification.	Critical Events: - 15% of monthly SOC operations charges High Priority Events: - 10% of monthly SOC operations charges Medium Priority Events: - 5% of the monthly SOC operations charges Low Priority/ Operational Events need to be logged and maintained for reference. An incident ticket need not be raised for such incidents. However these need to be included in the daily reports.

S. No	Service Area	Service Level	Penalty
		c. Medium priority events within 60 minutes of the event identification.	
6	Reports and Dashboard	Daily Reports: Critical reports should be submitted at 10.am everyday Weekly Reports: By 10:00 AM, Monday Monthly Reports: 3rd working day of each month	1. Delay in reporting for daily report for more than 2 hours shall incur a penalty of 3% of monthly SOC operations charges. 2. Delay in reporting by more than 3 days for both weekly and monthly reports shall incur a penalty of 10% of monthly SOC operations charges.
7	Periodic Reviews	The bidder is expected to improve the operations on an on-going basis. The bidder 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 bidder is expected to conduct a monthly 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.	Monthly meeting to be conducted within 5th of each month with the details of the past month, during the operations phase. A delay of more than five days will incur a penalty of 1% of SOC operations cost for that quarter
8	Security Intelligence Services	Advisories within 12 hours of new global threats & vulnerabilities disclosures.	A delay of more than 24 hours will incur a penalty of 1% of SOC operations cost for that quarter
9	New Patches, Vulnerabilities and Configuration Issues.	New patches are applied within three months of them becoming generally available to all related technologies supplied by the Bidder. Critical and High Vulnerabilities are to be addressed within 30 days	A delay of more than Five days will incur a penalty of 1% of SOC operations cost per day for that quarter.

S. No	Service Area	Service Level	Penalty
		and Medium/Low vulnerabilities are to be addressed within 45/90 days.	
10	Data model/Parser creation/Log Collector	Data model /parsers/Log Collector for data ingestion for all the current data sources and new data sources with 7 business days.	A delay of more than stipulated timeline will incur a penalty of 1% of SOC operations cost per week.
11	Return Material Authorization	All faulty components shall be replaced within 2 days.	Any delay in RMA (return material authorization) will incur a penalty of 1% of SOC Operations cost per day.

1. For repeat failure, same or higher penalty will be charged depending upon the delay in rectification of the problem.
2. Solution uptime is to be maintained without any consideration of devices in HA mode. If a function (like log collection, log management, log correlation) at the primary site is down, the same should be shifted to DR site within the SLA parameters.
3. Penalty will be calculated on monthly basis. Please refer clause on penalty for other details such as overall cap on penalty.

The bidder should provide uninterrupted services for ensuring implementation and maintenance of the Security Operations Center as per the requirements of this tender. Inability of the bidder to either ensure deliverables as per specifications within defined timelines or to meet the service levels as specified in this RFP shall be treated as breach of contract and would invoke the penalty clause. Overall cap for penalties will be 20% of the purchase order. Thereafter, the contract may be cancelled.

12. Amendment Of the RFP Document

a) Bank reserves the right in its sole discretion of inclusion of any addendum to this entire Bid process. The Bidders shall not claim as a right for requiring Bank to do the aforesaid.

b) At any time before the deadline for submission of Bids / offers, Bank may, for any reason, whether at its own initiative or in response to a clarification requested by prospective Bidders, modify this RFP / Bid Document and all such modifications shall be binding on them.

c) All prospective Bidders who have received this RFP shall be notified about the amendment in writing vide e-mail or post, and all such amendments shall be binding on them.

d) If required in order to allow prospective Bidders reasonable time in which they need to take the amendment into account in preparing their Bids, Bank at its sole discretion reserves the rights to extend the deadline for the submission of Bids. In no circumstance, the deadline for

submission of Bids shall be extended beyond a period of 7 days. However, no request from the Bidder, shall be binding on Bank for the same. Bank's decision in this regard shall be final, conclusive and binding on all the Bidders.

e) Any attempt by the Bidders to visit or meet Top management officials of the Bank in connection with or incidental to the Bid process, shall be construed by the Bank as an unlawful attempt by the prospective Bidder, to influence the RFP/ Bid process and may invite disqualification from bidding. Only two authorized representatives of each bidder would be permitted to visit for submitting the RFP Document/ or when called by the Bank.

13. Requests For Proposal

a) Recipients are required to direct all communications related to this RFP, through the below nominated point of contact:

Contact: Maya Sashi
Position: VP & CISO of Federal Bank
Email: isd@federalbank.co.in
Address: Information Security Division,
Integrated Risk Management Department,
Federal Bank Ltd, Federal Towers,
Aluva - 683101
Kerala, India.

b) Bank may, in its absolute discretion, seek additional information or material from any of the Bidders after the RFP closes and all such information and material provided must be taken to form part of that Bidder's response.

c) Bidders should provide details of their contact person, telephone, email and full address(s) to ensure that replies to RFP could be conveyed promptly.

d) If Bank, in its absolute discretion, deems that the originator of the question will gain an advantage by a response to a question, then Bank reserves the right to communicate such response to all Bidders.

e) Bank may, in its absolute discretion, engage in discussion or negotiation with any Bidder (or simultaneously with more than one Bidder) after the RFP closes to improve or clarify any response.

f) Bank will notify all short-listed Bidders in writing or by mail as soon as possible about the outcome of their RFP. Bank is not obliged to provide any reasons for any such acceptance or rejection.

14. Minimum Eligibility Criteria

a) Should be either a Government Organization/PSU/PSE/ partnership firm or a limited Company under Indian Laws or /and an autonomous Institution approved by GOI/RBI promoted.

b) The bidder should be Original Equipment Manufacturer [OEM] or authorized partner of OEM.

c) In case of authorized partner of OEM the bidder should submit Manufacturer Authorization Form (MAF) as per format given in Annexure-H.

d) Bidder should be in the business of supply, installation, configuration, maintenance, and support of SIEM solutions and SOC operations for least five(5) years as on date.

e) The Bidder must have experience of implementing Security Operations Centre involving same SIEM tool in India in at least -5- institutions out of which at least -2- institution should be from the Banking industry with at least 1 lakh EPS or 3 TB per day in the last -3- years.

f) The Bidder should have been managing well established own Security Operations Centre (SOC) in India for the past -5- years and should have provided services to at least -2- clients from Banking Industry, involving monitoring of logs using a SIEM tool for at least -3- years.

g) The Bidder should have provided Services (Operations) for Captive SOC to at least - 1- institution for -1- year, on the same SIEM tool in India in the last -3- years.

h) The Bidder must have at least 15 employees who are OEM Certified professionals on same SIEM tool.

i) The OEM of SIEM tool should have their presence in India for the last -5- years as on 30/09/2023 with its own support centre.

j) The bidder should have a minimum average annual turnover of 5 crores over the last three financial years. The bidder should have profit [i.e., no cash loss] in 2 years out of the last 3 years.

k) The bidder must have a currently valid GST registration certificate and PAN number.

l) The Bidder/bidder should have its own support office(s) in either Kochi or Bangalore.

m) The Bidder should have all necessary licenses, permissions, consents, no objections, approvals as required under law for carrying out its business.

n) The firm should not be blacklisted / barred by Government of India or any regulatory body in India.

o) Proposed Product should be in the Leaders quadrant/category as per Gartner or Forrester report published for the last three consecutive years.

15. Instruction to Bidders

The Bidders are expected to examine all instructions, forms, terms and specifications in the bidding documents. Failure to furnish all information required by the bidding documents may result in the rejection of its bid and will be at the bidder's own risk.

15.1 Clarification of bids

a) The bidder or its official representative is invited to attend pre-bid meeting to be held on 08/11/2023 at 11:00 hours at the venue selected by the Bank. It would be the responsibility of the Bidders representatives (only two persons per Bidder) to be present at the venue of the meeting.

b) Clarification sought by bidder should be emailed latest by 06/11/2023, 17:00 hours. Bank has discretion to consider any other queries raised by the bidder's representative during the pre-bid meeting.

c) The text of the clarifications asked (without identifying the source of enquiry) and the response given by the Bank, together with amendment to the bidding document, if any, will be posted on the website latest by 10/11/2023. No individual clarifications will be sent to the bidders. It would be responsibility of the bidder to check the website before final submission of bids.

15.2 Amendment to the bidding document

a) At any time prior to the date of submission of Bids, the Bank, for any reason, may modify the Bidding Document, by amendment. The amendment will be posted on Banks website www.federalbank.co.in

b) All Bidders must ensure that such clarifications have been considered by them before submitting the bid. Bank will not have any responsibility in case some omission is done by any bidder.

c) In order to allow prospective Bidders reasonable time in which to take the amendment into account in preparing their Bids, the Bank, at its discretion, may extend the deadline for the submission of Bids.

15.3 Language of bid

The bid prepared by the Bidders as well as all correspondence and documents relating to the Bid exchanged by the Bidder and the Bank and supporting documents and printed literature shall be written in English.

15.4 Documents comprising the bid

The bid shall consist of Pre-qualification/ minimum eligibility criteria, technical bid and commercial bid.

a) Documents comprising the Pre-qualifications-cum-Technical Bid should be:

- Bid Forwarding Letter as per Annexure-A.
- Documentary evidence establishing that the Bidder is eligible to Bid and is qualified to perform the contract i.e., Pre-Qualification Criteria / minimum eligibility criteria as per Annexure-B.
- Technical Bid Format as per Annexure-C
- Technical Specification as per Annexure-D.
- Profile of onsite manpower as per Annexure – E
- Masked (blank) commercial Bid without indicating the price should be submitted as per Annexure F.
- Compliance Certificate (on Company's Letter Head) as per Annexure G
- MAF(on OEM Letter Head) as per Annexure-H
- Undertaking of authenticity as per Annexure-I
- Power of Attorney for authorized signatory as per Annexure-J
- Mutual NDA on a stamp paper as per Annexure K
- Data sheets/printed literature of all the network hardware items being quoted.

b) Documents comprising the Commercial Bid should be:

- Commercial bid as per Annexure-F

15.5 Signing, sealing and marking of bids

The Bid shall be typed or written in indelible ink and shall be signed by the Bidder or a person or persons duly authorized to bind the Bidder to the Contract. Power of Attorney of the person authorized to sign the bid as per format given in Annexure-J is to be submitted. The Bidder shall seal the bids in non-window envelopes containing the documents as under:

a) First envelope (Superscripting "Tender No 1/2023/FBL/ISD – Prequalification/ Technical Bid"):

- Bid Forwarding Letter.
- Documentary evidence establishing that the Bidder is eligible to Bid and is qualified to perform the contract i.e., Pre-Qualification Criteria / minimum eligibility criteria.
- Technical Bid Format.
- Technical Specification.
- Profile of onsite manpower.
- Masked (blank) commercial Bid without indicating the price should be submitted.
- Compliance Certificate (on Company's Letter Head).
- MAF (on OEM Letter Head).
- Undertaking of authenticity.
- Power of Attorney for authorized signatory.
- Mutual NDA on a stamp paper.
- Data sheets/printed literature of all the network hardware items being quoted

Note: Under no circumstances the Commercial Bid should be kept in Technical Bid covers. The placement of Commercial Bid in Pre-qualification / Technical Bid covers will make bid liable for rejection.

b) Second Envelope (Superscripting "Tender No 1/2023/FBL/ISD - Commercial Bid"):

- Commercial bid

On the cover of each envelop name and address of bidder along with contact number should be clearly indicated. The envelope(s) shall be addressed to the Bank at the address given below:

The VP & CISO
Information Security Division
Integrated Risk Management Department,
Federal Bank Ltd, Federal Towers,
Aluva - 683101
Kerala, India.

If the envelop(s) are not sealed and marked as indicated above, the Bank will assume no responsibility for the Bid's misplacement or its premature opening.

16. Bid currency

Bids should be quoted in Indian Rupee only.

17. Period of validity of bids

a) Prices and other terms offered by Bidders must be firm for an acceptance period of 60 days from date of closure of this RFP.
b) In exceptional circumstances the Bank may solicit the Bidders consent to an extension of the period of validity. The request and response thereto shall be made in writing. The Bid security provided shall also be extended.
c) Bank, however, reserves the right to call for fresh quotes at any time during the period, if considered necessary.

18. Deadline for submission of bids

a) The bids must be received by the Bank at the specified address not later than 23/11//2023, 17:00 hours.
b) In the event of the specified date for the submission of bids, being declared a holiday for the Bank, the bids will be received up to the appointed time on the next working day.
c) The Bank may, at its discretion, extend the deadline for submission of Bids by amending the Bid Documents, in which case, all rights and obligations of the Bank and Bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

19. Late bids

Any bid received by the Bank after the deadline for submission of bids prescribed by the Bank will be rejected.

20. Modification and/ or withdrawal of bids:

a) The Bidder may modify or withdraw its bid after the bid's submission, provided that written notice of the modification including substitution or withdrawal of the bids is received by the Bank, prior to the deadline prescribed for submission of bids.

b) The Bidder modification or withdrawal notice shall be prepared, sealed, marked and dispatched.

c) No bid may be modified or withdrawn after the deadline for submission of bids.

d) Bank has the right to reject any or all bids received without assigning any reason whatsoever. Bank shall not be responsible for non-receipt / non-delivery of the bid documents due to any reason whatsoever.

21. Opening of bids by the Bank

a) On the scheduled date and time, bids will be opened by the Bank Committee.

b) No bid shall be rejected at the time of bid opening.

c) Bids that are not opened at Bid opening shall not be considered for further evaluation, irrespective of the circumstances.

22. Evaluation Methodology

22.1 Preliminary examination

a) The Bank will examine the Bids to determine whether they are complete, the documents have been properly signed; supporting papers/documents attached and the bids are generally in order.

b) The Bank may, at its sole discretion, waive any minor infirmity, nonconformity or irregularity in a Bid which does not constitute a material deviation, provided such a waiver does not prejudice or affect the relative ranking of any Bidder.

c) Prior to the detailed evaluation, the Bank will determine the substantial responsiveness of

each Bid to the Bidding document. For purposes of these Clauses, a substantially responsive Bid is one, which conforms to all the terms and conditions of the Bidding Document without material deviations. Deviations from or objections or reservations to critical provisions, such as those concerning Bid security, performance security, qualification criteria, insurance, Force Majeure etc. will be deemed to be a material deviation. The Bank's determination of a Bid's responsiveness is to be based on the contents of the Bid itself, without recourse to extrinsic evidence. The Bank would also evaluate the Bids on technical and functional parameters including possible visit to inspect live site(s) of the bidder/OEM, witness demos, bidders/OEM presentation, verify functionalities /response times etc.

d) If a Bid is not substantially responsive, it will be rejected by the Bank and may not subsequently be made responsive by the Bidder by correction of the nonconformity.

e) The Bidder is expected to examine all instructions, forms, terms and specification in the Bidding Document. Failure to furnish all information required by the Bidding Document or to submit a Bid not substantially responsive to the Bidding Document in every respect will be at the Bidder's risk and may result in the rejection of its Bid.

f) The bidder should satisfy the pre-qualification criteria as specified in the tender.

22.2 Technical evaluation

a) Pursuant to the evaluation of pre-qualification/ minimum eligibility criterion mentioned above, bidders will be short-listed for technical evaluation. Technical evaluation will be carried out only for the bidders who succeed the pre-qualification criterion.

b) Bank will review the technical bids of the short-listed bidders [who qualify the minimum eligibility criteria] to determine whether the technical bids are substantially responsive. Bids those are not substantially responsive are liable to be disqualified at Bank’s discretion.

c) During Technical evaluation, the Bank, at its discretion can ask the bidder/OEM for the demonstration of all or some components/ features and components of the hardware items quoted by them. However, Bank will not pay/ reimburse any expenditure incurred by the Bidder for arranging the demonstration.

d) Bank may waive off any minor infirmity or nonconformity or irregularity in a bid, which does not constitute a material deviation, provided such a waiving, does not prejudice or effect the relative ranking of any bidder.

e) Technical evaluation would be carried out and all bidders who qualify the technical evaluation will be short listed for commercial evaluation.

22.3 Commercial evaluation

a) All the bidders who qualify in Technical evaluation as per the criteria mentioned above would be shortlisted for commercial evaluation.

b) Bank will award the contract to the successful bidder(s) whose bid has been determined to be substantially responsive.

c) Bank shall however not bind itself to accept the lowest bid or any bid and reserves the right to accept any bid, wholly or in part.

22.4 Arithmetic errors correction

Arithmetic errors, if any, in the price break-up format will be rectified on the following basis:

a) If there is discrepancy between the unit price and the total price, which is obtained by multiplying the unit price with quantity, the unit price shall prevail and the total price shall be corrected unless it is a lower figure. If the supplier does not accept the correction of errors, its bid will be rejected.

b) If there is a discrepancy in the unit price quoted in figures and words, the unit price, in figures or in words, as the case may be, which corresponds to the total bid price for the item shall be taken as correct.

c) It the Bidder has not worked out the total bid price or the total bid price does not correspond to the unit price quoted either in words or figures, the unit price quoted in words shall be taken as correct.

d) Bank may waive off any minor infirmity or nonconformity or irregularity in a bid, which does not constitute a material deviation, provided such a waiving, does not prejudice, or effect the relative ranking of any bidder.

22.5 No commitment to accept the lowest or any offer

a) The Bank reserves its right to reject any or all the offers without assigning any reason thereof whatsoever.

b) The Bank will not be obliged to meet and have discussions with any bidder and/ or to entertain any representations in this regard.

c) The bids received and accepted will be evaluated by the Bank to ascertain the best and lowest bid in the interest of the Bank. However, the Bank does not bind itself to accept the lowest or any Bid and reserves the right to reject any oral bids at any point of time prior to the order

without assigning any reasons whatsoever. The Bank reserves the right to re-tender.

22.6 Conditional bids

Conditional bids shall not be accepted on any ground and shall be rejected straightway. If any clarification is required, the same should be obtained before submission of bids.

22.7 Contacting the Bank

a) Bidder shall NOT contact the Bank on any matter relating to its Bid, from the time of opening of Bid to the time a communication in writing about its qualification or otherwise received from the Bank.
b) Any effort by the Bidder to influence the Bank in its decisions on Bid evaluation, bid comparison may result in the rejection of the Bidder's Bid.

22.8 Issuance of contract

a) The Bank will award the contract to the successful Bidder, out of the Bidders who have responded to Bank's tender as referred above, who has been determined to qualify to perform the contract satisfactorily, and whose Bid has been determined to be substantially responsive and is the lowest commercial Bid.
b) The Bank reserves the right at the time of award of contract to increase or decrease of the quantity of goods or services or change in location where equipment is to be supplied from what was originally specified while floating the tender without any change in unit price or any other terms and conditions.

23. General Terms and Conditions

23.1 Term of implementation

The term of the implementation contract for SIEM and its components shall be initially for a period of 7 months, from the date of the release of purchase order. However, if for any reason the work is not completed to the satisfaction of the Bank within the stipulated time, the period of contract can be extended at the discretion of the Bank, at no extra cost. The decision to grant or refuse the extension shall be at the discretion of Bank.

The term of the SOC operations and Administration contract shall be initially for a period of 5 years. However, if for any reason if Bank is not satisfied with the Operations/Administration activity or the Bidder is unable to provide competent resources who met eligibility criteria mention, then Bank

reserves the right to cancel the contract with a three-month notice.

23.2 Adherence to terms and conditions

The Bidders who wish to submit responses to this RFP should note that they should abide (in true intent and spirit) by all the terms and conditions contained in the RFP. If the responses contain any extraneous conditions put in by the Respondents, such responses may be disqualified and may not be considered for the selection process.

23.3 Termination

The Bank may, terminate the Contract by giving the Bidder a prior and written notice indicating its intention to terminate the Contract under the following circumstances:

i) Where it comes to the Bank's attention that the Bidder (or the Bidder's team) is in a position of actual conflict of interest with the interests of the Bank, in relation to any of terms of the Bidder's Bid or this Contract.

ii) Where the Bidder's ability to survive as an independent corporate entity is threatened or is lost owing to any reason whatsoever, including inter-alia the filing of any Bankruptcy proceedings against the Bidder, any failure by the Bidder to pay any of its dues to its creditors, the institution of any winding up proceedings against the Bidder or the happening of any such events that are adverse to the commercial viability of the Bidder. In the event of the happening of any events of the above nature, the Bank shall reserve the right to take any steps as are necessary, to ensure the effective transition of the project to a successor Bidder, and to ensure business continuity.

iii) The Bank, without prejudice to any other right or remedy for breach of Contract, by a written notice of default sent to the Bidder, may terminate the Contract in whole or in part.

iv) In the event Agreement comes to end on account of termination or by expiry of the term / renewed term of the Agreement or otherwise, the bidder shall render all reasonable assistance and help to the Bank and to any new Bidder engaged by the Bank, for the smooth switch over and continuity of the Services. Self-Declaration to this effect should be submitted along with the bid.

23.4 Issuance of purchase order

Bank will issue purchase order for the installation and commissioning of the SIEM solutions as per the scope of work and onsite manpower for managing the SOC.

23.5 Software/Hardware requirements

All the software has to be brought by the Bidder at no extra cost and to be installed in Bank's laptop to carry out the installation and the same can be removed after completing the installation. Bank will not permit bidder/OEM to connect their laptop/tools in Bank's network without prior permissions.

23.6 Professionalism

Bidder should provide professional, objective and impartial advice at all times and hold the Bank's interest paramount and should observe the highest standards of ethics, values, code of conduct, honesty and integrity while implementation of the SIEM solutions and during support.

23.7 Adherence to safety procedures, rules regulations and restriction

i) Bidder shall comply with the provision of all laws including labour and industrial laws, rules, regulations and notifications issued there under from time to time. All safety and labour and industrial laws enforced by statutory agencies and by Bank shall be applicable in the performance of this Contract and Bidder shall abide by these laws. The Bidder shall indemnify and keep indemnified and hold harmless the Bank for any loss, damage, claims, costs, charges, expenses, etc. arising out of and/or suffered on account of actions, litigations, proceedings, suits, arising out of breach of the above laws.

ii) Bidder shall take all measures necessary or proper to protect the personnel, work and facilities and shall observe all reasonable safety rules and instructions.

iii) The Bidder shall report as soon as possible any evidence, which may indicate or is likely to lead to an abnormal or dangerous situation and shall take all necessary emergency control steps to avoid such abnormal situations.

iv) Bidder shall also adhere to all security requirement/regulations of the Bank during the execution of the work.

23.8 Expenses

i) Prices payable to the Bidder as stated in the Contract shall be firm and not subject to adjustment during performance of the Contract, irrespective of reasons whatsoever, including exchange rate fluctuations, changes in taxes, duties, levies, charges, etc. However, Bank shall be entitled to make applicable deductions including adjustment in the payment of Contract price in the event of levying liquidated damages on the Bidder as provided under the Contract.

ii) It may be noted that Bank will not pay any amount/expenses / charges / fees / traveling expenses / boarding expenses / lodging expenses / conveyance expenses / out of pocket expenses other than the 'Agreed Price'.

23.9 Payment terms

Bank will release the payment within 1 month of receiving the undisputed invoice, after deduction of applicable taxes at source of the agreed price to the selected Bidder. No advance payments will be made. Further, it may be noted that the below mentioned criteria is only for the purpose of effecting agreed price payment.

23.9.1 Payments of hardware and software items

Payment for the hardware / software (Item A in commercial bid format) will be as detailed below,

i) 100% payment on delivery, installation & receipt of licenses for hardware, implementation, completion of phase III, i.e. onboarding of critical applications to SIEM, support and on production of acceptance certificate and performance guarantee.

In case of a delay during installation due to technical reasons from Bank's end,

- 80% payment on delivery
- 20% on installation & receipt of licenses for hardware, implementation, completion of phase III, i.e. onboarding of critical applications to SIEM, support and on production of acceptance certificate and performance guarantee.

23.9.2 Payment for the SOC Operations

The payment for SOC operations will be paid quarterly in arrears post the successful commissioning of the project and acceptance of all the relevant requirements under this tender.

23.9.3 Payment for the other services

The payment of annual maintenance charges will be yearly in advance in the beginning of 4th 5th, 6th & 7th year respectively.

23.10 Contract performance guarantee

I. Bidder has to provide an unconditional and irrevocable performance guarantee for 15% of the contract value towards due performance of the contract in accordance with the specifications, terms and conditions of this RFP document, within 15 days from the date of work order. The Performance Guarantee shall be for 15 months (12 months plus 3 months

additional claim period) kept valid for the entire period and to be released at the end of the implementation period.

II. The Performance Bank Guarantee will be furnished for due performance of the complete solution /services.

III. In case successful bidder submits any false information or declaration letter during the tender process or period of contract, Bank shall invoke the EMD/ Performance Bank Guarantee submitted by the bidder to recover penalty/damages. In case successful bidder fails to perform the contract / to comply with the terms and condition of RFP, Bank shall invoke the Performance Bank Guarantee to recover penalty/damages.

IV. No interest on PBG will be paid by the Bank and bidder shall not have any claim regarding interest on PBG amount.

V. Further, the Bank reserves the right to invoke the Performance Bank Guarantee in case the Selected bidder is not able to fulfill any or all conditions specified in the document or is unable to complete the project within the stipulated time. In case the contract is getting extended, the selected bidder shall submit the Bank Guarantee of same amount of that period of time with a validity of the extension period with 12 months claim period. The selected bidder shall be responsible for extending the validity date and claim period of Performance Bank Guarantee as and when it is due on the account of non-completion of the project.

23.11 Single point of contact

Bidder has to provide details of single point of contact viz. name, designation, address, e-mail address, telephone/mobile no., etc.

23.12 Applicable law and jurisdiction of court

The Contract with Bidder shall be governed in accordance with the laws of India for the time being in force and will be subject to the exclusive jurisdiction of courts at Cochin, Kerala.

23.13 Liquidated damages (LD)

In case of termination of contract, the Bank reserves the right to recover an amount equal to 15% of the Contract value as Liquidated Damages for non-performance.

If bidder fails to complete the due performance of the contract in accordance with the specifications and conditions agreed during the agreement, the Bank reserves the right to recover LD @ 0.5% of

the Total Charges per week as per Commercial Bid Format or part thereof, subject to a maximum of 15 % of total charges as LD for non-performance/delayed performance.

23.14 Force majeure

Any failure or delay by selected Bidder or Bank in the performance of its obligations, to the extent due to any failure or delay caused by fire, flood, earthquake or similar elements of nature, or acts of God, war, terrorism, riots, pandemics, civil disorders, rebellions or revolutions, acts of governmental authorities or other events beyond the reasonable control of non-performing party, is not a default or a ground for termination. The affected party shall notify the other party of the occurrence of a Force Majeure Event forthwith. In case the force majeure period continues for a period beyond 60 days, non-affected/non-defaulting party shall have the right to terminate the contract.

23.15 Authorized signatory

The selected Bidder shall indicate the authorized signatories who can discuss and correspond with the Bank, with regard to the obligations under the contract. Bidder shall submit at the time of signing the contract, a certified copy of the resolution of their Board, authenticated by Company Secretary/Director, authorizing an official or officials of the company or a Power of Attorney to discuss, sign agreements/contracts with the Bank. Bidder shall furnish proof of identification for above purposes as required by the Bank.

23.16 Due Diligence

Bidder shall submit the necessary details/documents and permit Bank and its appointed third parties to conduct Due Diligence, in defined frequency, as per the Bank's policy.

23.17 Indemnity

Bidder shall indemnify Bank and keep the Bank indemnified from and against any losses suffered by the Bank arising out of any breach of the Agreement, violation of any applicable laws, negligence, wilful misconduct or wrongful act or omission in connection with the services, misfeasance, malfeasance, fraudulent acts by any employees/agents and all third party claims, liabilities, damages, losses, costs, charges, expenses, proceedings and actions of any nature whatsoever made or instituted against the Bank directly or indirectly, provided there is no negligence, default, wilful misconduct or breach of the Agreement by the Bank and its authorized

representatives, employees(s)or agent(s) in performing their part under the Agreement.

23.18 Agreements

Bidder shall execute agreements such as NDA, MSA, SLA, Scope of Work etc., with the Terms & Conditions mentioned in the RFP. These Agreements shall be stamped at rate applicable to agreement plus indemnity. If the same is executed in two States, stamp duty applicable in the first State would have to be paid. However, if the rate of stamp duty is higher in the second State, the difference would have to be paid at the time of execution in the second State. It shall also be ensured that the persons executing the Agreement are duly authorized on this behalf.

23.19 Non Payment of agreed price

If any of the items/activities as mentioned in the price bid and as mentioned in Commercial Bid format are not taken up by the Bank during the course of this implementation, the Bank will not pay the contracted agreed price quoted/agreed by the Bidder in the price bid against such activity/item.

23.20 Assignment

Neither the contract nor any rights granted under the contract may be sold, leased, assigned, or otherwise transferred, in whole or in part, by the Bidder without advance written consent of the Bank and any such sale, lease, assignment or transfer otherwise made by the Bidder shall be void and of no effect.

23.21 Confidentiality

i) The Bidder shall treat all documents, information, data and communication of and with Bank as privileged and confidential and shall be bound by the terms and conditions of the Non-Disclosure Agreement, draft of which is given in Annexure-K. The Bidder shall sign and execute this Non-Disclosure Agreement before the execution of this Contract.

ii) The Bidder shall not, without Bank's prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, sample or information or data or drawings / designs furnished by or on behalf of Bank in connection therewith, to any person other than a person employed by the Bidder in the performance of the Contract. Disclosure to any such employed person shall be made in utmost confidence and shall extend only so far as may be necessary and relevant for purpose of such performance and shall be subject to the terms and conditions

of the Non-Disclosure Agreement.

iii) The Bidder shall not, without Bank's prior written consent, make use of any document, data or information etc., enumerated in this Bid Documents save and except for due performance and observance of the Contract.

iv) Any document, other than the Contract itself, enumerated in this Bid Documents shall remain the property of Bank and shall be returned (in all copies) to Bank on completion of the Bidder's performance under and in accordance with the Contract, if so required by Bank.

23.22 Use Of Name/Logo of the Bank

Bidder shall not use for publicity, promotion, or otherwise, any logo, name, trade name, service mark, or trademark or any simulation, abbreviation, or adaptation of Bank or any of its affiliate, or the name of any of the Bank's employee or agent, without the Bank's prior, written, express consent. The Bank may withhold such consent, in case so granted by it, in its absolute discretion. Violation thereof shall constitute a material breach of the terms of this Contract and shall entitle the Bank to take appropriate actions as available to it in law and under this Contract.

23.23 Non-solicitation

Bidder, during the term of the contract and for a period of two years thereafter shall not without the express written consent of the Bank, directly or indirectly: a) recruit, hire, appoint or engage or attempt to recruit, hire, appoint or engage or discuss employment with or otherwise utilize the services of any person who has been an employee or associate or engaged in any capacity, by the Bank in rendering services in relation to the contract; or b) induce any person who shall have been an employee or associate of the Bank at any time to terminate his/ her relationship with the Bank.

23.24 No employer-employee relationship

The selected Bidder or any of its holding/subsidiary/joint-venture/ affiliate / group / client companies or any of their employees / officers / staff / personnel / representatives/agents shall not, under any circumstances, be deemed to have any employer-employee relationship with the Bank or any of its employees/officers/ staff/representatives / personnel /agents.

23.25 Subcontracting

The selected Bidder shall not subcontract or permit anyone other than its personnel or OEM to

perform any of the work, service or other performance required of the Bidder under the contract without the prior written consent of the Bank.

23.26 Cancellation of contract and compensation

The Bank reserves the right to cancel the contract of the selected Bidder and recover expenditure incurred by the Bank in any of the following circumstances. The Bank would provide 30 days' notice to rectify any breach/ unsatisfactory progress if:

- Bidder commits a breach of any of the terms and conditions of the bid/contract;
- Bidder becomes insolvent or goes into liquidation voluntarily or otherwise;
- an attachment is levied or continues to be levied for a period of 7 days upon effects of the bid;
- the progress regarding execution of the contract, made by the Bidder is found to be unsatisfactory.
- if deductions on account of penalty and liquidated damages exceeds more than 10% of the total contract price.
- if the Bidder fails to complete the due performance of the contract in accordance with the agreed terms and conditions.

After the award of the contract, if the selected Bidder does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one month's notice for the same. In this event, the selected Bidder is bound to make good the additional expenditure, which the Bank may have to incur to select and carry out the execution of the balance of the contract. This clause is also applicable, if for any reason, the contract is cancelled.

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 Bank Guarantee/Security Deposit, if any, under this contract.

23.27 Dispute resolution

If a dispute, controversy or claim arises out of or relates to the contract, or breach, termination or invalidity thereof, and if such dispute, controversy or claim cannot be settled and resolved by the

Parties through discussion and negotiation, within 30 days from the date of initiation of such discussion/negotiation, then the Parties shall refer such dispute to arbitration. Both Parties may agree upon a single arbitrator. The arbitration shall be conducted in English and a written order shall be prepared. The venue of the arbitration shall be Cochin. The arbitration shall be held in accordance with the Arbitration and Conciliation Act, 1996. The decision of the arbitrator shall be final and binding upon the Parties, provided that each Party shall at all times be entitled to obtain equitable, injunctive or similar relief from any court having jurisdiction in order to protect its intellectual property and confidential information.

23.28 Ownership of documents

i) Bank shall own the documents, prepared by or for the Bidder arising out of or in connection with this Contract.

ii) Forthwith upon expiry or earlier termination of this Contract and at any other time on demand by the Bank, the Bidder shall deliver to the Bank all documents provided by or originating from the Bank and all documents produced by or from or for the Bidder in the course of performing the Services, unless otherwise directed in writing by the Bank at no additional cost. The Bidder shall not, without the prior written consent of the Bank, store, copy, distribute or retain any such documents.

Annexure A: Bid Forwarding Letter (Submitted on Bidder's letter head)

The VP & CISO
Information Security Division
Integrated Risk Management Department,
Federal Bank Ltd, Federal Towers,
Aluva - 683101
Kerala, India.

Date:

Dear Sir/Madam,

Purchase of SIEM solution and implementation of next gen security operations centre

We, the undersigned, offer to submit our bid in response and accordance with your tender No. 1/2023/FBL/ISD dated 30/10/2023. Having examined the tender document including all annexures carefully, we are hereby submitting our proposal along with all the requisite documents as desired by the Bank.

Further, we agree to abide by all the terms and conditions as mentioned herein the tender document. We agree to abide by this offer till 2 months from the date of last day for submission of offer (Bid). If our offer is accepted, we undertake to provide service support for the hardware supplied as per the above referred RFP, during warranty as well as AMC period of 4 years if contracted.

We have also noted that Federal Bank reserves the right to consider/ reject any or all bids without assigning any reason thereof.

We understand that the Bank is not bound to accept any proposal it receives.

We remain,

Yours sincerely,

Date
Place

Signature & name of the authorised signatory
Designation

Phone & e-mail:
Name of the organisation

Annexure B: Minimum Eligibility Criteria

Bidder who wishes to bid should conform to the following criteria.

Sl.no.	Eligibility criteria	Documents to be submitted	Page/ Ref no.
1	Bidder should be either a Government Organization/PSU/PSE/ partnership firm or a limited Company under Indian Laws or /and an autonomous Institution approved by GOI/RBI promoted,	Limited Company-Certified copy of Certificate of Incorporation and Certificate of Commencement of Business. Partnership firm-Certified copy of Partnership Deed. Reference of Act/Notification For other eligible entities- Applicable documents.	
2	The bidder should be Original Equipment Manufacturer [OEM] or authorized partner of OEM. In case of authorized partner of OEM the bidder should submit Manufacturer Authorization Form (MAF) as per format given in Annexure H.	MAF as per format given in Annexure-H, to be submitted.	
3	Bidder should be in the business of supply, installation, configuration, maintenance and support of SIEM solutions and other security appliances. for at least Five [5] years as on date.	Proof of same to be attached by way of purchase order	
4	Bidder should have implemented the proposed SIEM solutions in a public/private sector Banks in India with atleast 1 lakh EPS or 3 TB per day.	Satisfactory Performance Certificate from the Clients OR Copy of purchase order	

Sl.no.	Eligibility criteria	Documents to be submitted	Page/ Ref no.
5	Bidder should have managed security operations center in a public/private sector Bank in India with at least 1 lakh EPS or 3 TB per day for at least 3 years.	Satisfactory Performance Certificate from the Clients OR Copy of purchase order	
6	The Bidder should have provided Services (Operations) for Captive SOC to at least -1- institution for -1- year, on the same SIEM tool in India in the last -3- years.	Satisfactory Performance Certificate from the Clients OR Copy of purchase order	
7	The OEM of SIEM tool should have been in existence in India for the last -5- years as on 30/09/2023 with its own support centre and the proposed solution should have End of Life/End of Support after 7 years.	Provide the documentary evidences	
8	The bidder should have a minimum average annual turnover of 5 crores over the last three financial years. The bidder should have profit [i.e. no cash loss] in 2 years out of the last 3 years	Financial auditor's certificate for last three years	
9	The bidder must have a currently valid GST registration certificate and PAN number.	Copies of PAN / GST Registration Certificate to be enclosed.	
10	The Bidder/bidder should have its own support office(s) in either Kochi or Bangalore.	Details of support center at Kochi or Bangalore to be submitted.	

Sl.no.	Eligibility criteria	Documents to be submitted	Page/ Ref no.
11	The Bidder should have all necessary licenses, permissions, consents, no objections, approvals as required under law for carrying out its business.	An undertaking (on their letter head) that they have all necessary licenses, permissions, consents, no objections, approvals as required under law for carrying out its business, as on date of submission of the Bid.	
12	Should have at least fifteen numbers of staff on their rolls with each of these following certifications: CISA, CISM, CISSP and Certifications in the proposed solution etc.	Provide the documentary evidences	
13	The Bidder must have at least 15 employees who are OEM Certified professionals on same SIEM tool.	Provide the documentary evidences	
14	The firm should not be blacklisted / barred by Government of India or any regulatory body in India.	Self-Declaration	
15	Proposed Product should be in the Leaders quadrant/category as per Gartner or Forrester report published for the last three consecutive years.	Please provide copies of the reports.	
16	The bidder should not be involved in any litigation which threatens solvency of company.	Undertaking to be submitted by CA.	
17.	Labour Law Compliance	Undertaking to be submitted on Letterhead	

Note: Bidder must comply with all the above mentioned criteria as specified above. Photocopies of relevant documents / certificates should be submitted as proof in support of the claims made for each of the above mentioned criteria. The Bank reserves the right to verify / evaluate the claims made by the bidder independently. Proposals of bidders who do not fulfil the above criteria or who fail to submit documentary evidence thereon would be rejected.

Annexure C: Technical Bid Format

Particulars to be provided by the Bidder in the technical proposal:

No	Particulars	Bidder to furnish details	Reference Page no of relevant document in RFP response
1	Name of the Bidder		
2	Date of establishment and constitution. Certified copy of "Partnership Deed" or "Certificate of Incorporation/commencement of business" should be submitted. For entities other than partnership firm and limited company, other relevant documents to be submitted.		
3	Location of Registered Office /Corporate Office/ Cochin office/Bengaluru Office with addresses.		
4	Mailing address of the Bidder		
5	Names, mobile number, E-mail address and designations of the persons authorized to make commitments to the Bank		
6	Telephone number of contact persons. (give at least 2 contact persons details)		
7	E-mail addresses of contact persons		
8	Whether MSE(quote registration no. and date of registration, copy to be attached)		
9	Bank Account Detail: Account Number, Account Name, IFSC, Bank Name		
10	Whether company has been blacklisted for		

No	Particulars	Bidder to furnish details	Reference Page no of relevant document in RFP response
	service deficiency in last 3 years. If yes, details thereof.		
11	Any pending or past litigation (within three years)? If yes, please give details		
12	Please mention turnover for last three financial years and include the copies of Audited Balance Sheet in support of it.		
13	Details of description of business and business background, Service Profile & client profile, Domestic & International presence.		
14	Experience of implementing the SIEM solutions at other organizations in India in the last -3- years as per the following details :(For item nos. 14a to 14c, Name of the organization, time taken for implementation and documentary proofs in the form of copy of purchase order etc. are to be furnished)		
14a	SOC implementation in Banks		
14b	SOC implementation in BFSI Sector other than Banks.		
14c	SOC implementation in organizations other than BFSI institutions.		
15	Details of the similar implementations on hand as on date (Name of the Bank, time projected for installation and commissioning of the SIEM appliance)		

Annexure D: Technical Specification

1) SIEM Solutions at Data Center, Aluva and Disaster Recovery site, Bangalore

S.No	High level technical specifications	Bidder Compliance	Deviation
	SIEM Device Specifications - Technical and general		
1	The solution should be scalable to support minimum 10000 devices to up to 15000 devices with sustainable Events per Second (EPS) of 50,000 EPS or equivalent TB/day whichever is higher in DC & DR separately from day one. The solution, including hardware, should be scalable to support without dropping or queuing of logs, 1 lakh EPS or equivalent TB/day whichever is higher in DC & DR separately during contract period.. EPS specifies the ability of the solution to gather, store, monitor, correlate and report events per second. There should not be limitations on the types of the end-points like servers, network devices, virtual machines or any other data source(s) that is to be integrated.		
2	The SIEM tool can be either software based, or appliance based. In case of Software based SIEM solutions, bidder shall bundle necessary hardware. OEM must certify that the hardware proposed by the bidder is sufficient to cater RFP requirement. Hardware proposed in both cases should be rack mountable with dual power supply and should comply with DataCenter Standards.		
3	The solution should allow vertical and horizontal scale out for future growth. Proposed hardware shall handle additional 100% growth.		
4	Proposed SIEM solution should be able to scale to capture Layer2-Layer 7 Traffic along with the logs.		
5	The solution should be implemented on a Hardened OS and database in Hardware / Appliance. The storage configuration must offer a RAID configuration to allow for protection from disk failure.		
6	The solution should have a High Availability feature built in. There should be an automated switch over to secondary collectors/Agent Server in case of failure on the primary collector/Agent Server. No		

S.No	High level technical specifications	Bidder Compliance	Deviation
	performance degradation is permissible even in case of collector/Agent Server failure.		
7	The solution shall be capable to host an instance in Cloud, for log collection, parsing, storage of logs from event sources hosted in Cloud and connect to the head unit hosted on-premise for correlation & incident management. Multiple instances shall be allowed for the same CSP (Ex: Hosting 2 or more instances in AWS alone shall be feasible) There shall be no limit on the number of instances that can connect to the head unit.		
8	In case of need, it should be feasible for migrating the entire solution to Cloud, solution shall be platform agnostic, compatible with all the Cloud platforms. In such scenario, solution should be capable to collect logs from the event sources hosted on-premise along with the logs from other Cloud platforms.		
9	The Solution should provide secure web-based administration for device management and monitoring.		
10	The Bidder should facilitate that in case of failure of the assigned collector, the devices should be able to send the data to another collector (if available) without losing any data so that there be no gaps in analysis and reporting. In case the connectivity with the SIEM management system is lost, the collector should be able to store the data in its own repository. The retention, deletion, synchronisation with SIEM database should be possible automatic but configurable for this repository.		
11	The proposed solution must include Next Gen SIEM and Security Analytics with necessary automation capabilities. To avoid maintaining multiple data repositories, proposed solution should have central data repository which should act as common repository for SIEM, UEBA and similar components.		
12	To virtually segregate different types of data, proposed solutions should support multiple virtual storage groups or indexes. Each index/ virtual		

S.No	High level technical specifications	Bidder Compliance	Deviation
	storage group should be used for searching specific data and retention period should be configurable as per indexes.		
13	The proposed solution must support the data replication natively without relying on other third-party replication technologies on the operating system or storage level with near zero RPO and RTO. The solution should also allow the admin to decide on the replication factor between DC and DR. DR should be updated with artefacts for any incident, analyst is working on in DC.		
14	The proposed solution should provide a test/development licence as part of the solution.		
15	Machine learning should be embedded across the platform. It should empower every user in the SOC with ML. Security analyst to become citizen data scientist i.e. used predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate various ML frameworks		
16	The solution must ensure that if data ingested is not parsed then with the new parser old data ingested should also be parsed without need to re-ingest data throughout the retention period of online 180 days and offline 1 year.		
17	The proposed solution should have Out of The Box support for identifying data gaps for deploying MITRE ATTACK & Kill Chain use cases. It should help to check data availability and guide on data sources are required to implement MITRE ATTACK Technique & Sub techniques		
18	The proposed solution should have physical or logical separation of the collection module, logging module and analysis / correlation module with the ability for adding more devices, locations, applications, etc.		
19	The Proposed solution must offer all the below built-in threat detection techniques out of the box:		
	a. Detect Web Application Threats.		

S.No	High level technical specifications	Bidder Compliance	Deviation
	b. Detect APT Threats		
	c. Detect threats indicated by advisories		
	d. Give visibility of endpoints also by integrating with EDR, Antivirus etc. for endpoint analytics .		
20	Proposed solution must integrate with the security tools implemented in the Bank, including but not limited to the below		
	Extended Detect and Respond		
	Web Application Firewall		
	Intrusion Prevention System		
	Database Activity Monitoring		
	Data Leakage Prevention		
	File Integrity Monitoring		
	Network Access Control		
	Information Rights Management		
	Privilege Management		
	Data Classification		
	TACACS		
	Terminal Security Solution		
21	The proposed solution must provide an interface that allows the same query string to be configured as an alert, report or a dashboard panel.		
22	OEM to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 7 business days from date of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will		

S.No	High level technical specifications	Bidder Compliance	Deviation
	provide parsers for data ingestion in maximum 7 business days from date of intimation of the same, without dependency of the bidder.		
23	The proposed solution must be scalable and have a distributed architecture with native replication of data across DC & DR. DR should be active all the time to ensure continuous security monitoring. The dual forwarding feature should be configurable as per Bank requirements and capability for enabling & disabling should be available depending on the device, IP address, and other related parameters.		
24	The proposed solution must support single site or multiple site clustering allowing data to be replicated across the peer's nodes and across multiple sites with near zero RTO & RPO.		
25	The proposed solution must support viewing of the same log data in different formats or should support multiple schema views during search time or report building time without redundant storage or re-indexing so that complex report or user defined reports can be built.		
26	The proposed solution must come with pre-packaged alerting capability, flexible service-based hosts grouping, and easy management of many data sources, and provide analytics ability to quickly identify performance and capacity bottlenecks and outliers in Unix and Linux environments. It should quickly compare resources and capacity utilisation across many hosts		
27	The proposed solution should provide dashboards for insight into resource consumption of desired systems, service availability status of critical services, integration with NMS tools for network status visibility, security alerts, risky users & entities, anomalies and outliers across all the data etc. from a single dashboard.		

S.No	High level technical specifications	Bidder Compliance	Deviation
28	The proposed solution should give visualisation of operational health of the Windows, Linux & Unix environment through a single dashboard customizable to service-groupings in your environment		
29	The proposed solution should have community portals and knowledgebase which can be used to learn about sample integration and forum to discuss issues or use cases.		
30	The system should have a provision of view filters when displaying the logs related to specific IP address, specific service or specific time duration or geographical location.		
Log Collection and retention			
1	The system shall be capable of supporting both real-time and on-demand access to data sources from files, network ports, database connections, custom APIs etc .,		
2	The proposed solution must be able to read data input from the following log file formats and other evolving format:		
	a. Archived Log Files (Single line, Multi-line, and Complex XML and JSON Structure)		
	b. Windows Events Logs		
	c. Standard Log Files from applications such as Web (HTTP) servers, FTP servers, Email (SMTP/Exchange) servers, DNS servers, DHCP servers, Active Directory servers, etc.		
	d. S/FTP,ODBC,CP-LEA,SDEE, OPSEC, raw text files, ODBC/JDBC and XML files.		
3	Logs should be collected from various devices including operating systems, security and network devices, applications, databases etc. Network traffic should be collected from gateway devices using port mirroring/span.		
4	The proposed solution shall be capable to collect the logs from Cloud instances, including but not limited to AWS, Azure, GCP, Oracle.		

S.No	High level technical specifications	Bidder Compliance	Deviation
	The proposed solution shall be able to collect the logs from storage spaces (S3 Buckets, Azure Blob storage etc.,) in Cloud platforms.		
5	In addition to the Cloud platform integration, proposed solution shall be capable to collect the logs from individual applications hosted in various Cloud platforms.		
6	The proposed solution must be able to accept the following indicative live data streams feeding through the network:		
	a. Syslog Messages		
	b. Security Alerts		
	c. JSON streaming over HTTP/HTTPS		
7	The proposed solution must support the decoding of the following indicative network protocols from log data or picking the meta data from network traffic: HTTP, FTP, DNS, MySQL, SMTP, SNMP, SMB, TCP, UDP, NFS, Oracle (TNS), LDAP/AD, PostgreSQL, Sybase/SQL Server (TDS), IMAP, POP3, RADIUS, IRC, SIP, DHCP, AMQP, DIAMETER, MAPI		
8	The proposed solution must come with out-of-the-box integration and dashboards, reports, rules etc. to provide rapid insights and operational visibility into large-scale CentOS, Windows, Unix and Linux environments machine data: syslog, metrics and configuration files.		
9	The proposed solution must collect, process, and store event log information in a manner that complies with log management best practices. The solution should allow administrators to extract logs in its raw format for a specific period, device type or an identified IP address. The logs should be stored in a format to ensure security of the logs from any unauthorised modification		
10	The proposed solution shall handle surges in data events lasting up to 12 hours without interfering with its ability to operate.		
11	The log/event collector should have active/failover configuration.		
12	The solution should allow creating custom metadata like usernames, event categories, actions, Department id, VLAN, owner, Ex-Department, employee type, Leave status etc if required. All raw logs		

S.No	High level technical specifications	Bidder Compliance	Deviation
	will be retained in the data store for 180 days of duration . All logs should be automatically categorised into categories like usernames, event categories, actions and other metadata fields		
13	The solution should do automatic data enrichment of the collected data like geolocation, business criticality and asset details.		
14	The solution should be able to collect log and network data, and the complete visibility of the environment should be displayed on a single console.		
15	The proposed data store should retain data for 6 months. Offline data for 1 year and cold storage for 7 years		
16	The console should allow specifying the database to choose as data source (hadoop/NAS/SAN for long term), or local for short term reporting.		
17	The solution should allow extending storage space for extending retention of log data.		
18	The datastore should support ad hoc querying locally.		
19	The solution should support compression on NAS/SAN.		
20	The product internal logs must be ingested within the product for ease of troubleshooting and investigation and those logs do not consume the product licence.		
21	The solution must provide granular licence utilisation down to devices/log sources		
22	Log Filtering – Not all logs are needed for the compliance requirements faced by an organization, or for forensic purposes. Logs can be filtered by the source system, times, or by other rules defined by the SIEM administrator.		
23	The proposed solution must support caching mode of transfer for data collection, to ensure data is being logged in the event of loss of network connectivity, and resume sending of data upon network connection.		
24	The proposed solution shall provide log filtering options at the event source end and at collector end. Licensing should be based on post		

S.No	High level technical specifications	Bidder Compliance	Deviation
	filtering of events. If log events are filtered, then they should not be counted in the license.		
25	Proposed solution should forward data to multiple destinations apart from its own SIEM processing/data storage layer. Log collectors should be able to forward data to multiple destinations.		
26	The solution must allow the adding/modifying/removing of log parsers without impacting log collection from the web interface.		
27	The solution should be able to collect raw logs in real-time to a Central Datastore from any IP Device including in house, customised and proprietary applications.		
28	The solution should be able to continue to collect log data during any activities performed without any disruption to service.		
29	The solution shall permit different user-defined categories of data events to be retained for different durations.		
30	System should have an interface to monitor and alert non reporting event sources.		
31	For the above cases, system should generate alerts in various formats like SMTP, SMS, Syslog, SNMP, instant messengers		
Normalization			
1	The proposed solution must be able to index all data from any application, server or network device including logs, configurations, messages, traps and alerts, metrics and performance data without any custom adapters for specific formats so that the analyst can have end to end visibility of the ecosystem.		
2	The proposed solution must be able to store data in its original format along with parsed/normalized data.		
3	The proposed solution shall build specific repositories which includes categories like including event types, tags, lookups, parsing/normalizing, actions and saved searches etc. It should help to discover and analyse various aspects of data. For example, event types should enable analysts to quickly classify and group similar events; then use them to perform analytics on events.		

S.No	High level technical specifications	Bidder Compliance	Deviation
4	The solution must support viewing data in different formats without re-ingesting, re-indexing, redundant storage. Historical data also should be viewed as per new format or schema without re-ingesting or without additional storage utilisation.		
5	The solution must provide inbuilt functionality to create parsers and allow testing and validation with existing live or historical data within the system from the web interface		
6	The solution must provide the same search language for search, investigate, alert, report and visualise licence utilisation. A proper error handling screen should be available.		
Correlation and Analysis			
1	The solution should allow creating correlation rules on desired meta.		
2	The solution should support correlation of logs from all the devices integrated and all security scenarios like spoofing, authentication failures, etc. The solution must support multi-device, multi-event and multi-site correlation across the Bank. The solution should be able to correlate on any fields in raw data.		
3	The system should support the following types of correlation:		
	a. Rule-Based Correlation		
	b. Vulnerability Based Correlation		
	c. Statistical Based		
	d. Historical Based		
	e. Heuristic Based		
	f. Behavioural Based		
4	The solution should have native geo-location feature support. The solution must support GeoIP location, name / IP address resolution, Google Earth visualisation (or similar).		

S.No	High level technical specifications	Bidder Compliance	Deviation
5	Solution should provide advanced threat intelligence that automatically collect, aggregate, deduplicate indicators of compromise from both open source and commercial intelligence feeds to enrich captured network traffic for contextual analysis, for botnet C&C servers, malware domains, proxy networks, known bad IPs and hosts, traffic to APT domains. The solution should be able to retrieve threats in various ASCII/UTF-8 file formats like text, csv, xml. Must be able to automatically parse IOC from STIX and OpenIOC formats. Must be able to support multiple transport mechanisms such as TCP or Trusted Automated exchange of Indicator Information (TAXII).		
6	The platform should support various structured and unstructured Threat Intelligence feed formats gathered from a combination of Commercial, Open source, User-led, and Community-driven Intel sharing sources and also provide complete advisory of threats to enable the Bank to plan counter-measures for taking proactive actions.		
7	The solution should provide out of box rules for alerting on threats found in log or network data. Ex- failed logins, account changes, expirations, port scans, suspicious file names, default usernames, default passwords, security tools, AV signature updates, failure of signature/policy updates, successful authentications, bandwidth by IP, email senders, failed privilege escalations, VPN failed logins, group management system configuration changes, traffic to non- standard ports, URL blocked, accounts deleted, accounts disabled, top intrusions etc.		
8	The solution should display summarization of events		
9	The solution should allow a wizard based interface for rule creation. The rules should support logical operators for specifying various conditions in rules.		
10	The solution should have the ability to correlate all the fields in a log		
11	The solution should be able to detect Advanced persistent threat		
12	The solution should support the following types of correlation conditions on log data.		
	a. Event following by another event		

S.No	High level technical specifications	Bidder Compliance	Deviation
	b. ON OFF conditions.		
	c. Grouping, aggregations, sort, filter, merge etc.		
	d. Alert suppression,		
	e. Avg count, min, max		
	f. Regex Support		
13	The solution should allow creating rules that can take multiple scenarios like and create alert based on scenarios like		
	a. Login on VPN followed by multiple failed logins to windows Where source IP(from VPN) is not India		
	b. Multiple Failed logins from users where the user has not changed the account password in the last 2 days.		
14	The solution should also support historical correlation. Capability search for matching historical data using a new correlation rule		
15	Capability to do trend analysis on collected data.		
	a. Report on all machines connecting outside the country only once a week.		
	b. No of events received for a particular event ID for last 3 months		
16	The solution must provide advanced threat intelligence content from multiple threat sources to enrich captured network traffic for contextual analysis.		
17	The proposed solution shall have the ability to consider following when performing the correlation:		
	- source system type.		
	- source system versions or patch levels		
	- the number of sources affected or involved		
	- the source system's timestamps.		
	- whether the source has stopped logging events or whether there has been a significant interruption in logging when performing correlations.		
	- logins, unsuccessful login, and logouts		
	- privileged user actions, connections, and requests		
	- changes to security policies in monitored devices and operating		

S.No	High level technical specifications	Bidder Compliance	Deviation
	systems		
	- changes to security and/or audit logging services		
	- changes to user accounts and permissions (on the source system)		
	- escalation of privileges		
	- Changes to file system objects		
	- Failed file or resource access attempts		
	- web server unauthorised or not found failures		
	- startup and shutdown of systems and services		
	- operating system, database, and applications changes		
	- SANS top 5 log report coverage		
	- suspicious or unauthorised network traffic patterns		
	- correlation of IP based events with users		
	- client(s) generating excessive DHCP requests		
	- server(s) generating large numbers of authentication failures		
	- a single machine receiving authentication failures from multiple servers		
	- a single machine receiving authentication failures when trying different usernames when performing correlations.		
	- recognition of related events		
	The bidder shall describe any other correlation considerations.		
18	The proposed solution update shall provide an automated process for updating the correlation signatures.		
19	The solution including services shall support auditing and forensic analysis processes by collecting all relevant data events for an incident into a single report. The Bidder shall provide support to export the correlation report/ subset of correlation report with all supporting data events.		
20	The proposed solution shall have the capability of detecting already compromised systems.		
21	The proposed solution must be fully integrated with the log platform without the need to duplicate the collected raw logs.		
22	The proposed solution must be able to assign any arbitrary risk score		

S.No	High level technical specifications	Bidder Compliance	Deviation
	based on a self defined query based on any correlated events, statistical analysis, threat indicator match.		
23	The proposed solution must be able to support the following indicative list		
	- Network		
	- HTTP Referrer, User Agent, Cookie, Header, Data, URL		
	- IP		
	- Domain		
	- Endpoint		
	- File Hash, Name, Extension, Path and Size		
	- Registry Hive, Path, Key Name, Value Name, Value Type, Value Text, Value Data		
	- Process Name, Arguments, Handle Name, Handle Type		
	- Service Name, Description		
	- Certificate		
	- Certificate Alias, Serial, Issuer, Subject, Start Time, End Time, Version, Handshake Type, Public key Algorithm, Signature Algorithm		
	- Email		
	- Email Address, Subject Body		
24	Beside event matching signature use cases, the proposed solution must have the following analytical capabilities to address anomalies and behavioural based use cases.		
	- Basic Statistical analysis that can be applied to any fields like calculating the length of command line arguments, HTTP user agent string, sub domains, URLs, standard deviation of count of events over time		
25	The proposed solutions should use distance formula to detect geographically improbable access		

S.No	High level technical specifications	Bidder Compliance	Deviation
26	The proposed solutions should use randomness to measure domain names that can be potentially from malware domain generated algorithms.		
27	The proposed solution should use statistical functions or techniques like percentile or standard deviation to detect unusual activities that can be applied to insider or fraudulent use cases.		
28	The proposed solution should find relationships between pairs of fields by change in randomness in pairs of fields.		
29	The proposed solution's detection use cases should consist of guidance that provides an assessment of the Security Threat and how it helps detect and investigate it using the proposed solution. In addition, it should provide a summary of how the attack or detection technique maps to the following:		
	- ATT&CK MITRE, an adversary behaviour model that describes the actions an adversary might take.		
	- Kill-Chain, a model that identifies the phases an adversary must complete to achieve their objective.		
	- CIS Critical Security Controls		
	- Data types that are referenced within the rules/search and that need to be populated.		
	- Technologies, example technologies that map to the data types.		
	- There should be template to upload advisories in an automated manner.		
	- There should be templates to design and trigger workflows automatically.		
	- Any other customizable templates as per Bank requirements.		

S.No	High level technical specifications	Bidder Compliance	Deviation
30	The proposed solution should also guide administrator on data sources required to implement detection techniques from the same console (ATTACK MITRE, CIS, NIST, Kill Chain etc.)		
31	The system should be able to capture information about criticality ratings of assets and should leverage that information while performing correlation and raising alerts/incidents.		
32	The system should be able to integrate with external tools used for VA, change management, asset inventory, incident management etc to enrich the data collected from the event sources and Bank may choose to deploy/integrate other tools in future.		
33	The solution shall include the ability to add a timestamp to each collected event. The solution shall include the ability to automatically synchronise its timestamp clock to External/Bank servers using NTP.		
34	The proposed solution should be able to receive, ingest and index structured or unstructured data without schema or normalization and no events should be dropped if log source changes the format of log data. Unparsed events should be usable for correlation and machine learning models.		
Alert and Incident Management			
1	Solution should allow setting up of alerts based on event types, system events, attacks, failure count, geographical location, department wise, etc.		
2	The solution should provide full forensic event playback to ensure comprehensive trend and historical analysis and reporting.		
3	It should allow filtered view of alerts classified on the basis of severity/device/traffic-on-tcp or udp- port/location / segment to different teams, geographical locations		
4	The system should support alert suppression for specific events like :		
	- Number of duplicate alerts that come within specified time frame.		
	- Suppression based on specified time frame.		
	- Based on variables like Device IP address.		
5	The solution should have the below features on alerts/incidents		

S.No	High level technical specifications	Bidder Compliance	Deviation
	- Rules shall have the provision to consider another alert as an input		
	- Incident shall have entire lifecycle management & escalation to next levels		
	- Clubbing of multiple alerts into one in specific cases Ex: If there's an alert for a failed login attempt by user X, the next set of alerts for failed login attempts by same user shall be added in to the first alert		
	- Automated notification for alerts on mail/sms/instant messengers etc., E-mail notifications should contain the contents of the report as an attachment capable of being saved as Excel and or PDF.		
	- Escalation Matrix configurable		
6	The Solution must support Investigation notes/outcome to be chronologically captured and presented		
7	The Solution must provide information in such a way that analysts can quickly understand the source and impact of an attack, enabling teams to respond more effectively		
8	The system should provide investigators with a dashboard interface for reviewing assigned incidents, adding case notes and attachments and tracking tasks.		
9	The Solution must support retention of incidents, case notes and attached artifacts, should be retained for 1 year.		
10	The proposed Solution must have built-in MITRE ATT&CK alignment		
11	The solution must out-of-the-box include an analytics engine that displays relationship between incidents based on similar artefacts.		
12	The solution must provide long term trend analysis of incidents.		
13	The solution must provide the ability to correlate artefacts across potentially disparate incidents.		
14	The solution must provide visualization of incident correlation out-of-the-box across IOCs and other artefacts automatically with timeline support.		

S.No	High level technical specifications	Bidder Compliance	Deviation
15	Solution should support sending notifications to external users on per incident / escalation basis		
16	Solution should specify the mode of receiving an incident for example (REST API, mails, Syslog etc)		
17	Solution should support grouping of multiple incidents of similar type into one incident		
18	Solution must maintain repository of IOCs which can be associated with any stage of a cyber-kill chain for an incident		
19	Solution should integrate with third party Incident management tools and IT ticketing system (third party)		
20	The solution must have a provision to remove duplicate incidents and merge all duplicate ones in a single incident automatically and manually.		
21	The system should have an Event display Window for all alerts coming in real time		
22	The process should allow applying filters and sorting to query results.		
23	The proposed solution must be able to run any search on a schedule and set alerting conditions based on thresholds and deltas in the number and distribution of results across a time range or days like a histogram visualisation.		
24	The proposed solution must be able to support sophisticated statistical and summary analysis by pipelining advanced search commands together in a single search.		
25	The proposed solution must be able to support predictive analytics to predict future values of single or multi-valued fields. This will help security analytics to predict the attack patterns or specific attacks using multiple fields in the alerts or logs.		
26	The proposed solution must possess built-in function for Predictive Analysis/Anomaly detection:		
	a. Uses historical data as a baseline to forecast future patterns, thresholds, and tolerances		

S.No	High level technical specifications	Bidder Compliance	Deviation
	b. Ability to identify the future needs of critical system resources, no prior knowledge in predictive modelling algorithms required to use this functionality, and the ability to easily interpret and customise the results		
27	The proposed solution report or table must be able to be embedded in third-party business applications incl. Email and Teams		
28	Once the incident is created, the system should provide an overall workflow from investigation, analysis, notification and resolutions.		
29	The solution should automate the incident management workflow for critical security events from detection, investigation, analysis and resolution. The solution should automatically create the incident and enrich the incident with the latest business context.		
30	Additionally, the solution should have the capability to create user definable dashboards of incidents, i.e., one at the CISO level that provides an overall view of an organisation's security incidents and another dashboard could specifically focus on the security analyst		
31	Also, the system should allow the workflow of the incident to be managed as per the organisation's standard document workflows. For example, depending on the incident, the organisation could have specific notification and resolution procedures. The system should enable organisation to establish these procedures and manage the workflow accordingly.		
32	System, should provide ability to		
	- Allow creation of library of predefined response procedures that can be categorised by incident type and automatically assigned as incidents are reported.		
	- assign incidents to specific users and response teams, and access to incident data to be restricted to only those users.		
	- Assign Incidents to functional groups and geographical location.		
	- Auto-notified via email Investigators when incidents are reported to which they are assigned.		

S.No	High level technical specifications	Bidder Compliance	Deviation
	- Allow Multiple investigators can work on a single incident, and track changes made to incident data with a user/date/time stamp.		
33	The proposed solution must provide investigation auditing capability to enable analysts to easily:		
	- Track searches and activities		
	- Review activities at any point		
	- Select and place into timeline for temporal analysis		
	- Help remember searches, steps taken, provide annotation support		
34	The solution must be able to provide a built-in facility to centralise incident analysis of entities in one location.		
35	The proposed solution should be able to trigger actions. These actions can be automatically triggered by correlation alerts or offences or manually run on an ad hoc basis from the Incident.		
36	The proposed solution should have integration with major commercially available tools OOTB for triggering actions without dependency with SOAR solution.		
37	Should provide Asset Criticality of the Banks infrastructure and allow analysts to scale the alerts based on the criticality ratings.		
38	Following process like Incident Response, Breach response, Policy Management should be automated		
39	Proposed solution should allow automation of SOC related activities like Shift Handover, Administrative , Incident Measurement, Risk Averse against all incident, alert consolidation from various channels [XDR, DLP, IDS, Etc..]		
40	Proposed solution should also provide preliminary incident response activities / checklist for Analysts to refer and adhere to the best practices		
41	Proposed Solution should allow analysts to do quick Impact analysis of the incidents and record the same		
42	Proposed solution should allow SOC Stakeholders to define the policies & SLA and Measure them on ongoing basis		
43	The proposed solution must be able to execute automated corrective or follow-on actions via scripted alerts		

S.No	High level technical specifications	Bidder Compliance	Deviation
	Dashboard and reports		
1	The dashboard should be a unified web based online portal and provide collaboration for the following		
	i. SIEM events/incidents related alerts, log stoppage alerts, monthly summary reports and analysis.		
	ii. Threat advisory alerts relevant to assets being monitored with feeds from VA tool.		
	iii. Dashboard should be customizable as per the individual user business need		
2	The portal should allow users to view alerts/incidents triggered		
3	The portal should make use of qualified security event and incident alerts raised from SIEM into useful periodic reports (weekly, monthly basis) and analysis. These reports should be available for view or download.		
4	The portal should provide a summary of log stoppage alerts and automatic suppression of alerts.		
5	The portal should also allow users to initiate and track alert related mitigation action items. The portal should allow reports to be generated on pending mitigation activities based on ageing analysis		
6	The portal should also provide 360* view of assets i.e. Asset Properties, events & incidents, vulnerabilities and issue mitigation tracking mappable to individual assets/users.		
7	The portal also should provide knowledge base and best practices for various security vulnerabilities		
8	Reports should be consolidated in an integrated online dashboard		
9	Proposed Solution should have Executive dashboard depicting the business aspects of SOC dashboards to Analysts Level Dashboards		
10	Should measure the Key Performance Indicators of the Security Operation centre and depict the same on the dashboard		
11	There should be a feature to create any kind of report from any of the available data from the feeds like top incidents by application, by hosts, users etc.		

S.No	High level technical specifications	Bidder Compliance	Deviation
12	Bidder should design report format for management reporting including heat maps, executive scorecards for top management that covers security performance of different business units, compliance, asset status		
13	Dashboard should display asset list and capture details including name, location, owner, value, business unit, IP address, platform details etc		
14	Dashboard should capture the security status of assets and highlight risk level for each asset. The asset status & risk scores should be consolidated at a higher level to report on overall security status of Bank, status of different business units within the Bank, status of key locations		
15	Dashboards should have a graphical display of asset security status based on locations, business units. Graphical display should support different methods of representing information including bar charts, pie charts, line charts as relevant to the information that is represented. Dashboard should support drill down graphs to click and move to the level of individual assets		
16	Dashboard should capture risks in each asset. Dashboard should have the provision to click on the asset and track mitigation status corresponding to risks		
17	Dashboard should support reporting and provide out of the box templates for relevant compliance across all major standards and regulatory requirements. This includes ISO 27001, BS25999, ISO 20000, RBI regulations, IT ACT, PCI DSS standards, SOX etc		
18	Dashboard should support different views relevant for different stakeholders including top management, operations team, Information Security Department		
19	Dashboard/report should support export of data to multiple formats including CSV, XML, Excel, PDF, word formats		
20	Dashboard should be Capable of Distributed viewing as well as single consolidated viewing and delegation of user rights across devices and access to individual components of the application.		

S.No	High level technical specifications	Bidder Compliance	Deviation
21	Ability to provide an intuitive user interface with features such as display correlated events, unlimited drill down to packet level event details, simultaneous access to real-time, raw logs and historical events, customizable at-a-glance security view for administrators. The drill down should be directly from the dashboard using a single mouse click		
22	The dashboard should display the security status of IT infrastructure in the Bank. Dashboard should have graphical display of asset status based on locations, business units etc		
23	Compliance to SLA should be captured in the dashboard		
24	The system should have a facility to view Summary of all Dashboard views for the entire enterprise.		
25	The system should permit setting up geographical maps/images on real time dashboards as a placeholder for alerts.		
26	The solution should allow creating reports from the rules provided by bidder or created by administrator		
27	The solution should provide both tabular and graphical reports		
28	The solution should allow adding custom content to the report like headers, footers, table of content, notes etc.		
29	The solution should allow creating consolidating multiple reports in a single report.		
30	The system should allow scheduling reports		
31	The system should provide a calendar view. Clicking on a date should show all reports generated on the selected date		
32	The solution must provide a flexible dashboard with chart and summary displays for a complete view of real-time captured data.		
33	The solution must be able to schedule reports and also provide the flexibility to generate on-demand reports.		
34	The solution must provide fully customizable queries and report library to define report and alert combinations		
35	The solution shall have a flexible, drag-and-drop report builder and scheduling engine.		
36	The solution must have graphical analytical capability on the objects that		

S.No	High level technical specifications	Bidder Compliance	Deviation
	were captured in the network traffic.		
37	The solution must support direct drill-down from the reports and charts to the underlying session traffic. The solution must provide drill down functionality that is user defined, allowing users to drill down into another report, dashboard, raw events or passing URL parameters to any third-party website. The Report should be scalable IP-wise, device-wise, user-wise, data-wise, location-wise based on requirement between any two dates.		
38	The system shall allow custom dashboards for real time alerts, reports etc		
39	Create chart rules, schedule and view dynamic charts in time and summary series format.		
40	Reports can be scheduled in a dynamic fashion with schedule windowing and prioritisation to improve run priority of high value scheduled reports and manage concurrently running reports to meet the requirements of completing reports under 24 hours. The report should be parameterized, and the user should be able to scale the parameter as needed. And Out of box ageing analysis of incidents should be available.		
41	The solution's reports should run fast on large data sets. Proposed solution should use next generation functionalities like creating a set of data from the main index or data store. This will avoid running the queries on large index or full index and faster response for searching and reporting.		
42	The system should provide capabilities to run both ad hoc and standardised reports for operational and trending metrics.		
43	The proposed solution must have a user-friendly interface to convert statistical results to dashboards with a single click. The Dashboard should be accessible from the endpoints as & when required.		
44	The proposed solution must provide the following capabilities as a Security Analytics Platform:		
	a. One single syntax that can be used universally for search queries, alerts, reports or dashboards.		

S.No	High level technical specifications	Bidder Compliance	Deviation
	b. Incident management technique to facilitate incident tracking, investigation, pivoting and closure		
	c. Risk management technique to apply risk scores to any asset or user based on asset inventory scoring		
45	The Solution must provide the ability to have multiple, detached, dashboards that provide quick access to a wide variety of security management metrics.		
46	The Solution must provide multiple out-of-the-box dashboards to provide default views for specific roles including: security, compliance, and management. Additionally, users should be able to easily create their own dashboards suited to their responsibilities.		
47	The Solution must support a flexible dashboard environment that allows users to leverage saved searches and views that can easily be deployed as an alert/report in case of need.		
48	System should provide for watch list feature to enable the user to populate the list based on various parameters like IP Address, URL etc		
49	The solution should provide flexible dashboard interface customised to individual user preferences allowing the examination of a specific event or a holistic view of the systems within the enterprise		
	Forensics		
1	The GUI based data export capability should be present in standard formats such as XML, JSON, etc which can be used by the ML libraries/tools. .		
2	The proposed solution empowered with machine learning capabilities must include API access, role-based access controls for machine learning models.		
3	The proposed solution machine learning capabilities must allow addition of custom machine learning algorithms from popular open source libraries like NLP, Python etc. (Same as 5)		
4	The proposed solution should natively have ML capabilities and should not have separate engine/compute requirements for running ML models.		

S.No	High level technical specifications	Bidder Compliance	Deviation
5	The SIEM Solution should write logs in tamper proof manner. Once the logs are written no one should be able to modify/tamper/delete the stored logs till correlation and archival of the same.		
6	There should be No parting of logs, or filtering of logs at any stages of log collection or log storage. Log collection process should satisfy the needs of Regulatory compliance, forensic evidence gathering and data retention policy.		
7	Bidder must collect and store log information in a manner that preserves litigation quality for use in legal proceedings without increasing storage requirements.		
8	The solution shall ensure the integrity of the data events against inadvertent changes. At a minimum, the Bidder solution shall be able to identify that stored data events have been altered, removed, or had events inserted.		
9	The solution shall include the ability to specify when data events are deleted. This ability shall include the capability of specifying different retention Periods for different services and sources of data events.		
10	The solution shall have the capability of readily (1) identifying data events that meet all of the criteria of (1a) received on or after a specified date and time, (1b) received before a second specified date and time, (1c) received from any of a list of sources, and (1d) are for any of a list of services; (2) electronically exporting those events; and (3) providing audit trail and chain-of- custody information for evidential and forensic purposes. Specify the process followed; the options for exporting, including how large numbers of data events are handled; and what audit trail and chain-of-custody information is available:		
11	Ability to gather actional IOC based on the organization vertical/Geo and then run automated searches for related indicators of compromise across different datastores in the organization like SIEM, EDR, NDR, Data lake etc		
Administration and Support			
1	The system should allow centralised management and reporting for		

S.No	High level technical specifications	Bidder Compliance	Deviation
	various components from central site		
2	The system should allow centralised system updates for application & its components.		
3	The system should have an interface to monitor the health of the various components of the solution and provide details like CPU usage, interface usage, disk status etc.		
4	The system should not restrict/limit concurrent logins.		
5	The system should audit all changes made to the system. Alerts and reports are to be generated for the changes made at system level		
6	The solution should be completely web based		
7	Technical Support should be available through OEM or the registered partners of OEM. Please specify the proposed Technical Support framework to be provided to the Bank.		
8	OEM certified onsite engineer should be available in office hours and available over call in non-office hours in case of any technical issues		
9	The system shall provide configurable automated actions in response to security problems. The same shall be sent as E-mail Notifications, SMTP notification, SYSLOG notification, SNMP Notifications to operators		
User and Entity Behavior Analytics			
1	Proposed SIEM solution shall have the inbuilt capability to perform UEBA.		
2	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.		
3	Assess frequency of assets such as User's volume of activity suddenly spikes or access to number of assets increases rapidly		
4	Usage deviates from peer group such as User pattern of activity starts deviating from the peer group		
5	Change in account privileges such as User attempts to change privileges on existing account or open new accounts on other systems		

S.No	High level technical specifications	Bidder Compliance	Deviation
6	Application misuse by sequence of actions: User performs a sequence of actions which no other user is performing		
7	Dynamic adjustment of risk scores such as Dynamically adjust the risk score of rules when triggered against particular user or users		
8	UEBA should activate rules for a set of users until a specified condition or specified time window.		
9	Solution should leverage Machine learning to perform analytics to gain additional insight into user behavior with predictive modelling.		
10	UEBA 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		
11	The UEBA must be able to monitor all the users in the organization. UEBA should consume and operate on SIEM data repository.		
12	The UEBA must create a baseline of user activity by analyzing behavior. It should have multi dimensional baselining specific to users, devices etc., and automatically detect anomalous behavior from users, devices, and applications, combining those patterns into specific, actionable threats.		
13	The proposed solution should use unsupervised machine learning algorithms to analyze the data for activity deviating from normal behavior.		
14	The proposed solution should have threat detection technique and models to correlate series of violations and generate an incident that must be investigated. Threat detection models should stitch together events/anomalies to provide a high level incident. This shall be mapped to stages of MITRE framework / Cyber Kill Chain, etc		
15	Access & Authentication:		
	- Account used for the first time in a long time		
	- Rare privilege escalation		
	- Accounts being used from peculiar locations		

S.No	High level technical specifications	Bidder Compliance	Deviation
	- User involved in previously malicious or threatening behavior		
	- User an outlier within their peer group.		
	- Account accessing more high value assets than normal		
	- Privileged account accessing high-value servers from a new location for the first time		
	- Initial Access Followed by Suspicious Activity		
16	Exfiltration:		
	- Data Exfiltration by Print		
	- Data Exfiltration by Removable Media		
	- Large Outbound Transfer by High Risk User		
	- Multiple Blocked File Transfers Followed by a File Transfer		
17	Browsing Behaviour:		
	- Accessing new website		
	- Repeatedly attempting to access blocked website		
	- Access to Domain categories such as Blacklist/DGA/Tunnelling etc.,		
18	Geography Based:		
	- User Access from Multiple Locations		
	- User Geography Change		
	- Access from Unusual Locations		
	- Time Based		

S.No	High level technical specifications	Bidder Compliance	Deviation
	- Access during unusual timings based on past history		
	Network Behaviour Analysis		
1	Proposed SIEM solution shall have the inbuilt capability to perform Network Behavior/Traffic Analysis for anomaly detection		
2	Timebased learning and alert deviations		
3	NBA UI/panel should be integrated in SIEM dashboard. Thus, which will help in monitor desired elements of network behaviors, risks and trends from a single screen		
4	Alert deviation in network utilisation - More data being transferred than a normal to and from servers and / or external location		
5	Solution should leverage Machine learning to perform analytics to gain additional insight into user behavior with predictive modelling.		
6	Large outbound transfer		
7	Access high-value assets such as User starts accessing and downloading high-value assets with increased frequency.		
8	Application misuse by malware or bots such as A bot or malware attacks an application or exfiltrates data		
9	The solution must dynamically learn behavior and alert anomalies		
10	The solution must support traffic profiling based on IP addresses, groups of IP addresses, source/destination IP pairs etc.		
11	Solution must support Netflow, JFlow, SFLow , IPFix collection and correlation.		
12	The solution must display traffic profiles in terms of packet rate, in multiple timeframes - daily/weekly/monthly		
13	The solution must detect denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks.		
14	The solution must display visual traffic profiles in terms of bytes, packet rates and number of hosts communicating. These displays must be available for applications, ports, protocols, threats and each monitoring		

S.No	High level technical specifications	Bidder Compliance	Deviation
	point in the network. All of these views must support network location specific view such that they can present information from a single location, the entire network or any other defined grouping of hosts.		
15	The solution must support application definition beyond protocol and port. The system must support the identification of applications using ports other than the well-known, and applications tunneling themselves on other ports (e.g., HTTP as transport for MS-Instant Messenger should be detected as Instant messenger - not HTTP).		
16	The solution must be able to profile communication originating from or destined to the internet by Geographic regions in real-time.		
17	The solution must allow the user to create custom profiles and views using any property of a flow, log, data source or already profiled traffic.		
18	The solution must be able to detect suspicious communication channels, traffic over non standard ports		
19	The SIEM must correlate/stitch log events and network flows into single incident.		
20	The SIEM must identify certain protocols that need to be monitored and controlled, such as TOR, telnet, ftp, p2p.		
21	The SIEM must have the ability to generate reports on flows and events and to declare higher level aggregation of raw events into meaningful "Security Incidents" worth investigating.		
22	The Solution should have provision to import/deploy YARA rules, even from opensource such as github		
SOAR			
1	The solution must include a module, out-of-the-box, that provide incident response playbooks		
2	The solution must include out-of-the-box playbooks based on SANS and NIST for incidents like Malware , Phishing , DOS, IOC search, Threat Hunting etc., and should support creation of multiple playbook based on the SIEM Usecases.		
3	Solution should allow creating new playbooks to map out the Incident Response processes. There should be provision for building custom		

S.No	High level technical specifications	Bidder Compliance	Deviation
	playbooks within the solution.		
4	The solution must be able to provide incident response playbooks that consist of phases and tasks that guides the user on how to adequately respond to the incident; integrating people, processes and technology.		
5	The Proposed Solution should have out-of-the-box bi-directional integration with third party security/network solutions, to generate deeper insights into threats, orchestrate actions and automate responses.		
6	The proposed solution should have out-of-the-box provision for creation of incident from the SIEM automatically.		
7	Solution should offer below features for playbooks		
	- Support re-use of playbooks in bigger playbooks		
	- Allow creation of Manual Tasks, Automated Tasks and Conditional Tasks in Playbooks		
	- Allow a single playbook to have Automated and Manual Tasks within the same playbook.		
	- Allow a complete playbook to be run automatically or manually and list out any exceptions.		
	- Support step by step debugging of the running playbooks with provision of starting from where it stopped on error.		
	- Should record all manual and automated entries during execution of a playbook		
	- Should allow addition of adhoc tasks within a playbook		
	- Should support running playbooks as scheduled tasks at pre-defined time intervals		
8	Solution must support provision to pass parameters to upstream/downstream task within a playbook		
9	The solution must have an integrated versioning mechanism to save and maintain multiple versions for the playbooks.		

S.No	High level technical specifications	Bidder Compliance	Deviation
10	The solution should allow for viewing version history for all or selected playbook and provide option for restoring to an older version		
11	Solution should support updates for Playbooks, Integrations and should specify the procedure to update each of them		
12	The proposed solution should have out-of-the-box provision of closing incident simultaneously on SIEM and the proposed SOAR platform based on closure in ticketing platform.		
13	The proposed solution should have out-of-the-box capability to query or add IOC/Artefact to existing reference set of the deployed SIEM solution.		
14	The solution must be able to automatically extract email attachments from emails and store that for the related incidents as attachments.		
15	The solution must be able to support storing of incident related files not limited to malware specimens, logs, screenshots.		

Annexure E: Profile of onsite manpower at Cochin / Aluva

Administration

SIEM Admin	Qualification and Skills	B.E./B. Tech At least one security certification in Linux Operating System Advanced certification from SIEM OEM Minimum 2 years of experience in administration of SIEM solution. Person should have knowledge of security devices like Firewalls, IPS, Web Application Firewall, DDOS, XDR, Incident Response, SOAR, UEBA, NBAD, DAM, PAM, Deception, DLP, other security tools and other Operating Systems.
	Job Role	Administration & Operations of SIEM / Security devices / Solutions implemented at DC and DR System health monitoring. Point of contact for device issue resolution. Coordinate with OEM for device issues including hardware & software. Maintain knowledge base. Create and maintain all necessary documents/SOPs. Support integration of new devices/servers/applications to SIEM including log shipping, parsing, reviewing the monitoring requirements, and deploying necessary rules for alerts/incidents/reports. Performing periodic DR drills as per frequency defined by Bank. Take periodic backup like Configuration, Incidents etc and do restoration testing as per frequency defined by Bank. Patch the SIEM systems as and when required in case new updates are available and new vulnerabilities identified, if any. Scheduled activities. Any other activities assigned

Shift – General Shift on all Working days. Shall be available on non-working hours & holidays in case of exigency.

Operations

Level 1	Qualification and Skills	B.E./B. Tech At least one security certification such as CCNA-Security, CCSA, CEH etc. Minimum 2 years of experience in handling security related products & services and preferably 1 year in SIEM solution. Person should have knowledge of security devices like Firewalls, IPS, Web Application Firewall, DDOS, XDR, Incident Response, SOAR, UEBA, NBAD, DAM, PAM, Deception, DLP and other security tools. Knowledge of SIEM analysis Experience in 24X7 monitoring.
	Job Role	Incident detection, reporting and escalation. 24X7 monitoring of incidents/alerts and raise tickets. Report creation System health monitoring Operations of Security devices / solutions implemented at DC and DR Scheduled activities. Any other activities assigned

Level 2	Qualification and Skills	B.E. /B. Tech in Computer Science/ Electronics /ECE / EE / ECS / IT / MCA At least one SIEM solution certification. At least one security certifications such as CCSA/CEH/CompTIA/GCIH/GCIA Minimum overall 5 years of experience in handling security related products & services in a reputed organization out of which 3 years' experience should be in SIEM solution. Person should have adequate knowledge of Windows, Linux, Aix platforms and security devices like Firewalls, IPS, Web Application Firewall, DDOS, XDR, Incident Response, SOAR, UEBA, NBAD, DAM, PAM, Deception, DLP and other security tools. Administration of SIEM environment (eg: deployment of solution, user management, managing the licenses, upgrades and patch deployment, addition or deletion of log sources including custom applications, creating custom parsers, configuration management, change management, report management, manage backup and recovery etc) Construction of SIEM content required to produce Content Outputs (e.g., filters, active lists, correlation rules, reports, report templates, queries, trends, variables) Knowledge of networking protocols and technologies and network security Sound analytical and troubleshooting skills
	Job Role	Administration of SIEM & other security products Incident Validation Detailed analysis of attacks and Incident Response Point of contact for device issue resolution Administration and Management of Security devices / solutions implemented at DC and DR Identify missed incidents. Maintain knowledge base. Investigate logs/packets for anomalies and deploying necessary rules for alerts. Any other activities assigned.

Level 3	Qualification and Skills	B.E. /B. Tech in Computer Science/ Electronics /ECE / EE / ECS / IT Engineering/MCA At least two certifications in Security products/solutions with one in SIEM. At least one security certifications such as CCIE/CISSP/CISA/CCNP etc. Minimum 7 years of experience in handling security related products & services in an organization and out of total experience, 5 years of minimum experience should be as an L2 or above in SOC management. Person should have adequate knowledge of Windows, Linux, Aix platforms and security devices like Firewalls, IPS, WAF, DDOS, XDR, Incident Response, SOAR, UEBA, NBAD, DAM, PAM, Deception, DLP and other security tools. Administration of SIEM environment (eg: deployment of solution, user management, managing the licenses, upgrades and patch deployment, addition or deletion of log sources including custom applications, creating custom parsers, configuration management, change management, report management, manage backup and recovery etc) Construction of SIEM content required to produce Content Outputs (e.g., filters, active lists, correlation rules, reports, report templates, queries, trends, variables) Experience in, vulnerability management products and security/networking tools. Experience in setting up SOC processes, Threat Hunting, Packet Monitoring, Digital forensic investigation. Integration of customized threat intelligence content feeds provided by the Threat Intelligence & Analytics service. Sound analytical and troubleshooting skills. Good Team Management and co-ordination skills

	Job Role	Track Incident detection and reporting Incident closure & escalation Periodic review of usecases & identify new alert requirement based on industry best practices & changes in the environment. Ensure services are being provided within SLA parameters Ensuring logs are received in both DC & DR, Usecases deployed are same in DC & DR. Alerts/Incidents are handled in both DC & DR Identifies possible Root cause and fixes gaps to prevent recurring incidents. Collects/updates threat intelligence feeds from various sources. Conducts regular security briefings to the team. Follow-up with departments for closure of various reports/incidents and escalate the long outstanding issues. Investigate logs/packets for anomalies and deploying necessary rules for alerts. Identify log outages and submit necessary reports. Compare the trends of logs/alerts of security tools and submit necessary reports. Conduct the first level of forensic analysis in required cases and support expert agencies in required cases for intensive analysis. Coordinate overall SOC operations & Team management. Any other activities assigned.

Shift – Two L1 & One L2 in all shifts (3 shifts/day) on all days & One L3 in General Shift on all Working days.

Proper attendance system must be in place. If any resource proceeds on leave suitable substitute needs to be provided well in advance. The above is the minimum requirement and might increase in case of exigency.

Before deploying any resource, Bank has the right to assess his/her skills and retain the right to refuse. In case of any exigencies, Bank may call upon L3 resource on non-working days / Holidays or beyond working hours as per Business Requirement of the Bank.

On resignation, the resources must not be relieved unless replaced with resources having equivalent or higher qualification and experience with due approval from Bank.

Proper background check of the onsite support staff shall be conducted and BGV (background check verification) document shall be submitted regarding compliance of Education Qualification, Certification, Experience and Police Verification from HR at the time of Onboarding of resources to the Bank.

Annexure F: Commercial Bid Format

Segment	Item Name and Model No.	Total Cost
A) SIEM Solution Charges at DC & DR including Licensing, Installation, Configuration and Training Cost (With three-year warranty)		
B) SOC Operations Charges (5 Years)		
C) Annual Maintenance Charges 4th, 5th, 6th & 7th Years		
Grand Total		

S No	Item Description	Item Specification (Make/ Model/Capacity)	Qty	Rate (INR)	Total (INR) (Rate * Qty)
A	**SIEM Solution at DC & DR including Licensing, Installation, Configuration and Training cost (With 3 Year Warranty)**				
1	**Data Center**				
1	Collector with minimum 50000 EPS				
2	Log Management system				
3	SIEM Database system				
4	SIEM Correlation Engine				
5	SIEM Reporting System				
6	Storage for SIEM				
2	**DR Site**				
7	Collector with minimum 50000 EPS				

8	Log Management system								
9	SIEM Database system								
10	SIEM Correlation Engine								
11	SIEM Reporting System								
12	Storage for SIEM								
Sub Total (A)									
B	**SOC Operations**								
			Number of resources per day	Year 1	Year 2	Year 3	Year 4	Year 5	Total
1	**Administrator**	Administrators	2						
2	**Analyst**	SOC L1 Engineer	6						
		SOC L2 Engineer	4						
		SOC Manager	1						
Sub Total (B)									
C	**Annual Maintenance Charges**								
1	**DC**	4th Year AMC							
		5th Year AMC							

		6th Year AMC	
		7th Year AMC	
2	**DR**	4th Year AMC	
		5th Year AMC	
		6th Year AMC	
		7th Year AMC	
Sub Total (C)			

The prices quoted above should be exclusive of all taxes. Taxes is payable on actual basis.

Place:

Date: Seal & Signature of the Bidder

Annexure G: Compliance Certificate (On company's letterhead)

To,

The VP & CISO
Information Security Division
Integrated Risk Management Department,
Federal Bank Ltd, Federal Towers,
Aluva - 683101
Kerala, India.

Date:

Dear Sir/Madam,

Ref: RFP for Procurement of Security Operation Center Implementation

1. Having examined the Request for Proposal (RFP) including all annexures, the receipt of which is hereby duly acknowledged, we, the undersigned offer to provide the SIEM solutions and SOC operations in conformity with the terms and conditions of the said RFP and in accordance with our proposal and the schedule of Prices indicated in the Price Bid and made part of this bid. Any deviation may result in disqualification of our bid.

2. If our Bid is accepted, we undertake to complete the installation and commissioning of SIEM Solutions and SOC Operations within the scheduled timelines.

3. We confirm that this offer is valid for 8 weeks from the last date for submission of RFP to the Bank.

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

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

7. We have not been barred/black-listed by any regulatory / statutory authority in India and we have required approval, if any, to be appointed as a service provider.

8. We shall observe confidentiality of all the information passed on to us in course of the tendering process and shall not use the information for any other purpose than the current tender.

9. We confirm that we have obtained all necessary statutory and obligatory permission to carry out the implementation, if any.

Seal& Signature of the Bidder

Name:
Phone
No.:
Fax:
E-mail:

Annexure H: Manufacturer Authorization Format (On OEM's letter head)

Ref: Date:

To
The VP & CISO
Information Security Division
Integrated Risk Management Department,
Federal Bank Ltd, Federal Towers,
Aluva - 683101
Kerala, India.

Dear Sir/Madam,

Sub: Manufacturer Authorisation for RFP No. 1/2023/FBL/ISD dated 30/10/2023

We <OEM Name>having our registered office at <OEM Address>are an established and reputed manufacturer of <hardware details>do hereby authorise M/s_____(Name and address of the Partner) to offer their quotation, negotiate and conclude the contract with you against the above invitation for tender offer.

We hereby extend our full guarantee and warranty as per terms and conditions of the tender and the contract for the solution, products/equipment and services offered against this invitation for tender offer by the above firm and will extend technical support and updates / upgrades if contracted by the bidder.

We also confirm that we will ensure all product upgrades (including management software upgrades and new product feature releases) are provided by M/s for all the products quoted for and supplied to the Bank during the three year product warranty period.

<OEM Name**>**

<Authorised Signatory**>**

Name:
Designation:

Note: This letter of authority should be on the letterhead of the OEM and should be signed by a person competent and having the power of attorney to bind the manufacturer. It should be included by the bidder in its bid.

Annexure I: Undertaking of authenticity (to be signed by authority not lower than the Company Secretary of the Bidder)

Ref: Date:

To
The VP & CISO
Information Security Division
Integrated Risk Management Department,
Federal Bank Ltd, Federal Towers,
Aluva - 683101
Kerala, India

Dear Sir/Madam,

Sub: Undertaking of Authenticity for RFP No. 1/2023/FBL/ISD dated 30/10/2023

With reference to the SIEM Solutions and SOC Operations equipment quoted to you vide our quotation No.:_____ dated _____ in response to your tender no. 1/2023/FBL/ISD dated 30/10/2023, we hereby undertake that all the components / parts / assembly / software used in SIEM Solutions/other hardware items shall be original/ new from respective OEMs of the products and that no refurbished / duplicate / second hand components / parts / assembly / software are being used or shall be used.

We also undertake that in respect of licensed operating system if asked for by you in the purchase order, the same shall be supplied along with the authorised license certificate and also that it shall be sourced from the authorised source. Should you require, we hereby undertake to produce the certificate from our OEM supplier in support of above undertaking at the time of delivery/installation. It will be our responsibility to produce such letters from our OEM supplier's at the time of delivery or within a reasonable time.

In case of default and we are unable to comply with above at the time of delivery or during installation for the IT hardware / software already billed, we agree to take back the same, if already supplied and return

the money if any paid to us by you in this regard. We (Bidder name) also take full responsibility of both parts & service SLA as per the content even if there is any defect by our authorised service center / reseller / SI etc.

Authorised Signatory
Name
Designation
Place
Date

Annexure J: Power of Attorney (Executed on a non-judicial stamp paper)

BY THIS POWER OF ATTORNEY executed on _____, 2023, We _____, a Company incorporated under the Companies Act, 1956, having its Registered Office at (hereinafter _____ referred to as "the Company") doth hereby nominate, constitute and appoint <Name>, <Employee no.>, <Designation>of the Company, as its duly constituted Attorney, in the name and on behalf of the Company to do and execute any or all of the following acts, deeds, matters and things, namely :-

Execute and submit on behalf of the Company a Proposal and other papers /documents with 'The Federal Bank Limited' relating to 'Request for proposal no. 1/2023/FBL/ISD dated 30/10/2023 for purchase of SIEM Solutions and to attend meetings and hold discussions on behalf of the Company with Federal Bank in this regard.

THE COMPANY DOES hereby agree to ratify and confirm all whatsoever the attorney shall lawfully do or cause to be done under or by virtue of these presents including anything done after revocation hereof but prior to actual or express notice thereof being received by the person or persons for the time being dealing with the attorney hereunder.

IN WITNESS WHEREOF, has caused these presents to be executed by _____ _____on the day, month and year mentioned here in above.

For and on behalf of the Board of Directors of

_____

WITNESS:

Signature of _____

_____

Attested

_____

Annexure K: MUTUAL NON-DISCLOSURE AGREEMENT (On a Stamp paper)

This Non-Disclosure Agreement (the "Agreement") is entered into this _____, by and between;

THE FEDERAL BANK LIMITED, a Banking Company within the meaning of Companies Act, 2013 having its registered office at Federal Towers, Aluva – 683101, Kerala (hereinafter referred to as the "Federal Bank", which expression shall, unless repugnant to the context or meaning thereof, be deemed to mean and include its successors and assigns) of the ONE PART;

AND

_____., a company incorporated under the Companies Act, 1956 having its registered office at _____ hereinafter referred to as the "_____", which expression shall, unless repugnant to the context or meaning thereof, be deemed to mean and include its successors and permitted assigns, of the OTHER PART.

(The Federal Bank Ltd and _____shall hereinafter be referred individually as "Party" and collectively as "Parties")

WHEREAS, Federal Bank is a Bank interalia providing various financial services, promoting financial products, doing Banking business as permitted by the Banking Regulation Act,1949.

WHEREAS, _____ is engaged in the business of _____.

WHEREAS, _____ and Federal Bank are exploring the scope of entering into a contract for a mutually beneficial business association (hereinafter referred to as the "Transaction").

During the course of the Transaction, Federal Bank and _____may disclose to each other certain information which may be proprietary and/or of confidential nature as more particularly described below. The Party disclosing the Confidential Information is referred to as 'Disclosing Party' and the Party receiving the Confidential Information is referred to as 'Receiving Party'.

AND WHEREAS, in consideration of the disclosure of such Confidential Information to the Receiving Party by the Disclosing Party, Receiving Party agrees to keep the Confidential Information in strict confidential in accordance with

the terms and conditions set forth in this Agreement and undertakes not to disclose the Confidential Information to any individual/person/entity/ group of persons.

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS;

1. **EFFECTIVE DATE**

The effective date of this Agreement shall be the date of signing of this Agreement.

2. **DEFINITION OF CONFIDENTIAL INFORMATION**

The parties hereto agree that for the purposes of this agreement, the Confidential Information shall mean and include all documents, forms, papers, designs or other records and information in whatever form gathered and/or received by the Receiving Party in pursuance of its duties and such data, documents, material and information`, which are not available in the public domain and which shall include but not be limited to information relating to the products, Equipments, manuals, Instructions, software, customers, prospective customers, business plans, business opportunities, business ventures, strategic plans, finances, financial condition, projections, marketing strategies, programs, research, development, derivatives, copyrightable or copyrighted material, any translation, abridgment, revision or other form in which an existing work may be recast, transformed or adapted, patentable or patented material, any improvement thereon, material which is protected by trade secret, any new material derived from such existing trade secret material, including new material which may be protected by copyright, patent and/or trade secret, trademarks, trade names, designs, art work, or third party confidential information including information derived or developed on the basis of such information including any study material, analysis, notes, valuation etc., prepared by the Receiving Party in the process of the Transaction, in relation to the Disclosing Party, its subsidiaries, holding or associate companies or its affiliates or Business Partners whether or not explicitly designated as “Confidential Information” Disclosed or to be Disclosed by the Disclosing Party or the representatives of the Disclosing Party in any tangible form (including information transmitted in oral, written, electronic, magnetic or other form and also information transmitted visually or any other means) (here referred to as the “Confidential Information”).

1. NONDISCLOSURE AND NON-USE OF CONFIDENTIAL INFORMATION

The Receiving Party hereby agrees that the Confidential Information of the Disclosing Party will be used solely for the purpose of the Transaction and agrees and covenants that it shall not disclose, publish, or

disseminate Confidential Information to anyone other than the employees of the Receiving Party on a need to know basis, and Receiving Party agrees to take precautions which shall at all times be at least to the same extent the Receiving Party protects its own Confidential Information, to prevent any unauthorised use, disclosure, publication, or dissemination of Confidential Information. It shall be the responsibility of the Receiving Party to ensure that those employees who receive the Confidential Information on a need to know basis are bound by the confidentiality obligations mentioned herein.

The Receiving Party agrees to accept and use Confidential Information for the sole purpose of the Transaction and not for any third party's benefit. The Receiving Party agrees not to use Confidential Information without the prior written approval of the Disclosing Party or an authorised representative of the Disclosing Party in each instance. The Parties agree that if any disclosure of such Confidential Information is required to be made by the Receiving Party upon requisition by any Statutory Authority or any Court of Law, such a disclosure shall be upon prior notice to the Disclosing Party, to enable the Disclosing Party to take protective measures against such disclosure requirement.

2. OWNERSHIP OF CONFIDENTIAL INFORMATION

All Confidential Information disclosed by the Disclosing Party and any Derivatives thereof, created by the Disclosing Party, remains the property of the Disclosing Party; and no license or other rights whatsoever to Confidential Information is granted or implied hereby.

3. RETURN OF DOCUMENTS

Within seven business days of the written request of the Disclosing Party or upon termination or expiration of this Agreement, the Receiving Party will at the option of the Disclosing Party, return to the Disclosing Party or destroy and/or certify destruction of all documents and copies and other tangible objects thereof containing Confidential Information. For the purposes of this section, the term "documents and copies" includes all information fixed in any tangible medium of expression, in whatever form or format. Receiving Party also agrees to purge all copies of Confidential Information stored in electronic memories or media.

4. EQUITABLE RELIEF

The Receiving Party hereby acknowledges that unauthorised disclosure or use of Confidential Information could cause irreparable harm and significant injury to the Disclosing Party that may be difficult to ascertain.

Accordingly, Receiving Party agrees that the Disclosing Party will have the right to seek and obtain immediate injunctive relief to enforce obligations under this Agreement without prejudice to any other rights and remedies it may have in law or under this Agreement. The Receiving Party shall be liable for all loss, damages, expenses (including Advocates fee) incurred or suffered by the Disclosing Party as a result of the breach of this Agreement by the Receiving Party or its employees.

5. ENTIRE AGREEMENT

This Agreement constitutes the entire agreement with respect to the Confidential Information disclosed herein and supersedes all prior or contemporaneous oral or written agreements concerning such Confidential Information. This Agreement may not be amended except by the written agreement signed by authorised representatives of both parties. It is clearly agreed between the parties hereto that unless and until the parties hereto enter into a definitive agreement in respect of the transaction contemplated herein neither party shall be under any legal obligation of any kind whatsoever with respect to a transaction by virtue of this agreement except for the matters specifically agreed to herein.

6. NO WAIVER OF RIGHTS

It is understood and agreed that no failure or delay by the Disclosing Party in exercising any right, power or privilege hereunder shall operate as a waiver thereof, nor shall any single or partial exercise thereof preclude any other or further exercise thereof or the exercise of any right, power or privilege hereunder.

7. DISPUTE RESOLUTION

Any disputes or differences arising between the parties hereto from and out of any of the provisions of the agreement as to the construction, meaning or effect thereof or as to the rights or liabilities of the parties hereto, either during the term of this agreement or upon expiration thereof shall be settled amicably by mutual accord by the parties within 30 days from the date of such disputes.

8. GOVERNING LAW

This Agreement will be governed by and construed in accordance with the laws of the Republic of India. The Courts at ……. alone shall have jurisdiction to entertain and try all matters arising from and out of this agreement.

9. TERM

This Agreement shall remain in effect for a period of 10 years from the date hereof, provided that Receiving Party's duty to protect the Disclosing Party's Confidential Information shall survive expiration of termination of this Agreement.

10. TERMINATION AND CONSEQUENCES

Either party may terminate this Agreement at any time during the tenure without assigning any reason whatsoever.

Upon termination of this Agreement either by efflux of time or prior determination as provided herein above, the Receiving Party shall promptly upon the request of Disclosing Party, either return to Disclosing party or at the Disclosing party's option destroy all Confidential Information, as referred in Clause 5.

11. DISCLAIMERS

Neither this Agreement nor any disclosure of Information made under it grants the Receiving Party any right or license under any trademark, copyright or patent now or subsequently owned or controlled by the Disclosing Party, unless expressly agreed otherwise in writing.

12. ASSIGNMENT

The Receiving Party shall not have the right to assign or otherwise transfer, in whole or in part, any of its rights or obligations under this Agreement.

13. SEVERABILITY

If any condition, clause or provision of this Agreement is held or found by a court to be invalid, void, illegal or unenforceable, the remaining provisions shall remain in full force and effect.

14. SURVIVAL

The terms and provisions of this agreement that by their nature and contents are intended to survive the performance hereof by any or all the parties hereto shall so survive the completion and / or termination of this agreement.

15. RELATIONSHIP

This agreement shall not be construed to create any relationship either of employee/employer, joint venture, principal/agent, partnership/associate or any other relationship of a like nature between the parties hereto or between either party and the employees, agents and representatives of the other party.

16. NOTICES

All notices or other communications to be given or made under this Agreement shall be in writing, shall either be delivered personally or sent by courier, registered or certified mail or facsimile. The address for service of each Party and its facsimile number is set out under its name on the signing pages hereto. Without prejudice to the foregoing, a Party giving or making a notice or communication by facsimile shall promptly deliver a copy of such notice or communication personally, by courier or mail to the addressee of such notice or communication. Any Party may by notice change the addresses and/or addresses to which such notices and communications to it are to be delivered or mailed. Such change shall be effective when all the Parties have notice of it.

17. OTHER RIGHTS OF ACTION

The Parties acknowledge and agree that no provision of this Agreement shall prejudice or preclude a Party's rights to seek for injunctive or other equitable/specific relief, available to a Party. The Receiving Party agrees to waive any requirement for security or posting of any bond in connection with such remedy. Such remedy shall not be deemed to be the exclusive remedy for breach of this Agreement but shall be in addition to all other remedies available under Information Technology Act 2000 and other allied and applicable laws and further remedies at law or equity to the Disclosing Party.

18. HEADINGS

The headings used herein are inserted only as a matter of convenience and for reference and shall not affect the construction or interpretation of this Agreement.

The parties have caused this Agreement to be executed and do hereby warrant and represent that their respective signatory whose signature appears below has been and is on the date of the Agreement duly authorised by all necessary and appropriate action to execute this Agreement.

Signed for and on behalf of	Signed for and on behalf of
THE FEDERAL BANK LTD.	----------
Signature : _____	Signature: _____
Name : _____	Name: _____
Title : _____	Title : _____
Date : _____	Date : _____
Address :_____	Address :_____