Original RFP Specs	Clarification	Suggestion	ReBIT's Reply
Penalties will be applicable after 6 weeks, if the Delivery is still not completed. (Delivery shall be considered completed on the Confirmation of delivery of all items as per Purchase Order) A penalty of 1% per week for first two weeks, 2% per week for every subsequent week subject to a maximum of 10% of the total contract value. Penalty will be computed on the total one-time cost between the ReBIT and Bidder.	LD Penalty supposed to be on the value of goods not delivered on time.	Request to read clause as "Penalties will be applicable after 6 weeks, if the Delivery is still not completed. (Delivery shall be considered completed on the Confirmation of delivery of all items as per Purchase Order) A penalty of 1% per week for first two weeks, 2% per week for every subsequent week subject to a maximum of 10% of the total contract value. Penalty will be computed on the value of goods undelivered between the ReBIT and Bidder.	Hardware delivery changed to max of 8 weeks, please refer to the corrigendum
6 weeks from the date of Issue of Purchase Order	delivery time taken of material takes around 5-6 weeks. Post that Implementation would take atleast 10 weeks. Would request to provide more time for Installation and Operationalization	Request to read clause as "10 weeks from the date of delivery of material" or "16 weeks from the date of Issue of Purchase Order"	6 weeks from the date of ~~Issue of Purchase Order~~ completion of delivery of all the hardware Please refer to the corrigendum
The bidder should have experience in executing similar solutions in minimum2 PSBs / PSUs / BSE / NPCI /RBI/ Central Government organizations in India.	please include private organizations also.	Request to read clause as "The bidder should have experience in executing similar solutions in minimum 2 PSBs / PSUs / BSE / NPCI /RBI/ Central Government/Private organizations in India."	No change in this criteria
The selected Bidder shall give warranty for three (3) years from the date of acceptance of the systems by ReBIT. During the warranty period, the Bidder will have to undertake comprehensive maintenance of the Total Solution including hardware and software part of the solution.	Need clarification on this as in Point C of 4.8 on page no. 38. it is mentioned that "Even though ReBIT is requesting for 3 years TCO in commercial sheet, PO would be raised for licenses only on yearly basis"		No change in this criteria Explanation: 3+1 + 4 years of AMC renewal
The Initial AMC will be for a duration of 3 years with the Product warranty of 3 years and an additional year without the OEM product warranty. ReBIT may request for additional AMC of 4 years which will also need to cover the hardware as the OEM warranty has expired.	Need clarification on this as in Point C of 4.8 on page no. 38. it is mentioned that "Even though ReBIT is requesting for 3 years TCO in commercial sheet, PO would be raised for licenses only on yearly basis"		Explanation: 3+1 + 4 years of AMC renewal After Product warrant by OEM expires ReBIT will need AMC for the entire solution to keep it in operation even after expiry of the warranty.
Even though ReBIT is requesting for 3 years TCO in commercial sheet, PO would be raised for licenses only on yearly basis.	Need Clarification for how many years PO will be placed.		No change in this criteria
The Solution provider should provision separate solution for integrating Next Generation SIEM features like True Machine Learning, multi algorithm based User Entity Behaviour Analytics including additional Hardware, licensing, software and pricing, and any other detail deemed necessary. ReBIT will take final decision to procure and integrate this feature with the SIEM solution at any point of time within 1 year of Commercial opening with the same proposed cost in Indian Rupees.	Need Clarification.		We need True UEBA on a separate Hardware, decision to implement this UEBA may be taken as per ReBIT's convenience. If implemented within 1 years of commercial opening then the cost will remain the same as provided in the commercials.
The proposed OEM should have warehouse on its own/through partner in Mumbai/Thane/Navi Mumbai.	It is assumed that mentioned requirement is only applicable if appliance based solution is proposed by the OEM. Please confirm.	Request to remove this clause	No change in this criteria This criteria is for the hardware OEM, may or may not be the SIEM OEM as per the solution (e.g.. Dell server)
The vendor shall guarantee the availability of spares/Software for a period of at least Seven years in respect of all the equipment supplied by them, from date of Acceptance Test of the total solution.	It is assumed that mentioned requirement is only applicable if appliance based solution is proposed by the OEM. Please confirm.	Request to remove this clause	No change in this criteria This criteria is for the hardware OEM, may or may not be the SIEM OEM as per the solution (e.g.. Dell server)

Support for the integration (means collect, parse, normalize and use in co-relation rules, etc.) of Security Logs from the following Devices/application systems but not limited to (List the leading compatible OEM names):	Please provide the make and model details of all the Devices which need to be integrated with SIEM solution		Please specify if your Solution is NOT able to integrate successfully with any of the follows: Please specify if your Solution is able to integrate successfully with: Operating Systems (Windows 2003, 2008, 2012, Linux) Database - Oracle, MYSQL,SQL, etc. Anti-Virus Solution = Trend Micro, Symantec, Mcafee Internet Gateway Proxy = Trend Micro, Symantec, Mcafee Next Generation Firewall with IPS, Sandbox and Anti Malware engine = Checkpoint, Cisco, PalaAlto WAF Network Routers = Cisco, Extreme, Juniper Network Switches = Cisco, Extreme, Juniper Network access point and controllers = Cisco, Aruba, dlink Patch Management Solutions = wmi based, SCCM APC Rack PDU monitor Data Leakage Protection (DLP) solution = Mcafee, Symantec Mobile Application Management Solutions = IBM, Mobile Iron Directories (AD, LDAP) = Microsoft Email Gateway security solutions = Microsoft Mail exchange = Microsoft based Network Flows Vulnerability Scanners = Nessus, Microsoft Baseline Security Analyser (MBSA), Wireshark Application inspection MFA access control solutions and PIM = O365, Nexus Logs from Applications (in house applications, Internet Portal, etc.)
The SIEM should be able to integrate with ReBIT's Sandbox solutions for Antivirus, Next Generation Firewall, Proxy etc. The Sandbox may be on premises or Cloud based.	Please explain the use case of this integration		We have Sandboxes implemented for our other Security solutions, we need the security logs from them to be integrated with the SIEM. Sandbox emulates unknown suspected threat to give out correct results in case of malwares/infections.
The SIEM should have advance network log analysis capability to show activity inside the network. The solution should have diverse tool set that includes network discovery, flow data analysis, network metadata analysis, packet capture and analysis, and network forensic tools	It is assumed that network forensic tool requirement is related to capability to search raw logs. Please confirm the same.		The SIEM solution should have capability to analyse packet captured file generated from 3rd party solutions. Packet capture capabilities built-in the solution are optional. We do not need any add-on solution.

ReBIT to provide list of Security vendors currently deployed in ReBIT environment	Need Clarification.		Please specify if your Solution is NOT able to integrate successfully with any of the follows: Please specify if your Solution is able to integrate successfully with: Operating Systems (Windows 2003, 2008, 2012, Linux) Database - Oracle, MYSQL,SQL, etc. Anti-Virus Solution = Trend Micro, Symantec, Mcafee Internet Gateway Proxy = Trend Micro, Symantec, Mcafee Next Generation Firewall with IPS, Sandbox and Anti Malware engine = Checkpoint, Cisco, PalaAlto WAF Network Routers = Cisco, Extreme, Juniper Network Switches = Cisco, Extreme, Juniper Network access point and controllers = Cisco, Aruba, dlink Patch Management Solutions = wmi based, SCCM APC Rack PDU monitor Data Leakage Protection (DLP) solution = Mcafee, Symantec Mobile Application Management Solutions = IBM, Mobile Iron Directories (AD, LDAP) = Microsoft Email Gateway security solutions = Microsoft Mail exchange = Microsoft based Network Flows Vulnerability Scanners = Nessus, Microsoft Baseline Security Analyser (MBSA), Wireshark Application inspection MFA access control solutions and PIM = O365, Nexus Logs from Applications (in house applications, Internet Portal, etc.)
What is the current ITSM vendor	Need Clarification.		Ticketing tool is sapphireims - https://www.sapphireims.com/
What is the number of concurrent analyst login into SOAR platform	Need Clarification.		Optimise, SOAR operation and management will be with the SI's SOC
Does the automatic reporting back to SIEM for example for closing cases state and the action needs to be audited	Need Clarification.		Integration with our existing Ticketing tool to generate al types of tickets
The Bidder should be Top Rating Classified Authorized Partner of the OEM (Original Equipment Manufacturer) at least for the last 3 years	Can this clause be re-Considered into Authorized partner.		Authorized Partner certificate from OEM is required
The bidder should have experience in executing similar solutions in minimum 2 PSBs / PSUs / BSE / NPCI / RBI/ Central Government organizations in India.	The similar solution means the onprem SIEM installation of proposed OEM. Is our understanding correct?		No change in this criteria On Prem SIEM of the partnered OEM and SIEM remote management & operations. Both these can be for different organizations- 2 Onprem SIEM deployment reference and 2 references for SIEM remote management and operations.
The solution provider should supply, install, commission, integrate and operate the Security Information and Event Management (SIEM) solution with all required accessories hardware and software.	Please share location of installation, DC and DR. As per our understanding ReBIT DC is onprem at Vashi office and there is on DR. The installation will happen at Vashi office. Is our understanding correct?		Only one office, both the Pri and Sec will be placed in the same server room: Reserve Bank Information Technology Pvt. Ltd (ReBIT), “Mindspace Juinagar”, Plot Nos. Gen 2/1/D, Gen 2/1/E & Gen 2/1/F, TTC Industrial Area, Juinagar, Navi Mumbai 400706.

The Solution provider should provision for a separate solution for integrating Next Generation SIEM features like Security Orchestration and Response including additional Hardware, licensing, software and pricing, and any other detail deemed necessary. ReBIT will take final decision to procure and integrate this feature with the SIEM solution at any point of time within 1 year of Commercial opening with the same proposed cost in Indian Rupees.	Can we propose SOAR of OEM other than SIEM OEM? Will SOAR price be considered in TCO?		SOAR can be through any OEM but it should get integrated with the SIEM. If ReBIT considers to procure SOAR at the time of SIEM implementation then SOAR costing will be considered in the commercials.
The bidder should allow yearly Audit for the ReBIT's SIEM solution and its remotely managed SIEM management and Operation Services and/or provide latest external Audit reports like SSAE 18, SOC1, SOC 2, etc.	Can we provide ISO 27001 Audit report of our SOC?		ISO 27001 is ok for now, however if we feel that the audit is not satisfactory ReBIT will conduct its own Audit for our SIEM management and Operations at your SOC
The OEM should provide 5 working days of "Business requirement mapping and use case building" specific to ReBIT with all the documentation, test results and future use case building process, workflow and SOP to the bidder's Operation team and ReBIT for future enhancements.	Please clarify your expectation. Will this engagement be on demand and in multiple instances with total effort of 5 days? Can we optimize this with Bidder's effort and OEM supporting to bidder remotely? Suggest ReBIT to include this in commercial format to be reflected in TCO.		No change in this criteria: SIEM only This specialised effort is needed from the OEM's SIEM expert - and should create a foundation for all the future SIEM use case creation. Mandatory from ReBIT office, Bidder's team may be in co-ordination with the expert remotely or onsite.
Installation and Operationalization: 6 weeks from the date of Issue of Purchase Order	Request to increase this to 10 weeks to be realistic.		6 weeks from the date of ~~Issue of Purchase Order~~ completion of delivery of all the hardware Please refer to the corrigendum
In case ReBIT's EPS consumption falls below the proposed base EPS requirement then the billing/licensing needs to be reduced in proportion to the costing provided. An EPS review will be completed before the Project signoff.	Please clarify your expectation. We will consider 1000 EPS including peak requirement as per RFP ask. This can not be reduced once billing is done.		The EPS count review will be performed at the time of EPS License renewal factoring in EPS increment and optimization
The Solution provider should provision separate solution for integrating Next Generation SIEM features like True Machine Learning, multi algorithm based User Entity Behaviour Analytics including additional Hardware, licensing, software and pricing, and any other detail deemed necessary. ReBIT will take final decision to procure and integrate this feature with the SIEM solution at any point of time within 1 year of Commercial opening with the same proposed cost in Indian Rupees.	UEBA can be deployed on the SIEM tool itself however to get benefit with features like ML along with UBA, it is suggested to deploy it in a different server. Please let us know your expectations. Will UEBA price be considered in TCO?		Standalone UEBA with separate hardware needs to be quoted in the solution. UEBA can be through any OEM but it should get integrated with the SIEM. If ReBIT considers to procure UEBA at the time of SIEM implementation then UEBA costing will be considered in the commercials.
The OEM's have to give the certificate to ReBIT 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.	Software based SIEM solution deployed on ReBIT infrastructure (VM) will be cost effective option, we can also consider appliance based if ReBIT requires to do so. Please let us know your expectation.		No change in this criteria: ReBIT needs Onprem Solution including Hardware from SI, the OS and the SIEM
The Solution should have capability of providing Forensics capability	PCAP is generally used for incident forensic analysis purpose and this is an add on module/license with appliance option. Do we consider PCAP from day one? If yes, please share bandwidth details to size it.		Basic Pcap analysis feature is needed if the pcap file is provided.
The Solution should support analysis of packet capture files like pcap	PCAP is generally used for incident forensic analysis purpose and this is an add on module/license with appliance option. Do we consider PCAP from day one? If yes, please share bandwidth details to size it.		Basic Pcap analysis feature is needed if the pcap file is provided.

The SIEM should have advance network log analysis capability to show activity inside the network. The solution should have diverse tool set that includes network discovery, flow data analysis, network metadata analysis, packet capture and analysis, and network forensic tools	Advance network analysis requires NBAD feature to collect network flow record and Forensic also requires add on module. Do we consider NBAD from day one?		Basic Netflow without a dedicated NBAD
After completion of warranty period, bidder has to give Comprehensive Annual Maintenance Service Contract (AMC) for at least four years. The Initial AMC will be for a duration of 3 years with the Product warranty of 3 years and an additional year without the OEM product warranty. ReBIT may request for additional AMC of 4 years which will also need to cover the hardware as the OEM warranty has expired.	Request bank to clarify if the AMC for 4 years is required after the expiry of the warranty of the OEM.		3+1 + (4) 4 years AMC which includes 3 years OEM warranty and then 1 years of AMC without OEM warranty. After the initial 4 Years (above) ReBIT may request for additional 4 Years of AMC.
d. Payment towards Annual Maintenance cost will be made on annual basis. The invoice should be submitted at the end of the year with satisfaction report from the concerned users/owner of the Project.	Request Bank to release the payment on quarterly advance basis		No change in this criteria.
e. Payment towards SIEM Management and Operation service cost will be made on quarterly basis. The invoice should be submitted at the end of each quarter along with satisfaction report from the concerned users/owner of the Project.	Request Bank to release the payment on quarterly advance basis		No change in this criteria.
The OEM's SIEM solution should be categorized a Leader as per global IT rating methodology & research such as Gartner Magic Quadrant or Forrester Wave or equivalent in their latest report.	Can we propose SIEM solutions which are also in Challenger's quadrant? Also, are we allowed to propose "Make In India" products which are not in Gartner or Forrester report	1. Customer to change the clause from Leaders to Leaders / Challengers. 2. Customer to confirm if they would want to consider a Make In India Product if it is not listed in the Gartner.	No change in this criteria.
The technical evaluation will be based on the extent to which Vendor's proposal fulfils ReBIT's requirements as stated in the Technical_Specification_SIEM workbook that will be provided to the interested parties.		Customer to share the Technical_Specification_SIEM workbook	Workbook provided
OEM should bid for latest model with latest specifications as per requirements stated in the Technical_Specification_SIEM workbook		Customer to share the Technical_Specification_SIEM workbook	Workbook provided
Interlinks between the devices should be on 1G ports and there should be resiliency between the devices. All possible high availability scenarios should be considered & tested.	Please suggest at which layer (collection, logging, correlation) is HA expected. Is HA expected at DR as well		Only one office with no DR, both the Pri and Sec will be placed in the same Server room. All hardware need to have dual power supply
The Solution provider will deploy and validate all the features in the SIEM solution including (but not limiting to) co-relation, use cases, Threat Intelligence Integration, User behaviour analysis, Integration with Ticketing tools, Dashboard setup and Report Customization, etc.	Please suggest the current ticketing tool with which the SIEM solution needs to be integrated with		current Ticketing tool is sapphireims - https://www.sapphireims.com/
The Solution provider will deploy and validate all the features in the SIEM solution including (but not limiting to) co-relation, use cases, Threat Intelligence Integration, User behaviour analysis, Integration with Ticketing tools, Dashboard setup and Report Customization, etc.	Please confirm if separate UEBA solution with agent deployment is required or the native UEBA features of SIEM are sufficient		Standalone UEBA with separate hardware needs to be quoted in the solution. UEBA can be through any OEM but it should get integrated with the SIEM. If ReBIT considers to procure UEBA at the time of SIEM implementation then UEBA costing will be considered in the commercials. If the UEBA needs an agent installation we can go ahead with it.
The bidder should be able to provide remote 24x7x365days Security Operation and management Services for this solution for a duration of 3 years from the date of SIEM Solution Sign Off.	Where are the resources to be deployed?		Remotely at bidder's SOC Incase of outage no remote session will be provided, SI's engineer needs to be present onsite to investigate and fix the issue.

	Who will provide the hardware for SIEM solution ?		Bidder needs to provide Hardware, SIEM and the SIEM monitoring, management and the operations services
In the event of delay in stage wise execution of work, specified in this Contract / furnishing deliverables due to negligence or in-efficiency attributable to the selected bidder, the selected bidder shall be liable to a penalty up to a maximum of 10% (ten percent) of the contract value.	Please CAP it to 5%	Please CAP it to 5%	No change in this criteria.
Delivery of hardware and software at all sites - 6 weeks from the date of Issue of Purchase Order Penalties will be applicable after 6 weeks, if the Delivery is still not completed. (Delivery shall be considered completed on the Confirmation of delivery of all items as per Purchase Order) A penalty of 1% per week for first two weeks, 2% per week for every subsequent week subject to a maximum of 10% of the total contract value. Penalty will be computed on the total one-time cost between the ReBIT and Bidder.	Please CAP it to 5%	Please CAP it to 5%	No change in this criteria.
Installation and Operationalization 6 weeks from the date of Issue of Purchase Order Penalties will be applicable after 6 weeks, if the installation and Operationalization is still not completed. (Installation and operationalization shall be considered completed on the date of submission of all relevant installation documents) A penalty of 1% per week for first two weeks, 2% per week for every subsequent week subject to a maximum of 10%. Penalty will be computed on the total one time cost between the ReBIT and Bidder.	Please CAP it to 5%	Please CAP it to 5%	No change in the penalty %. Please refer tot the corrigendum for change in the timeline
availability Less than 99.5% Greater than or equal to 99.5% and less than 99.8% Greater than or equal to 99.8% and less than 99.9% Downtime More than 219 minutes Greater than 88 Minutes but less than 219 minutes Greater than 44 Minutes but less than 88 minutes Penalty 5% of total annual value for the measurement period up to 10% of Annual Amount payable 3% of total Annual value for the measurement period up to 10% of Annual Amount payable 2% of total Annual value for the measurement period up to 10% of Annual Amount payable	Please CAP it to 5%	Please CAP it to 5%	No change in this criteria.
The maximum penalty during a measurement or invoicing period will be capped to 10% of total invoicing value during that measurement or invoicing period	Please CAP it to 5%	Please CAP it to 5%	No change in this criteria.
Eighty percentage (80%) of the Total cost of Bill of material will be released on delivery, successful installation and operation of the total solution in ReBIT. This would also include signing the User Acceptance Test (UAT) document and Service Level Agreement (SLA)/Purchase Agreement by ReBIT and Implementation certificate. b. Twenty percentage (20%) of the Total cost of Bill of material will be released after one month on completion of Project Sign Off.	What would be the signing off period		Once implementation, UAT, and documentation is completed successfully
Payment towards SIEM Management and Operation service cost will be made on quarterly basis.	Payments to be Quarterly in Advance	Payments to be Quarterly in Advance	No change in this criteria.
Payment towards Annual Maintenance cost will be made on annual basis. The invoice should be submitted at the end of the year with satisfaction report from the concerned users/owner of the Project. E	Payments to be Yearly in Advance	Payments to be Yearly in Advance	No change in this criteria.

The bidder should be able to provide remote 24x7x365days Security Operation and management Services for this solution for a duration of 3 years from the date of SIEM Solution Sign Off. The Security Operation and management Service will include, but not limited to, real time monitoring of all security events, all security operations through this SIEM, its maintenance, upgradation, reporting, dashboard presentation, highlight risk, suggest improvements, monthly review meeting, quarter ending review meeting with ReBIT onsite , compliance, auditing, forensics, assisting in incident response, etc. Details are available in the Technical_Specification_SIEM workbook.	What kind of audit RBI wants to conduct here?		Operational & Security Auditing of our solution and its allied resources.
The Bidder selected as the apparently successful Bidder will be expected to enter into a contract with ReBIT. If the selected Bidder fails to sign and return the contract within fifteen (15) business days of delivery of the final contract, ReBIT may elect to cancel the award and award the contract to the next-highest-ranked Bidder.	Does the contract open for negotiation?		No changes will be made in the contract
Each Party agrees to indemnify, and keep indemnified, the other Party, its directors and affiliates against any and all liability, loss, fines, penalties, fees, damages, costs, amounts and expense arising out of any obligations, claims (including third party claims), actions, suits, judgments, orders, litigations, enforcements and/or proceedings arising from breach by such Party of any material terms and conditions of this Agreement and/or its employees', personnel's, contractors, services providers' negligent acts, misconduct, commissions and/or omissions.	Indemnity must remain limited to losses or damages to tangible property, personal injury or death caused due to gross negligence or wilful misconduct.		No change in this criteria.
The Service Provider hereby undertakes to observe and perform at all times the applicable provisions of law and regulations in force for the time being and from time to time required to be observed and performed by the Service Provider for the proper observance and performance by it of its duties and obligations under and in accordance with this Agreement. The Service Provider hereby undertakes to indemnify and keep indemnified the Company from and against all direct and proven claims, actions or proceedings brought against it, losses, damages, fines or penalties imposed on the CLIENT or other liabilities suffered or incurred by the CLIENT, its directors or officers, as a consequence of any direct breach by the Service Provider of its obligations under this Agreement or any negligence on its part or its employees or agents under this Agreement.	Compliance with applicable laws should be made mutual in nature and each party should indemnify the other if it breaches any applicable laws.		No change in this criteria.
The limitation in clause 1.5 shall not extend to any legal injuries suffered by Client due to the Service Provider's a. Fraud, wilful misconduct or gross negligence; b. Breach of intellectual property with respect to third party claims; and	The bidder propose the following for limitation of liability: Bidder's liability will exclude any special, indirect, incidental, consequential damages including without limitation loss of profit, loss of revenue, loss of data, negligence, damage to data etc. For any liability not excluded by the foregoing and below section (i) Bidder's overall liability shall be limited to immediately preceding 12 months of charges collected by the Bidder under the order in which the liability has arisen. (I) Further Bank sole remedy and the Bidder sole liability for any service related matters shall remain limited to applicable liquidated damages/penalties imposed by Bank under this RFP.		No change in this criteria.

The limitation in clause 1.5 shall not extend to any legal injuries suffered by Client due to the Service Provider's a. Fraud, wilful misconduct or gross negligence; b. Breach of intellectual property with respect to third party claims; and	We request RBI that the Vendor's liability for infringement of intellectual property rights (IPR) should be limited i.e. "To the extent authorized, Vendor will pass through to RBI any transferable indemnities provided to the Vendor by Vendor's vendors, if any, including any indemnities for intellectual property infringement." As for the deliverables created by Vendor, its indemnity should remain capped to the immediately preceding 12 months of charges collected by Vendor under the order in which the liability has arisen. The Vendor will not be liable nor responsible for any infringement if such infringement is caused due to use of the product not intended by Vendor, modifications not made by Vendor, use of Vendor deliverable in conjunction with products not provided by Vendor, etc.		No change in this criteria.
The peak EPS (or equivalent normalised data per day or month) that the proposed solution can address without any additional license, server, storage or appliance should be minimum twice than the sustained EPS (or equivalent normalised data per day or month) proposed	No events should be dropped even if the license limit is exceed. During data burst scenarios like DDOS attack or malware outbreak huge logs are generated and hence we request ReBIT to make this specification mandatory. This will benefit ReBIT if this functionality is not available then most solutions disable functionalities and ReBIT will have no visibility.		No change in this criteria. All OEMs have different metering criteria so a knockout could not be specified. ReBIT will make sure that we get the burst capability and it carries a high weightage.
The proposed solution should be in the latest Gartner's Leader Quadrant or in the leaders section in the Forrester wave or equivalent global IT rating methodology & research. Please provide the Original report.	Most leading SIEM solutions are part of either Gartner leaders or challengers quadrant. Most of BFSI and public sector RFP's have considered both Leaders and Challengers. Solutions in Challengers quadrant also have proven track record and is being used by major BFSI's, Government, enterprises, Energy & Utilities etc. in India and world wide. We request ReBIT to please consider solutions in Gratner leaders or challengers quadrant.		No change in this criteria.
The Solution should support analysis of packet capture files like pcap	Packet Capture solutions are dedicated solutions which does packet capture and lot of other functionalities. We request ReBIT to ask for integration of proposed capture solution and ask for dedicated packet capture solution separately. As this only single specification will not give full functionalities of packet capture.		Basic pcap analysis feature is needed if the pcap file is provided.
High availability for the proposed SIEM solution itself with all its functions under normal operational conditions, both Primary and Secondary as on-premises solutions. Please specify the total number of physical appliances with the number of Virtual appliance built on them.	Is ReBIT looking for appliance based solution or software based solution installed on VM?		Every OEM has a unique solution architecture, please fit the best design to meet ReBIT's requirement including HA, EPS, storage, lookup time of queries, performance, etc. Hardware needs to be provided by the bidder.
High availability would be required at the log-collection layer and Broker (SIEM engine), both Primary and Secondary as on-premises solutions	Is ReBIT looking for High availability of log collection and log correlation layer in both locations? As most of the large organizations have gone ahead with HA at log collection layer to avoid single point of failure and Standalone correlation engine in DC and in DR. Logs will be dual forwarded to both correlation engines from collection layer in DC & DR. This will give near zero data loss and will solution up anytime in any Data Center and will reduce the total TCO. We request ReBIT to change it below for ReBIT's benefit: High availability would be required at the log-collection layer and Broker (SIEM engine), both Primary and Secondary as on-premises solutions		Every OEM has a unique solution architecture, please fit the best design to meet ReBIT's HA requirement - at least 2 physical servers/appliances, both will be placed in the same server room. If Primary setup goes down or malfunctions, entire SIEM should function through the Backup solution. All hardware needs to have dual Power supply feature.

In case of data burst beyond the peak EPS the SIEM should handle the additional data without dropping packets with a warning / alert	We assume packet should be read as logs. Please confirm.		logs
The solution should provide for custom parsers for integrating proprietary/custom applications. These parsers should be part of the solution and should be implemented by the OEM	Custom parsers are used for integration of unsupported devices and most of the RFP's ask for integration from SI. If SI is not able to build custom parser then OEM should support to build the same. We request ReBIT to change it to below: The solution should provide for custom parsers development kit for easily integrating proprietary/custom applications. These parsers should be part of the solution and should be implemented by the SI and if SI is not able to build parser then OEM should support building custom parsers.		SI can implement this in co-ordination with the OEM.
The Solution should support analysis of packet capture files like pcap			Basic Pcap analysis feature is needed if the pcap file is provided.
The solution must be capable of detecting patterns of activity that would otherwise go unnoticed over long duration that may go unnoticed by real time monitoring	Packet Capture solutions are dedicated solutions which does packet capture and lot of other functionalities. We request ReBIT to ask for integration of proposed capture solution and ask for dedicated packet capture solution separately. As this only single specification will not give full functionalities of packet capture.		This should be achieved through threat hunting and
The SIEM solution should have out of the box advance **user behaviour** analytic techniques for detecting malicious insiders, compromised accounts, user carelessness, etc.	ReBIT has asked for dedicated UEBA solution which will track such user behaviour. Is ReBIT looking for bi-directional integration of proposed UEBA solution?		Rule based UBA in this case
SIEM Solution should leverage big data infrastructure to handle the massive volume of events and data sources they process. Provide benchmark numbers showcase performance improvement	We would like to know what exactly ReBIT is looking for? Is ReBIT planning to build security big data lake in future? If yes then proposed SIEM solution should be able to consume logs from big data or push logs to big data. Please let us know the use case.		Only performance and underlying structure details are required. Provide benchmark numbers showcase performance improvement.
The SIEM should have ability to integrate with ReBIT's existing ITSM tool. Integration, testing and normal operation should be part of this SIEM solution	Which is the ITSM tool?		Current Ticketing tool is sapphireims - https://www.sapphireims.com/
The SIEM OEM should on its own or a partnered/acquisition third party solution be able to provide capabilities for providing True Machine Learning based multiple algorithm, advance UBA/UEBA capabilities. List out the hardware, software, ticketing tool, licensing, and other details deemed necessary for this UBA/UEBA.	We understand from the EOI that ReBIT is looking for dedicated UEBA solution. Analytics solutions are typically dedicated solutions. We request ReBIT to ask for dedicated UEBA solution as solution which some vendors have in SIEM has limited functionality on UEBA and this specs looks like specific to those vendor. We request ReBIT to add more technical specifications for UEBA.		We have used generic terms like "True Machine Learning based multiple algorithm, advance UBA/UEBA capabilities."

The UBA/UEBA should be able to profile user's IT behaviour, Risk rank them and be able to run ML based algorithms to identify Insider threat, Anomalies identification, careless user, Intellectual property theft, Data exfiltration, Account abuse, lateral movement, compromised user, Rare Events Model, Unusual Login, all these missed out in the normal correlation based rules.	We request ReBIT to has UEBA solution as entity plays a very very important role of assigning risk scores and to identify threats. We request to remove UBA/UEBA and put UEBA clearly as some vendors who have UBA solution on SIEM as just a add-on module will miss out entity and ReBIT will have no analytics done on entities and will miss out critical incidents.		No change in this criteria. "ability to run ML based algorithm**s**" "all these missed out in the normal correlation based rules" should safeguard ReBIT's requirement.
In case ReBIT's EPS consumption falls below the proposed base EPS requirement then the billing/licensing needs to be reduced in proportion to the costing provided. An EPS review will be completed before the Project signoff.	ReBIT has asked for SIEM solution as on-premise and license will be provided in the name of ReBIT. Hence Licenses will be provided as per ReBIT's ask. As reducing the licenses post implementation is not possible as OEM has to provide license based on the requirement of RFP.		This can be taken up at the time of EPS renewal after reviewing EPS optimization and EPS increase.
The OEM's should be involved in the overall implementation, support, sustenance, etc.	Is ReBIT looking for implementation from OEM? Scope of OEM in implementation is not clear. Request to please give clear understanding on OEM scope.		No change in the criteria Please refer to RFP 3.2.2 pg. 15 for OEM scope We need a basic overlook and assurance by the OEM in all the milestones. No onsite Service Manager effort is needed.
The OEM's have to give the certificate to ReBIT 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.	Is ReBIT looking for OEM validation for implementation done?		yes
The OEM should provide 5 working days of "Business requirement mapping and use case building" specific to ReBIT with all the documentation, test results and future use case building process, workflow and SOP to the bidder's Operation team and ReBIT for future enhancements. The OEM should make sure that this customization enhances the SIEM solutions capabilities and the solution is a success.	Implementation of use cases identified post Business requirement mapping will be done by bidder. Please confirm.		No change in this criteria: This specialised effort is needed from the OEM's SIEM expert - and should create a foundation for all the future SIEM use case creation. Mandatory from ReBIT office, Bidder's team may be in co-ordination with the expert remotely or onsite.
Sign off by Bidder and OEM for Go live of respective component.	As OEM is not implementing the solution; OEM will do the validation of implementation done by bidder. Hence OEM is not required for signoff. Please confirm.		No change in this criteria
OEMs shall provide support for their respective solutions during the implementation phase for: o Validation of solution design and architecture o Continuous monitoring of implementation. o Provide SME support to working teams. o Ensure customization is in line with ReBIT's requirements. o OEM sign off would be necessary after implementation of its products. o Yearly health check-up of the solutions implemented by the OEM. o Review of the Security Operation and management Service for the SIEM with Industry Best practices and highlight gaps to ReBIT and the bidder o The OEM should recognize the SOC services by the bidder as partner service and provide relevant documents or a declaration	Is ReBIT looking for Project Manager from OEM for monitoring of implementation? As monitoring can be only done if OEM is implementing the solution. OEM can guide bidder if they get stuck during implementation. Please clarify. As OEM is not implementing directly; then please let us know if OEM signoff is required. Please clarify and confirm. o Review of the Security Operation and management Service for the SIEM with Industry Best practices and highlight gaps to ReBIT and the bidder o The OEM should recognize the SOC services by the bidder as partner service and provide relevant documents or a declaration The above two services are not clear. Please clarify.		No change in this criteria: OEM should overview in every milestone of the project to oversee progress, delay, issues, optimization of their Product. OEM should recognize that the bidder has a Security Operations Center using their SIEM product, with privilege to the bidder's team in providing Support, licensing, hardware, expert advice, etc.

Solution should support Filtering on Collection, Log Management.	· SIEM's log collection solution should have an option to filter or choose logs at collection layer to govern flexibility to forward security related events and filter for example ARP notifications from switches, routers etc....as they increase the EPS; which in-turn bring an impact log size and required storage + server cost significantly. On an average filtering can help reduce the logs to up-to 30% and is recommended as these logs are of not any signification value from security incident monitoring perspective. Also Filtering should be available on the Log Management Layer.		OEM Specific criteria will not be included
Proposed solution should support bandwidth throttling on Collection layer.	The vendor's product must provide the ability to limit bandwidth used for transmitting event data from remote sites. This is very important feature as this may cause congestion when there is link failure and collectors send all the log data at one shot.		OEM Specific criteria will not be included
Caching at collection layer with multi-destination log forwarding (full redundancy)	Collection layer should be able to forward logs to multiple destinations(minimum 4) this will help bank to forward logs to other locations (full redundancy) without any additional configurations.		OEM Specific criteria will not be included
Stored logs should be hashed	SIEM should store logs in hashed – NIST compliance and no modification should be allowed by the SIEM. This help during audits or fraud investigations to confirm that data is not tempered by SIEM Admin managing/running the set-up.		OEM Specific criteria will not be included, point 26 covers this
Proposed Solution should have physical segregation of roles of Collector, Log Management and Correlation layer with some enhanced features of Log Management layer. Log Management solution should have separate UI for searching, reporting, basic dashboards etc. even if Correlation layer is down or not available. i.e. Logs should should be available for audit even if correlation is down.	This is very important feature as Correlation Layer is not available still bank can do collect logs, quick and fast search events, compliance reports etc. The searching should have google like search.		Every OEM has a unique solution architecture, please fit the best design to meet ReBIT's HA requirement - atleast 2 physical servers/appliances, both will be placed in the same server room. If Primary setup goes down or malfunctions, entire SIEM should function through the Backup solution. As the operation are with the bidder any faults in the design will impact their teams delivery SLA.
Proposed Solution should support forwarding of logs(raw or normalized) to any third party solution or to any big data platform like hadoop			Please specify in additional features
The bidder should have at least 3 certified Engineers who are having experience on the solution proposed	Are the certified engineers having experience in proposed OEM solution required or even other OEM solution is ok?		of the OEM solution that the bidder is partnering for
The solution provider should suggest the appropriate OS/IOS for all the supplied devices; the OS/IOS should be of N-1 version. All critical/major vulnerabilities known till the time of implementation should be remediated for the provided version or a risk sign-off taken from ReBIT.	Kindly elaborate this point .		The operation system and the SIEM solution on the Appliance or the Server should not have any vulnerabilities. A VA scan will be performed by ReBIT before go-live. Latest version of the operation system and the SIEM solution on the Appliance or the Server should not be of the latest ver if it was released within 6 months of the go-live.

Interlinks between the devices should be on 1G ports and there should be resiliency between the devices. All possible high availability scenarios should be considered & tested.	Is this LAN interlink connectivity between Connector, logger & Correlation engine mentioned here? Are all the Logger & Correlation to be installed at ReBIT Juinagar office ?		LAN interlink, one office 1 Server room
The Solution provider should provision separate solution for integrating Next Generation SIEM features like True Machine Learning, multi algorithm based User Entity Behaviour Analytics including additional Hardware, licensing, software and pricing, and any other detail deemed necessary. ReBIT will take final decision to procure and integrate this feature with the SIEM solution at any point of time within 1 year of Commercial opening with the same proposed cost in Indian Rupees.	Is this separate solution to be quoted ?		Yes separate, there is a commercial bid template provided.
The Solution provider should provision for a separate solution for integrating Next Generation SIEM features like Security Orchestration and Response including additional Hardware, licensing, software and pricing, and any other detail deemed necessary. ReBIT will take final decision to procure and integrate this feature with the SIEM solution at any point of time within 1 year of Commercial opening with the same proposed cost in Indian Rupees.	Is this separate solution to be quoted ?		Yes separate, there is a commercial bid template provided.
	Please share list of devices to be considered under SIEM scope along with its location. The device details in format- Hostname, Device Type, Make, Model, Version, Device location.		operation system and the SIEM solution on the Appliance or the Server
	How much is the contract duration for?		3 years for the SIEM monitoring, management and operations
	Please share approx. EPS count to be considered for SIEM sizing		1000 on day one with bursting capability, scalable to 2500 in 5 years with the same hardware and software.
	What connectivity (MPLS/Internet) is available at ReBIT Juinagar office & whats the Bandwidth? Hope Perimeter Firewall can be used for building VPN with bidder?		Internet Leased Line with a NGFW
	Please clarify ReBIT will provide LAN Switch for connecting Connector, Logger & ESM engine?		ReBIT will provide all Generic LAN connection. Provide LAN connection details and any specialised need if any
	Is there existing SAN switch , Storage which can be reused ? Or is bidder to provide the same?		Log storage should be part of this solution, there is no sys log server at ReBIT.
The bidder should have experience in executing similar solutions in minimum 2 PSBs / PSUs / BSE / NPCI /RBI/ Central Government organizations in India.	We request to change the clause to "The bidder should have experience in executing similar solutions in atleast 1 PSBs / PSUs / BSE / NPCI /RBI/ Central Government organizations in India".		No change in this criteria.

The bidder should be able to provide remote 24x7x365days Security Operation and management Services for this solution for a duration of 3 years from the date of SIEM Solution Sign Off. The Security Operation and management Service will include, but not limited to, real time monitoring of all security events, all security operations through this SIEM, its maintenance, upgradation, reporting, dashboard presentation, highlight risk, suggest improvements, monthly review meeting, quarter ending review meeting with ReBIT onsite , compliance, auditing, forensics, assisting in incident response, etc. Details are available in the Technical_Specification_SIEM workbook.	Please confirm duration of contract period 3years or 5 years.		3 years
The Bidder shall provide detailed plan of the proposed staffing for the successful completion of the Works specified in the Proposal. Please indicate the number of proposed staff below and clearly identify personnel, if any, who would be dedicated for this Project.	Does REBIT needs a dedicated team of resources for SOC operations or bidder can propose for SOC operations and management from pool of existing resources.		We have left this open to the bidder however the bidder must ensure adherence to our service clause including limited access to their staff
Delivery of hardware and software at all sites - 6 weeks from the date of Issue of Purchase Order	We request to change the clause to "Delivery of hardware and software at all sites - 10 weeks from the date of Issue of Purchase Order".		Please refer to the corrigendum
Installation and Operationalization - 6 weeks from the date of Issue of Purchase Order	We request to change the clause to "Installation and Operationalization - 18 weeks from the date of Issue of Purchase Order"		Please refer to the corrigendum
	Will REBIT provide Hardware for installing software based SIEM solutions ? Will REBIT provide necessary operating system for installing software based SIEM solutions ?		All hardware and software need to be part of this solution.
	Will REBIT provide network connectivity from Bidder remote SOC till REBIT office ?		ILL with a NGFW, we will prefer creating a IP Sec Tunnel to your SOC
	Provide Site details where the solution will be implemented along with DC and DR		Only one office, both the Pri and Sec will be placed in the same server room: Reserve Bank Information Technology Pvt. Ltd (ReBIT), “Mindspace Juinagar”, Plot Nos. Gen 2/1/D, Gen 2/1/E & Gen 2/1/F, TTC Industrial Area, Juinagar, Navi Mumbai 400706.

	Provide details of Log sources along with count and versions for integrating with SIEM solution		Please specify if your Solution is NOT able to integrate successfully with any of the follows: Please specify if your Solution is able to integrate successfully with: Operating Systems (Windows 2003, 2008, 2012, Linux) Database - Oracle, MYSQL,SQL, etc. Anti-Virus Solution = Trend Micro, Symantec, Mcafee Internet Gateway Proxy = Trend Micro, Symantec, Mcafee Next Generation Firewall with IPS, Sandbox and Anti Malware engine = Checkpoint, Cisco, PaloAlto WAF Network Routers = Cisco, Extreme, Juniper Network Switches = Cisco, Extreme, Juniper Network access point and controllers = Cisco, Aruba, dlink Patch Management Solutions = wmi based, SCCM APC Rack PDU monitor Data Leakage Protection (DLP) solution = Mcafee, Symantec Mobile Application Management Solutions = IBM, Mobile Iron Directories (AD, LDAP) = Microsoft Email Gateway security solutions = Microsoft Mail exchange = Microsoft based Network Flows Vulnerability Scanners = Nessus, Microsoft Baseline Security Analyser (MBSA), Wireshark Application inspection MFA access control solutions and PIM = O365, Nexus Logs from Applications (in house applications, Internet Portal, etc.)
	Provide details of existing ITSM tool		Current Ticketing tool is sapphireims - https://www.sapphireims.com/

Please advise on the solution in used by ReBIT mentioned in 16c,j,k,s,u,v,w.			Please specify if your Solution is NOT able to integrate successfully with any of the follows: Please specify if your Solution is able to integrate successfully with: Operating Systems (Windows 2003, 2008, 2012, Linux) Database - Oracle, MYSQL,SQL, etc. Anti-Virus Solution = Trend Micro, Symantec, Mcafee Internet Gateway Proxy = Trend Micro, Symantec, Mcafee Next Generation Firewall with IPS, Sandbox and Anti Malware engine = Checkpoint, Cisco, PaloAlto WAF Network Routers = Cisco, Extreme, Juniper Network Switches = Cisco, Extreme, Juniper Network access point and controllers = Cisco, Aruba, dlink Patch Management Solutions = wmi based, SCCM APC Rack PDU monitor Data Leakage Protection (DLP) solution = Mcafee, Symantec Mobile Application Management Solutions = IBM, Mobile Iron Directories (AD, LDAP) = Microsoft Email Gateway security solutions = Microsoft Mail exchange = Microsoft based Network Flows Vulnerability Scanners = Nessus, Microsoft Baseline Security Analyser (MBSA), Wireshark Application inspection MFA access control solutions and PIM = O365, Nexus Logs from Applications (in house applications, Internet Portal, etc.)
What is the ITSM tool in used by ReBIT currently?			Current Ticketing tool is sapphireims - https://www.sapphireims.com/
Please provide details of the Threat Intelligence feed subscribe by ReBIT today.			We will provide this list to the winning bidders only or during the presentation
What is the ITSM tool in used by ReBIT currently?			Current Ticketing tool is sapphireims - https://www.sapphireims.com/
How many security events are the SOC analyst handling per day?			We do not have a SIEM right now, 1000 on day one with bursting capability, scalable to 2500 in 5 years with the same hardware and software.
How many users account will be monitored for UEBA?			110 from day one, scale to 250
The Earnest Money Deposit (EMD) may be forfeited: □ If a Bidder makes any statement or encloses any form which turns out to be false/incorrect at any time prior to signing of the contract □ If he/she withdraws/revokes his/her offer or modifies/changes the same during the validity of the Bid □ **In case of successful Bidder, if the Bidder fails to sign the contract within the specified date from the date of issuing the Letter of Acceptance** □ Failure to submit the Performance Bank Guarantee within the stipulated period makes the EMD liable for forfeiture. In such instance, ReBIT at its discretion may cancel the contract awarded to the selected Bidder without giving any notice □ Where the Bidder being technically qualified, withdraws the bid before the entire commercial evaluation process has been completed.	We hereby submit that in the event EIT is short listed as the successful Bidder, the contract to be entered into between the parties shall be a mutually accepted Agreement		No change in this criteria.

Delivery of hardware and software at all sites: A penalty of 1% week for first two weeks, 2% per week for every subsequent week subject to a maximum of 10% of the total contract value. Penalty will be computed on the total one-time cost between the ReBIT and Bidder.	LDs should be limited to no more than 0.5% of the value of the HW / SW in delay per week with an overall cap of 10% and should be the sole remedy for delay		No change in this criteria.
Installation and Operationalize tion: A penalty of 1% per week for first two weeks, 2% per week for every subsequent week subject to a maximum of 10%. Penalty will be computed on the total one time cost between the ReBIT and Bidder.	LDs should be limited to no more than 0.5% of the value of the services in delay per week with an overall cap of 10% and should be the sole remedy for delay		No change in this criteria.
5. A signed purchase order or contract furnished to the successful Bidder results in a binding contract without further action by either party.	A signed purchase order or contract furnished to the successful Bidder along with agreed T&C's results in a binding contract		No change in this criteria.
Neither party shall, in any event, regardless of the form of claim, be liable for any indirect. Special, punitive, exemplary, speculative or consequential damages, including, but not limited to any loss of data, business interruption, and loss of income or profits, irrespective of whether it had an advance notice of the possibility of any such damages. Subject to the above and notwithstanding anything to the contrary elsewhere contained herein, the maximum liability, of selected Bidder (Consultant) and purchaser (ReBIT) shall be, regardless of the form of claim, restricted to the total of bill of material received by Consultant/vendor from ReBIT for the event that gave rise to such liability, as of the date such liability arose, during contract period.	1) Consequential clause agreeable to DXC 2) the maximum liability, of selected Bidder (Consultant) and purchaser (ReBIT) shall be, regardless of the form of claim, restricted to the Annual total of bill of material received by Consultant/vendor from ReBIT for the event that gave rise to such liability, as of the date such liability arose, during contract period.		No change in this criteria.
The Service Provider hereby undertakes to indemnify and keep indemnified the Company from and against all direct and proven claims, actions or proceedings brought against it, losses, damages, fines or penalties imposed on the CLIENT or other liabilities suffered or incurred by the CLIENT, its directors or officers, as a consequence of any direct breach by the Service Provider of its obligations under this Agreement or any negligence on its part or its employees or agents under this Agreement.	1) Indeminity not applicable for direct breach as ame is covered under LD's / Penalties 2) Negligence should be gross. Gross negligence is defined as : “Gross Negligence” means an indifference to, and a blatant violation of a legal duty with respect to the rights of others, being a conscious and voluntary disregard of the need to use reasonable care, which is likely to cause foreseeable grave injury or harm to persons, property, or both. Gross negligence involves conduct that is extreme, when compared with ordinary negligence. A mere failure to exercise reasonable care shall not be a Gross negligence.		No change in this criteria.
	1) Bidder suggest gen RBI Responsibilities to be enumerated 2) EIT to propose adding appropriate relief event/savings clause to enable EIT’s ability to obtain schedule adjustments or financial relief in case of delay / inaction attributable to RBI 3) When Bank acts and omissions or other circumstances delay, disrupt or prevent EIT’s performance, EIT shall accordingly (i) extend delivery and milestone dates, (ii) be compensated for additional costs if incurred, and (iii) be paid for additional service performed due to such act & omission of the Bank		No change in the Terms & conditions

Section 3.8. Service Level Agreement (SLA) & Contracting **Implementation Service Level Agreement** 1. Delivery of hardware and software at all sites: Penalties will be applicable after 6 weeks, if the Delivery is still not completed. A penalty of 1% per week for first two weeks, 2% per week for every subsequent week subject to a maximum of 10% of the total contract value. Penalty will be computed on the total one-time cost between the ReBIT and Bidder. 2. Installation and Operationalization: Penalties will be applicable after 6 weeks, if the installation and Operationalization is still not completed. A penalty of 1% per week for first two weeks, 2% per week for every subsequent week subject to a maximum of 10%. Penalty will be computed on the total one time cost between the ReBIT and Bidder. **Infrastructure Availability SLA** **Hardware Failure Incident SLA** **Section 3.9. SLA for SIEM Management and Operation Services** **Section 4.9. Penalties and Liquidated Damages** In the event of delay in stage wise execution of work, specified in this Contract / furnishing deliverables due to negligence or in-efficiency attributable to the selected bidder, the selected bidder shall be liable to a penalty up to a maximum of 10% (ten percent) of the contract value.	1) Liquidated damages *(including Implementation SLA)* should be applicable only in the event of delay in delivery solely attributable to the Bidder and should be computed at the rate of 0.5% of the value of the affected service or product per week subject to the maximum of 10% of the value of affected service or product. 2) SLA Penalties *(including Infrastructure Availability SLA, Hardware Failure Incident SLA, SLA for SIEM Management and Operation Services)* should be capped @5% of the monthly charges.		No change in this criteria.
Section 4.7. Performance Bank Guarantee 1. The successful Bidder shall at his own expense deposit within thirty (30) working days of the date of notice of award of the bid, a Performance Bank Guarantee from a scheduled commercial bank, payable on demand in terms of relevant Annexure-A Performance Bank Guarantee format, for an amount equivalent to ten percent (10%) of the contract price for the due performance and fulfilment of the contract by the Bidder. 2. Without prejudice to the other rights of the Purchaser under the Contract in the matter, the proceeds of the performance bank guarantee shall be payable to ReBIT as compensation for any loss resulting from the Bidder's failure to complete its obligations under the Contract. ReBIT shall notify the Bidder in writing of the invocation of its right to receive such compensation, indicating the contractual obligation(s) for which the Bidder is in default. 6. The Performance Bank Guarantee will be valid till the end of the contract. Failure of the successful Bidder to comply with the above requirement, or failure of the Bidder to enter into a contract within 15 working days from the issue of the purchase order or within such extended period, as may be specified by ReBIT shall constitute sufficient grounds, among others. 7. In case of breach, there shall be a cure period of 5 calendar days. In case, if the issues are not resolved, the Performance Bank Guarantee would be invoked anytime thereafter as per the discretion of ReBIT.	Please modify the clause as: a) Bidder seeks PBG to be provided at 10% of annual contract value and shall be renewed yearly at 10% of relevant subsequent year's contract value. b) Bank shall invoke the PBG only on occurrence of material breach and after the Bank provides a 30 days cure period to the bidder to rectify the material breach for which the PBG is sought to be invoked.		No change in this criteria.

4.8 Payment Terms a. Eighty percentage (80%) of the Total cost of Bill of material will be released on delivery, successful installation and operation of the total solution in ReBIT. This would also include signing the User Acceptance Test (UAT) document and Service Level Agreement (SLA)/Purchase Agreement by ReBIT and Implementation certificate. b. Twenty percentage (20%) of the Total cost of Bill of material will be released after one month on completion of Project Sign Off. c. Even though ReBIT is requesting for 3 years TCO in commercial sheet, PO would be raised for licenses only on yearly basis. d. Payment towards Annual Maintenance cost will be made on annual basis. The invoice should be submitted at the end of the year with satisfaction report from the concerned users/owner of the Project. e. Payment towards SIEM Management and Operation service cost will be made on quarterly basis. The invoice should be submitted at the end of each quarter along with satisfaction report from the concerned users/owner of the Project.	Please change the Payment Terms as follows: a. Hundred percentage (100%) of the Total cost of Bill of material will be released on delivery, successful installation and operation of the total solution in ReBIT. b. Payment towards Annual Maintenance cost will be made on annual in advance basis. c. Payment towards SIEM Management and Operation service cost will be made on monthly basis.		No change in this criteria.
Invoicing Terms	Please add the following clauses: 1. Bank shall pay within 30 days from the date of invoice. 2. Late payment will bear an interest of 2% per month.		No change in the Terms & conditions
Termination by SI	Bidder seeks right to terminate or suspend services in the event of delay in payment of undisputed invoice.		No change in the Terms & conditions
3	Ticketing solution is required?		Stand Alone Ticketing solution is not required, the SIEM should have a basic ticketing capability for Event management
4	Its given that the complete solution is required as part of the proposal including hardware, software and services. Does that mean we need to factor for solutions like backup, Archival and network switches for ports and firewalls/routers required for remote connectivity?		The SIEM solution includes the servers or appliance including the storage. LAN network will be by ReBIT
6	Is it safe to assume that the current EPS is approximately 1000 and the growth over 5 years would be to 2500 in a linear fashion?		This is as per our projections, actual increase might differ however it will be within the 2500 EPS level
7	what are the compliance requirements for logs management that ReBIT would want to follow i.e. both online and offline.		6 months online, no offline log or archiving is required
8	As part of setting up the SOC, we will work on all people process and technology front which would require setting up relevant processes for SOC in accordance to the IS policy for ReBIT and setting up SOPs. Is this fine or do you already have these in place which the bidder needs to adhere to?		SOC SOP will be as per the Bidder however it needs to satisfy our SLA and our terms & conditions
9	DLP is one of the solutions asked for incident management. We have witnessed that multiple customers keep incident management for DLP separate from SOC incident management more specifically in remote management environments. Bidder would like to confirm if its the DLP solution components logging required to be integrated or DLP incident management is required to be added to the remote SOC		DLP logging from Day one

10	Infrastructure availability SLA talks about solution uptime and qualifying outage time. Bidder would request for clarity that if the solution is put up in HA and one of the component in HA goes down, the service would be up while a component would be down, would that be considered as a qualifying outage time while the service would still be up?		Outage is failure of SIEM to provide its security functionality, including log collection. Every OEM has a unique solution architecture, please fit the best design to meet ReBIT's HA requirement - atleast 2 physical servers/appliances, both will be placed in the same server room. If Primary setup goes down or malfunctions, entire SIEM should function through the Backup solution. hardware need to have dual power supply.
	SLAs and associated penalties. Bidder would like to submit that as per the requirement laid out in the RFP, there could be a period where Bidder has to support the solution even after its out of a valid OEM support contract, in such situation, the SLA shall be made on best effort basis and penalties be waived off for issues that have dependencies on the OEM		No change in the criteria
	Bidder would like to submit that the improvement expectation of 10% in security incident identification could be a challenge to achieve as with each round of optimization the scope of improvement also reduces. E.g. the reduction in the first round of improvement could be way higher than 10% too while it would reduce with each round for each category of incident. Is it possible to remove the absolute value of 10% from this requirement and modify it to improvement only.		No change in the criteria