

Addendum – RFP – Endpoint Compliance Management Solution

Corrigendum – Endpoint Compliance Management Solution (ECMS) – This Corrigendum is applicable to the [RFP](#) listed under this heading

Please refer to the [RFP](#) published on the ReBIT’s website on March 31, 2020 inviting submission of bids from eligible vendors for providing professional services for Endpoint Compliance Management Solution through tendering route. Corrigendum containing the following changes to the above RFP document has been released.

Corrigendum:

Page No.	Terms & Conditions/Section given in the RFP	Modified as
32	The Bidder should have a positive net worth and profit (after tax and partner disbursements - applicable to partnership firms only) making company in each of the three (3) financial years, i.e. 2016- 17, 2017 - 18 and 2018 – 19 (or Calendar year 2017, 2018 and 2019).	No Changes in RFP terms. The minimum eligibility criteria is mandated in the RFP to meet quality and technical specifications as appropriate for ReBIT.
32	Bidder should have completed at least 2 projects worth cumulative of at least 25 Lakhs INR (Cumulative Cost), in last 2 years for Indian Clients. The name of the Bidder (SI and / or OEM) needs to be in sync with the credential letters / contract copies, exceptions will be made in case of divesture, M&A.	It indicates that 2 or more projects cumulative value in last 2 years should be 25 lakhs for Indian Clients. The name of the Bidder (SI and / or OEM) needs to be in sync with the credential letters / contract copies, exceptions will be made in case of divesture, M&A.
48	8.6 Earnest Money Deposit	EMD is exempted to MSMEs, subject to providing the required document/certificate confirming the MSME status.

32	<p>MSME Point 1 - We suggest including "MADE IN INDIA" clause.</p> <p>MSME Point 2 - Exempt us from the experience part and producing 25 lacs Purchase order part</p>	<p>This RFP is not a global tender.</p> <p>The minimum eligibility criteria is mandated in the RFP to meet quality and technical specifications as appropriate for ReBIT.</p>
32	<p>MSME Point 3 - Also, the Government of India is promoting MSME for business. In case MSME is not L1 and the one who is L1, in that case L1 should award 15% or 25% of work order to MSME. This will help MSME and the country to grow. Such clauses are already getting included in Tenders in order</p>	<p>The requested MSME preference(s) will not be applicable for this tender.</p>
31	6.1 Objective of Evaluation Process	<p>If two or more bidders have same value of commercial bid, then the reverse auction process will be conducted.</p>
	<p>6.3 Technical Bid Evaluation Criteria.</p> <p>Two stage evaluation process:</p> <p>1) Technical Specification sheet - 208 Marks, "Must Have" features - 150 Marks "Good to Have" features - 48 Marks Must Have features is a knock-out criteria. In case, Bidder is not able to meet any one of the "Must Have" feature, he will not be qualified for further evaluation.</p>	<p>Three stage evaluation process:</p> <p>1) Technical Specification sheet - 208 Marks, "Must Have" features - 150 Marks, "Good to Have" features - 48 Marks, Must Have features is a knock-out criteria. In case, Bidder is not able to meet any one of the "Must Have" feature,</p>

<p>34</p>	<p>2) Tech Presentation – 10 Marks Overall Cut-off of Technical evaluation for Commercial Bid eligibility – 75%</p>	<p>he will not be qualified for further evaluation</p> <p>2) Mandatory Technical Product Demonstration of the solution – 60 Marks</p> <p>Bidder will disqualify in case doesn't score more than 90% in Demo.</p> <p>3) Technical Panel Presentations – 50 Marks</p> <p>Overall Cut-off of Technical evaluation for Commercial Bid eligibility – 80%</p> <p>Detailed Process: -</p> <p>3. Top 5 Bidders who have cleared the cut off in Technical Specification score, are required to carry out Technical Product Demonstration of the solution proposed by the Bidder. Demo should be done using web conferencing and videoconferencing. so that Bidder should be able to demonstrate all the “Must Have” and “Good to Have” feature as specified in the Technical Specifications Sheet. For successful demonstration of each “Must Have” feature, there</p>
-----------	---	---

will be 2 Marks awarded for the same. Total 60 Marks grade scoring. Break-up of the 60 Marks Technical Product Demonstration Scoring, please refer the **Annexure - S**. Top 5 Bidders who scored minimum 90% in Technical Product Demonstration Scoring activity will be qualified for further round of technical evaluation i.e. Technical Panel Presentations.

4. Top 5 Bidders who have cleared the cut off in technical specification score and cleared technical product demonstration scoring criteria, will be invited for presentation. 50 Marks grade scoring

For break-up of the 50 Marks scoring of Technical Panel Presentations, please refer the **Annexure - T**.

5. The total score of Technical Specifications score, Technical Product Demonstration score and Technical Panel Presentations score will be considered as technical evaluation score. Top 5 Bidders who have scored more than 80%

		as Technical evaluation score will be qualified for Commercial Bid.
35	6.3.2 Disqualification Parameters in Technical Bid Evaluation	If only one Bidder qualifies, the ReBIT at its discretion may select more than one Bidder for commercial evaluation.
NA	<p>Technical Specification Sheet</p> <p>Detailed Response (please be as elaborate as possible on how your solution addresses these points</p>	Detailed response is expected from bidder on each technical point. (please be as elaborate as possible on how your solution addresses these points) Only detailed response on each point will be considered for scoring, bidder will be disqualified in “Technical Specifications Sheet” scoring stage itself in case Bidder do not elaborate on any of the point of the technical specifications.
30	<p>6. Evaluation Process</p> <p>The Bidders have to submit ‘the Technical Bid’ and ‘the Commercial’ Bid simultaneously in separate sealed envelopes. The Bidder has to submit ‘Technical Bid’ keeping in view the information / criteria mentioned in Section 2 and 3 of these documents by the date and time stipulated as in Table 1 of Section 1.</p>	<p>Bid submission process: -</p> <p>Option A – Physical mode: EMD Cheque – Physical submission at ReBIT office Bid Documents – All 3 envelopes in Physical Form at ReBIT office</p> <p>Option A will remain as it is which is mentation in RFP.</p> <p>Bidder should submit all bid documents on or before 18th June 2020 (02:00 PM)</p>

Option B – Virtual mode:

EMD Cheque – Through NEFT /
RTGS Payment

Bid Documents – 3 different
Password Protected PDF files at
“Procurement” email ID

Online bid Process will be as
follows:

1. Bidders are required to submit the following three PDF files
 - a. “Minimum Eligibility Criteria”
 - b. “Technical Bid”
 - c. “Commercial bid”

Three separate password protected PDF files to
“procurement@rebit.org.in” email id on 18th June 2020 between 01:00 PM to 02:00 PM IST. (Email attachment size limit is 10 Mb). Any submission after given time would not be accepted for bid evaluation.

It is requested to send three separate emails with subject line stating – “Minimum Eligibility Criteria”, “Technical Bid” and “Commercial bid” respectively.

2. Password for “Minimum Eligibility Criteria” & “Technical Bid with Annexures” document to be shared to
“procurement@rebit.org.in” email id on 18th June 2020 between 01:00 PM to 02:00 PM IST.
3. Password for the Commercial bid document SHOULD NOT be shared at this point of time. Bidders who have successfully cleared the Technical criteria will be informed to share the password for “Commercial Bid” afterwards.

4. EMD should be submitted online by NEFT/RTGS. UTR No. to be shared and send while submitting the bid documents. Bidder should provide the Bank details / cross cheque for EMD refund.
5. ReBIT Bank details will be shared afterwards through procurement email ID.

Interested bidders should request on ReBIT procurement ID (3 Days Before) "procurement@rebit.org.in"

For Option 1 or Option 2 for Final bid Submission.

6. Post Technical Specification sheet evaluation, eligible bidders would be invited for Technical Product Demonstration. Details of same would be shared with eligible bidder.
7. Post Technical Product Demonstration evaluation and score, eligible bidders would be invited for Technical Panel Presentations. Details of same would be shared with eligible bidder.
8. Post evaluation of Technical Specification sheet, Technical Product Demonstration and Technical Panel Presentations eligible bidders would be invited for commercial bid opening over WebEx or in-person meeting. Details of same would be shared with eligible bidder.
9. Password for the commercial bid document attachment should be shared by the bidders-30 minutes prior to

		<p>Commercial bid opening on procurement email ID and same shall be used to open the commercial bid.</p> <p>Interested bidders should request on ReBIT procurement ID (3 Days Before) procurement@rebit.org.in”</p> <p>For Option 1 or Option 2 for Final bid Submission.</p>
--	--	---

Note: This document shall form part and parcel of the [RFP](#) and therefore bidders are advised to take the clarifications/responses into account, as applicable, while submitting the bids.

Pre-Bid Queries and Response:

RFP Page No.	RFP Point No.	RFP Description	Bidders Query	ReBIT Clarification
78	8	It should be able to deliver broad range of other security functions and gives you the ability to add other targeted functions as needed, without adding infrastructure or implementation cost.	Please explain the term "other security functions"	Other security functions like scanning of network devices such as switches, firewall to be achieved without adding additional infrastructure viz servers and without any additional implementation cost.

78	15	The solution must be able to auto-remediate the endpoints which fails the regulators controls like CIS benchmarks.	Please list the control from CIS benchmarks as there are 3 categories in CIS benchmarks.	We have already selected CIS policies for our environment which will be shared with the selected vendor for deployment.
78	23	The solution should be able to scan and give report of unmanaged endpoints.	Please explain how to connect to unmanaged end points, do they have IP address ? Or it is connected to to your network ?	The solution should give status of endpoints which are not being managed by the Central server by performing network scan and should give detailed reports of this unmanaged endpoints like patch, AV definition status, 3rd party installed endpoint protection client status etc.
78	42	Backup and Restoration of all policies and database.	Are you referring to policy and database backup at end points ? Or the application server ? Please clarify	Backup of Application and Database server.
78	43	Client agent should have anti tamper password. (requires additional credential to uninstall Software)	the uninstallation refer to the client agent ? If so we can restrict the user from uninstalling the agent in the client computer	Yes we don't want end user to be able to uninstall software apart from administrators.

78	NA	<p>The proposed solution should have hybrid architecture to get the update from public network (using authentic URL) when endpoint is connected over VPN. However, at the same time, it should simplify operations with a single console for management, configuration, discovery, creation and deployment of policies and other security functions.</p>	<p>Does ReBIT have their own VPN setup or do they expect the vendor to supply the same?</p>	<p>No, ReBIT have their own VPN setup.</p>
NA	NA	<p>Monitor and manage the status and health of various third-party endpoint protection clients such as anti-virus and anti-malware tools.</p>	<p>the third party endpoint protect</p>	<p>AV, DLP, Proxy, ITSM, MFT, 2FA, Vaultize, Encryption and Backup solution clients etc..</p>

NA	NA	The proposed solution should be able to retrieve and provide security information irrespective of vendors computing environment.	list of security devices/solutions being currently used by ReBIT	Necessary details will be shared with the selected bidder only.
NA	NA	Backup and Restoration of all policies and database.	Backup and restoration to be on-premise or cloud? In case of cloud, then how many months of data retention ? Does ReBIT has its own private cloud?	<p>Backup and restoration be on premise. Backup procedure for Application and Database server of the proposed solution is required and to be demonstrated.</p> <p>Data retention period will be shared with the successful bidder only.</p> <p>In future, if ReBIT decides to move to cloud environment whether private or public, then there should not be any hinderance in backup, restoration or any other functions.</p>
NA	NA	Integration with SIEM to analyze and parse security events/logs generated.	Does ReBIT have a SIEM installed? If Yes, then plz share the brand and specifications.	Yes, Necessary details will be shared with the selected bidder only.
NA	NA	Is ReBIT wish to achieve all the "must have" capability with single solution and agent		Yes single - centralized solution to achieve all the requirements.

Page No 32	78	It states that Companies should have positive network, and Profit after tax for 3 years 16-17,17-18 &18-19.	Please change the 3 years from (16-17,17-18,18-19) to (17-18,18-19 & 19-20)	<p>The Bidder should have a positive net worth and profit (after tax and partner disbursements - applicable to partnership firms only) making company in each of the three (3) financial years.</p> <p>However, the Bidder should have a positive net worth and profit during the last 3 financial years.</p>
Page No 24	78	States payment for licences subsequently purchased will be done at The licenced rate (unit rate) shared by bidder -There should be timeframe for such purchase Statement	Please make the license payment advance & services quarterly advance.	No Changes in payment terms.
Page No 78	17	Able to monitor any changes to operating system files, registry files and system configuration.	With Bigfix Semi realtime monitoring can be done and required information can be fetched from the endpoints. Request to change to Semi Realtime monitoring.	Bidder can use any supporting tool to meet technical requirement, however any solution should be seamlessly integrated with primary solution. Further, there should not be any additional cost / licenses for said requirement.

Page No 78	18	It should provide the complete lifecycle management of all the IT assets from request management via service catalog, through delivery, maintenance, support, to retirement and disposal.	Request you to kindly remove this clause.	It is good to have requirement, no Changes in RFP.
NA	NA	NA	Capable of monitoring critical operating system and application elements files, directories, registry keys to detect suspicious behaviour, such as modifications, or changes in ownership or permissions.	Solution Should monitor any changes to operating system files, registry files and system configuration.
NA	NA	NA	Monitor System Services, Installed Programs and Running Processes for any changes.	Solution Should monitor all the 3rd party endpoint protection clients like AV, DLP, Proxy, ITSM, MFT, 2FA, Vaultize, Encryption and Backup solution clients.

NA	NA	NA	<p>Extensive file property checking whereby files and directories are monitored for changes to contents or attributes (ownership, permissions, size, etc).</p>	<p>Not Part of RFP technical specification criteria.</p> <p>However, if Tool is providing such feature, then it will be considered as additional feature.</p> <p>This feature will not be considered as part of Technical specification evaluation criteria.</p>
NA	NA	NA	<p>Track addition, modification, or deletion of Windows registry keys and values, access control lists, or web site files are further examples of what can be monitored.</p>	<p>Not Part of RFP technical specification criteria.</p> <p>However, if Tool is providing such feature, then it will be considered as additional feature.</p> <p>This feature will not be considered as part of Technical specification evaluation criteria.</p> <p>Solution should be able to monitor any changes to OS files, registry files and configurations files irrespective of the approach proposed.</p>

NA	NA	NA	<p>Automated recommendation of integrity rules to be applied as per OS and can be scheduled for assignment/unassignment when not required.</p>	<p>Not Part of RFP technical specification criteria.</p> <p>However, if Tool is providing such feature, then it will be considered as additional feature.</p> <p>This feature will not be considered as part of Technical specification evaluation criteria.</p> <p>Auto-remediation of CIS benchmarks policies and patches, configurations for fixing vulnerabilities.</p>
NA	NA	NA	<p>Solution should have by default Rules acting at Indicators of Attacks detecting suspicious/malicious activities.</p>	<p>Not Part of RFP technical specification criteria.</p> <p>However, if Tool is providing such feature, then it will be considered as additional feature.</p> <p>This feature will not be considered as part of Technical specification evaluation criteria.</p>

NA	NA	NA	<p>In the Event of unauthorized file change, the proposed solution shall reports reason, who made the change, how they made it and precisely when they did so.</p>	<p>Not Part of RFP technical specification criteria.</p> <p>However, if Tool is providing such feature, then it will be considered as additional feature.</p> <p>This feature will not be considered as part of Technical specification evaluation criteria.</p> <p>Solution should be able to monitor any changes to OS files, registry files and configurations files irrespective of the approach proposed in the solution.</p>
NA	NA	NA	<p>Solution should have Security Profiles which allows Integrity Monitoring rules to be configured for groups of systems, or individual systems. For example, all Linux/Windows servers use the same base security profile allowing further fine tuning if required. Rules should be auto-Provisioned based on Server Posture.</p>	<p>Not Part of RFP technical specification criteria.</p> <p>However, if Tool is providing such feature, then it will be considered as additional feature.</p> <p>This feature will not be considered as part of Technical specification evaluation criteria.</p>

NA	NA	NA	<p>Solution should have an intuitive rule creation and modification interface includes the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories, and other features.</p>	<p>Not Part of RFP technical specification criteria.</p> <p>However, if Tool is providing such feature, then it will be considered as additional feature.</p> <p>This feature will not be considered as part of Technical specification evaluation criteria.</p> <p>The solution should have Centralized web-based management console to monitor and view dashboard, create, deploy and maintain policies.</p>
NA	NA	NA	<p>Multiple groups of hosts with identical parameters</p>	<p>Not Part of RFP technical specification criteria.</p> <p>However, if Tool is providing such feature, then it will be considered as additional feature.</p> <p>This feature will not be considered as part of Technical specification evaluation criteria.</p>
NA	NA	NA	<p>Regex or similar rules to define what to monitor</p>	<p>Not Part of RFP. However, if Tool is providing such feature, then it can be considered as Value added feature.</p> <p>Addon features shall not effect overall tech or comm evaluation processes and this also should not provide any specific advantage to some bidders</p>

NA	NA	NA	Any pre-defined lists of critical system files for various operating systems and/or applications (web servers, dns, etc..)	Details will be shared with the finalized vendor during implementation phase.
NA	NA	NA	Ability to apply a host template based on a regex of the hostname	<p>Not Part of RFP technical specification criteria.</p> <p>However, if Tool is providing such feature, then it will be considered as additional feature.</p> <p>This feature will not be considered as part of Technical specification evaluation criteria.</p>
NA	NA	NA	Ability to exclude some monitoring parameters if they are not required	<p>Not Part of RFP technical specification criteria.</p> <p>However, if Tool is providing such feature, then it will be considered as additional feature.</p> <p>This feature will not be considered as part of Technical specification evaluation criteria.</p>
NA	NA	NA	Ability to generate E Mail and SNMP alerts in case of any changes	<p>Not Part of RFP technical specification criteria.</p> <p>However, if Tool is providing such feature, then it will be considered as additional feature.</p> <p>This feature will not be considered as part of Technical specification evaluation criteria.</p>

NA	NA	NA	Solution should support creation of custom Integrity monitoring rule.	<p>Not Part of RFP technical specification criteria.</p> <p>However, if Tool is providing such feature, then it will be considered as additional feature.</p> <p>This feature will not be considered as part of Technical specification evaluation criteria.</p>
NA	NA	NA	Solution should provide an option for real time or scheduled Integrity monitoring based on operating system.	<p>Not Part of RFP technical specification criteria.</p> <p>However, if Tool is providing such feature, then it will be considered as additional feature.</p> <p>This feature will not be considered as part of Technical specification evaluation criteria.</p>
32	3	Bidder should have completed at least 2 projects worth cumulative of at least 25 Lakhs INR (Cumulative Cost), in last 2 years for Indian Clients.	Kindly clarify the Orders(PO) like End Point Security, Deep Security, Server Security solution, Asset Management & Vulnerability Assessment tool, WAF etc. which are relevant to end point compliance can be used for Bidder eligibility criteria.	No Changes in RFP terms, it indicates 2 or more projects cumulative value in last 2 years should be 25 lakhs.
45	8.4	Cancellation of contract & Compensation	Request you to kindly remove this clause.	No Changes in RFP terms.

NA	NA	Is ReBIT wish to achieve all the “must have” capability with single solution and agent		Yes, All requirements in Technical details are for one solution and agent.
Page No 32	78	It states that Companies should have positive network, and Profit after tax for 3 years 16-17,17-18&18-19.We do not have in 16-17.This needs to be changed	Please change the 3 years from (16-17,17-18,18-19) to (17-18,18-19 & 19-20)	<p>The Bidder should have a positive net worth and profit (after tax and partner disbursements - applicable to partnership firms only) making company in each of the three (3) financial years.</p> <p>However, the Bidder should have a positive net worth and profit during the last 3 financial years.</p>
Page No 24	78	States payment for licences subsequently purchased will be done at The licenced rate (unit rate) shared by bidder -There should be timeframe for such purchase Statement	Please make the license payment advance & services quarterly advance.	No Changes in quarterly payment as SLA are tagged with payment.

<p>Page No 78</p>	<p>18</p>	<p>It should provide the complete lifecycle management of all the IT assets from request management via service catalog, through delivery, maintenance, support, to retirement and disposal.</p>	<p>Request you to kindly remove this clause. Else we will need to add another solution.</p>	<p>This is good to have feature requirement,</p>
<p>Page No 78</p>	<p>17</p>	<p>Able to monitor any changes to operating system files, registry files and system configuration.</p>	<p>With our solution Semi realtime monitoring can be done and required information can be fetched from the endpoints. Request to change to Semi Realtime monitoring.</p>	<p>There should be push update / real-time monitoring from endpoint/system to Console/application on changes made on system.</p>

<p>Para 3.10</p>	<p>19</p>	<p>Para 3.10</p>	<p>Requesting you to kindly change the payment milestones as follows:</p> <ol style="list-style-type: none"> 1. Signing of Agreement - 10% of product license cost 2. Process and System Study - submission of SRS document - 20% of the implementation cost 3. Deployment and UAT sign off - 50% of product license cost, 50% of implementation & training costs 4. Implementation-VAPT Sign off and Training - 10% of product license cost and 10% of the implementation & 30% of the training costs 5. Go Live - Remaining 30% of product license cost 6. Go live + 30 days Remaining 20% of implementation & training cost 	<p>No Changes in payment Terms.</p>
------------------	-----------	------------------	--	-------------------------------------

<p>2.2 Defini tion of Terms</p> <p>3.11. 1 Warra nty</p>	<p>8 & 21</p>	<p>8 & 1</p>	<p>Please confirm that the warranty duration is 5 years or 3 years since there is a contradiction between page No. 8 & 21</p>	<p>Total 5 years of duration, Warranty duration is 3 years and 2 Years of AMC.</p>
<p>9.18 Annex ure R</p>	<p>78</p>	<p>Sr. No. 42</p>	<p>Please clarify the retention period for “Backup and Restoration of all policies and database”. This is required to size the Hardware storage configuration as per RFP clause 3.3.4 (pg-14)</p>	<p>Necessary details will be shared with the selected bidder only.</p>
<p>We highly recommend these additional features which are beneficial to ReBIT</p>	<p>T1</p>	<p>Automated network discovery with vulnerability scanning across all IP devices (Not just PCs and Servers, but also IP phones and all such IP enabled devices) including Host Discovery, Port scanning, Service scanning, OS auto detection etc in an agent less manner</p>	<p>It would be good to have this feature along with the requirements mentioned in technical specifications but that too without any additional cost to ReBIT.</p>	

	T2	Mobile app for asset movement tracking, GPS tagging of assets, Proximity based asset management based on GPS coordinates	<p>Not Part of RFP technical specification criteria.</p> <p>However, if Tool is providing such feature, then it will be considered as additional feature.</p> <p>This feature will not be considered as part of Technical specification evaluation criteria.</p>
	T3	Ability to monitor and manage all printers, cartridge levels and paper usage / cost management using the same agent. Also control printer access as needed, track files being printed by user, location etc	It would be good to have this feature along with the requirements mentioned in technical specifications but that too without any additional cost to ReBIT.
	T4	Ability to perform Patch management functions using the same agent as Compliance management	Yes, we don't need any additional agent to be installed to perform the patch management, it should be managed with one agent.
	T5	End point health management using the same agent (Health of fans and batteries), identify if the health issue is due to malware or environmental issues	It would be good to have this feature along with the requirements mentioned in technical specifications but that too without any additional cost to ReBIT.

	T6	Server-side solution pre-packaged as a Virtual Appliance.	It would be good to have this feature along with the requirements mentioned in technical specifications but that too without any additional cost to ReBIT.
	T7	Use AI/ML to learn and predict machine usage pattern, turn off/put machines to sleep when they are not in use (as per defined ruleset), Send security alerts if machines are turned-on/used during non-office hours.	
	T8	Provide Detailed analytics of usage duration of machines by date range, hostname/ip, location etc.	
	T9	Ability to Send security alerts if any hardware components of the system like Hard disk, RAM etc. are changed	
	T10	Design and implementation of security policies, enforcements and audit without providing any product updates or patches.	
	T11	GUI based tool for of definition of security polices and	

		enforcement rules.	
9.18 Annexure R	T12	Does the client environment have SCCM installed for policy enforcement? If yes, please mention versions used	No, we don't have SCCM, however we may implement the same.
	T13	Are there any reporting software already used by the ReBIT? If yes, please elaborate which one	Necessary details will be shared with the selected bidder only.
	T14	Are there any patch management software already used by ReBIT? If yes, please mention which one.	Necessary details will be shared with the selected bidder only.
	T15	What are the CIS policy enforceable applications / OS used by ReBIT?	We have already selected CIS policies for our environment which will be shared with the selected vendor for deployment.
	T16	Please provide version and details of SIEM software used that we should integrate with	We do have SIEM software. Details will be shared with the finalised vendor.
Page 21	3.11.1	As per this clause 3 years warranty period is expected with additional 2 years of 'Offsite' maintenance . What is the expectation in the Offsite	3 Years of Warranty and 2 Years of AMC, engineer should visit ReBIT Office as and when support request is created for any changes and / or fix the problem raised with the vendor.

			Preventive maintenance	
			As per this clause “Warranty – The Bidder will be required to provide 5 Years of on-site support “ – This seems to be different from the warranty requirement	3 Years of Warranty and 2 Years of AMC, engineer should visit ReBIT Office as and when support request is created for any changes and / or fix the problem raised with the vendor.
Page 11	3.2		Should we consider to provide 700 product license here , kindly confirm .	Currently we have 250 endpoints including Laptop, Desktop, Servers etc. which will increase gradually. So the license count will also increase gradually. No. of licenses required are as per Commercial Bid format.
Page 16	3.8		What is the expected duration of the hands-on training & the number of participants	The training should be precise enough to be understood by the intended users and duration would be max 2-3 days. Training should extensively cover Administration of the tools, L1 level troubleshooting.
NA	NA	Refer 3.2	Need more clarity on numbers users ?	As mentioned in RFP it would start with 250 endpoints including Laptops, desktops, servers and network devices which will scale to 700 or more as ReBIT is an growing organisation.

NA	NA		We need basic network architecture dig?	Details will be shared with the selected vendor.
NA	NA		Can you reduce test period for 15 days.	No change in this criteria.
NA	NA		The solution provider should produce detailed POA for implementation of ECM?	Yes, a detailed approach plan as how Bidder will implement this solution, how much time it will take for completion of UAT and Prod, who will be responsible for what activities etc. must be present.
NA	NA	Refer 6.2	Point 2 can we reduced Cumulative cost ?	No Changes in RFP terms, it indicates 2 or more projects cumulative value in last 2 years should be 25 lakhs.
NA	NA	Refer page 31	What will be score for Partial support ?	Query is not clear.

Page 14	3.3 .4	<p>The bidder should provide all the required hardware details along with detailed configuration required for hosting the Endpoint Compliance Management Solution at ReBIT site.</p> <ul style="list-style-type: none">· Bidder should provide the hardware configuration details while submitting the Technical Bid.	Bidder expects the hardware for the solution will be procured ,managed and maintained by ReBIT.	Yes, hardware details such as server configuration are required while submitting the Bid. Hardware will be managed and maintained by ReBIT.
------------	-----------	---	---	---

Page2 1	Point 3	If ReBIT desires, it could extend the onsite support (engineer will be needed onsite for any upgrades/updates/issue resolution/troubleshooting) beyond three (3) years as per the business need, Bidder should provide (Application / Software) 24X7X365 days support with no additional cost to ReBIT.	Please clarify on "No additional cost "clause	No Changes in RFP terms, Support case should include onsite support required as mentioned in RFP.
------------	------------	---	---	---

<p>Page 21</p>	<p>Poi nt 2</p>	<p>During the three (3) years of warranty, the Bidder will be required to provide on-site support, if required the on-site support may be extendable at the ReBIT's discretion. It is envisaged at this stage that the next two years of warranty would be on off-site support basis. Bidder should provide Preventive maintenance of application without any cost to ReBIT.</p>	<p>As understood the project duration is 5 years. Pls clarify "Preventive maintenance of application without any cost to ReBIT. "</p>	<p>Yes any maintenance/support/upg rade/Changes during this period would not be charged to ReBIT.</p>
		<p>General</p>	<p>Can Bidder leverage on existing Helpdesk tool for ticket logging, tracking, and SLA measurement</p>	<p>Yes for internal management ReBIT will use internal Helpdesk tool, Bidder should provide their support/helpdesk and SLA tracking tool for support management.</p>

<p>Page 13</p>	<p>Point 3</p>	<p>There shall be a provision for taking backups and archive the replica of the systems' database and the application as well. There should be a provision of adequate Business Continuity Management (BCM).</p>	<p>Can bidder leverage on current Backup tool, If yes, please share the details. Please confirm the backup policy</p>	<p>We don't have specific backup tool for servers and application. Necessary details regarding backup policies will be shared with the selected vendor only.</p>
<p>Page 12</p>	<p>Bidder shall submit the manufacturer / OEM authorisation letter to confirm that product / solution is delivered from Manufacturer / OEM and Selected bidder is partner with OEM for the above scope of work and submit the same as part of the bid. This agreement should include but not limited to the ownership of the activities, timelines and resources associated to the activities.</p>	<p>Please confirm if there is any format for the OEM authorisation letter</p>	<p>No specific format for the OEM authorisation letter. It has to be on the letterhead of OEM, Seal / Stamp and Signed by Authorised Signatory of OEM.</p>	

NA	NA	Technical Specification - Point 21	<p>The solution should be able to scan and give report of unmanaged endpoints. - What is meant by Unmanaged clients here, and does it refer to network monitoring that can discover any unmanaged clients that someone randomly adds to the network, or does it refer to the clients not managed by DC?</p>	<p>The solution should give status of endpoints which are not being managed by the Central server by performing network scan and should give detailed reports of this unmanaged endpoints like patch, AV definition status, 3rd party installed endpoint protection client status etc.</p>
NA	NA	Technical Specification - Point 15	<p>The solution must be able to auto-remediate the endpoints which fails the regulators controls like CIS benchmarks. - Does this mean if the endpoint gets connected to the network which fails CIS benchmarks can Saner quarantine, then patch the system and bring back in compliant state and back in the network or is it that we should have an automated remedy for any deviations that</p>	<p>Basically the solution should have an automated remedy for any deviations found during scan but if we can quarantine a particular endpoints till it gets compliant, then that will also comply our requirement.</p>

			are found during a scan?	
6.2.3	32	Bidder should have completed at least 2 projects worth cumulative of at least 25 Lakhs INR (Cumulative Cost), in last 2 years for Indian Clients. The name of the Bidder (SI &/or OEM) needs to be in sync with the credential letters/contract copies, exceptions will be made in case of divesture, M&A	<p>1.The cumulative orders worth 25 lacs should be of ECMS only or any other technology orders will also do.</p> <p>2. To change the condition as either OEM/Bidder to produce order worth 25 lacs for ECMS or solution proposed</p> <p>3. Request you to change cumulative order worth 3 lacs</p> <p>4. Since you are going to do POC and than choose the product I request you to eliminate this criteria so that better companies and technologies can participate in the tender</p>	Refer section 6.2 - Minimum Eligibility Criteria and section 6.3 - Technical Bid Evaluation Criteria.

<p>General Functionalities - Point 2</p>	<p>The proposed solution should have hybrid architecture to get the update from public network (using authentic URL) when endpoint is connected over VPN. However, at the same time, it should simplify operations with a single console for management, configuration, discovery, creation and deployment of policies and other security functions.</p>	<p>Requesting you to please provide an use-case for public network access. What kind of updates are going to come from public network (authenticate URL)</p>	<p>Updates like AV definitions updates, auto-remediation CIS policies updates, patch updates of vulnerabilities discovered during VM scan.</p> <ol style="list-style-type: none"> 1. If endpoint is connected to official network it should get the update from local server, 2. When endpoint is connected to public network / non official network using VPN, update should come from public network to reduce the network traffic over the VPN.
<p>General Functionalities - Point 4</p>	<p>The solution should be able to provide software license optimization by comparing the licenses you own, showing where you are overpaying and where you are under licensed.</p>	<p>We request you to clarify about the kind of licenses you are asking for? And what are the purpose of the licenses</p>	<p>The solution should provide the license optimization means it should give details of license utilization of ReBIT solutions like AV, DLP etc i.e. How many licenses purchased and how many utilized?</p>

<p>General Functionalities - Point 5</p>	<p>Should be able to create Whitelist application policy - defined which applications are appropriate and which are not allowed.</p>	<p>Requesting you to please provide the list of applications that are good to have in your environment. What is the definition of Whitelisting the applications according to you.</p>	<p>Necessary details will be shared with the selected bidder only.</p>
<p>General Functionalities - Point 7</p>	<p>Need to have functionality of performing vulnerability scan throughout the network to find out the vulnerabilities.</p>	<p>What are the type of vulnerabilities you are asking for. Cisco ISE alone cannot do this, need an integration with VA tool.</p>	<p>We expect that Tool should be able to understand the latest patch / version of AV, OS Patches, applications patch etc. and accordingly, should be able to update the same on Endpoint. We do not expect any Vulnerability scanning Tool incorporated in the solution.</p>
<p>General Functionalities - Point 19</p>	<p>It should be able to deliver broad range of other security functions and gives you the ability to add other targeted functions as needed, without adding infrastructure or implementation cost.</p>	<p>What other security features and functions are you referring to? What kind of integration you are focusing on?</p>	<p>Other security functions like scanning of network devices such as switches, firewall to be achieved without adding additional infrastructure - servers and without any additional cost.</p>

<p>General Functionalities - Point 8</p>	<p>Must be able to create remediation job to roll out the patch with immediate effect to fix the vulnerabilities.</p>	<p>What is the Patch management software that is being used or planning to use ?</p>	<p>The proposed solution should have this feature of patch management.</p>
<p>General Functionalities - Point 9</p>	<p>The proposed solution should be able to provide Operating system and 3rd party software patch management and status.</p>	<p>Requesting you to please provide the list of operating systems and 3rd party software that you are referring to?</p>	<p>Necessary details will be shared with the selected bidder only.</p>
<p>General Functionalities - Point 11</p>	<p>The proposed solution should be able to create security policies based on security benchmarks published by Center for Internet Security (CIS), NIST, PCI-DSS.</p>	<p>Please provide the list of policies that are being referred to?</p>	<p>Necessary details will be shared with the selected bidder only.</p>

<p>General Functionalities - Point 12</p>	<p>Must be able to analyse and report on endpoint compliance status and trends and identify endpoint security exposure and risks.</p>	<p>Please provide an usecase for the same. However this may be achieved by integration.</p>	<p>Compliance status like AV Defn, Patch updates etc and exposure risk like unsecured O.S configuration, vulnerabilities. It should give holistic picture of the compliance as well as risk in the ReBIT environment.</p> <p>Trend analysis report from the Tool should be available.</p>
<p>General Functionalities - Point 14</p>	<p>The solution must be able to identify vulnerable endpoints and software configurations.</p>	<p>Please provide an usecase for the same. However this may be achieved by integration.</p>	<p>We expect that Tool should be able to understand the latest patch / version of AV, OS Patches, applications patch etc. and accordingly, should be able to update the same on Endpoint. We do not expect any Vulnerability scanning Tool incorporated in the solution.</p>
<p>General Functionalities - Point 15</p>	<p>The solution must be able to auto-remediate the endpoints which fails the regulators controls like CIS benchmarks.</p>	<p>Please provide more details and clarity over CIS benchmark</p>	<p>Necessary details will be shared with the selected bidder only.</p>

<p>General Functionalities - Point 16</p>	<p>The solution should provide ability to roll back auto-remediated configurations, policies and patches deployed for fixing vulnerabilities.</p>	<p>Can be achieved by Patch management solution</p>	<p>We would like to have all the modules like compliance, patch, VM into single centralized solution.</p>
<p>General Functionalities - Point 19</p>	<p>It should be able to deliver / provide holistic view of endpoint security posture & should be able to manage and perform Asset management for Lan & remote location (VPN) systems.</p>	<p>What kind of Assets management is required? Can be achieved via 3rd party software's</p>	<p>Solution should provide the details of current endpoint security posture with Patch Operating System and Third-party applications. Automate the deployment and keep track of Assets and Complete Asset management and lifecycle management including the software.</p>
<p>General Functionalities - Point 23</p>	<p>Minimum utilization of network bandwidth while applying patches for vulnerabilities i.e. client should not utilize bandwidth more than 1 MB.</p>	<p>This point is under patch management and need to get it removed from specs</p>	<p>Good to have requirement, however 1 MB threshold is for application and management not for updates and patches, however it application provides the bandwidth capping will be good option.</p>

<p>General Functionalities - Point 27</p>	<p>The proposed solution should be able to retrieve and provide security information irrespective of vendors computing environment.</p>	<p>Please provide use case. What type of Security information is required?</p>	<p>Security information like AV,DLP,Encryption vendor name, version, definition status etc</p>
<p>General Functionalities - Point 33</p>	<p>Administrator should be able to create reports which gives detailed vulnerability result.</p>	<p>Can be achieved via Integration</p>	<p>It is up to the solution provider how they meet the requirements.</p>
<p>General Functionalities - Point 38</p>	<p>Ability to manage clients in different LANs from a central server.</p>	<p>What do you mean by different LAN?</p>	<p>Solution Access / communication should not restrict to one VLAN or Private network, there are changes that there will be many VLAN and network for communication internally. Secondly when client will be connecting from external network, it will connect from VPN, so there should not be any limitation on network for access to console.</p>

<p>General Functionalities - Point 40</p>			<p>Remote installation and uninstallation of client agent on all endpoints (desktop to laptop, servers, physical or virtual regardless of O.S flavours i.e. Windows, Linux & Mac OS and location)</p>	<p>Except Linux on all other OS its possible.</p>	<p>Linux O.S should be supported as in ReBIT, users are using Linux based laptops.</p>
NA	NA	NA	<p>In order to be 100% compliant is it ok that we have mix of products more than one?</p>	<p>It is preferred to have single - centralized solution to achieve all the requirements.</p>	
NA	NA	NA	<p>We suggest to include "MADE IN INDIA" clause</p>	<p>This RFP is not a global tender</p>	
NA	NA	NA	<p>Will you be qualifying bidders on technical criteria or eligibility criteria or based on POC? We suggest it should be based on POC. If POC is successful ReBIT should be flexible on order values, turnover, use cases etc</p>	<p>Refer section 6.2 - Minimum Eligibility Criteria and section 6.3 - Technical Bid Evaluation Criteria.</p>	
3	20	3.10	<p>Subscription cost will be on milestone basis 10% Advance 50% on delivery</p>	<p>No Changes in RFP terms.</p>	

			40% on installation	
3	20	3.10	Implementing cost should be on milestone basis	No Changes in RFP terms.
9	78	9.18	The solution must be able to auto-remediate the endpoints which fails the regulators controls like CIS benchmarks. - Does this mean if the endpoint gets connected to the network which fails CIS benchmarks can Saner quarantine, then patch the system and bring back in compliant state and back in the network or is it that we should have an automated remedy for any deviations that are found during a scan?	Basically the solution should have an automated remedy for any deviations found during scan but if we can quarantine a particular endpoints till it gets compliant then that is also a good feature to have.

9	78	9.18	<p>The solution should be able to scan and give report of unmanaged endpoints. - What is meant by Unmanaged clients here, and does it refer to network monitoring that can discover any unmanaged clients that someone randomly adds to the network, or does it refer to the clients not managed by DC?</p>	<p>The solution should give status of endpoints which are not being managed by the Central server by performing network scan and should give detailed reports of this unmanaged endpoints like patch, AV definition status, 3rd party installed endpoint protection client status etc.</p>
---	----	------	---	--

Note: This document shall form part and parcel of the [RFP](#) and therefore bidders are advised to take the clarifications/responses into account, as applicable, while submitting the bids.

ReBIT Procurement Team
21 May 2020