REQUEST FOR PROPOSAL

For Implementation of Cyber Security Operations Centre

Tender Reference No.	TSCAB/DCCBs/CSOC/072019
Date of Issue of RFP	15.07.2019 10-00 AM
Last date of Submission of RFP Response	25.07.2019 01-00 PM
Last date for submitting Queries	17.07.2019 04-00 PM **(no queries will be entertained after the due date and time)**
Pre-Bid Meeting	17.07.2019 04.00 PM
Responses to the queries	19.07.2019 05.00 AM
Earnest Money Deposit (refundable)	Rs. 1,00,000/- (One lakh only) Payable by DD on in favour of The Telangana State Cooperative Apex Bank Limited (TSCAB), Payable at Hyderabad.
Tender Application Fee (Non-Refundable)	Rs. 10,000/- (Ten Thousands) Payable by DD on in favour of The Telangana State Cooperative Apex Bank Limited (TSCAB), Payable at Hyderabad.
Contact	**Harish B** **Telangana State Cooperative Apex Bank Limited (**TSCAB), **4-1-511/3, Street Number 5,** **Troop Bazaar, Abids,** **Hyderabad, Telangana 500001** **Ph: 040-24685667, 99666 39111** **Email:** infosec@tscab.org
Address for submitting the tender	**CIO Office, 3rd Floor** **Telangana State Cooperative Apex Bank Limited (**TSCAB), **4-1-511/3, Street Number 5,** **Troop Bazaar, Abids,** **Hyderabad, Telangana 500001**
Website For Download	https://tscab.org

1. Objective of the RFP

Telangana State Cooperative Apex Bank Ltd invites bids from short listed bidders for design, implement , operationalize and maintenance of Cyber Security Operations Centre (C-SOC) to provide comprehensive cyber security monitoring and Network management. The selected Bidder will be responsible for implementation of onsite C-SOC, TSCAB campus, TSCAB Buildings, Troop bazar, Hyderabad. Selected Bidder will also supply and install other security solutions and all required infrastructure for operations of the C-SOC as per the broad objectives outlined in scope of work of this RFP.

BUSINESS REQUIREMENTS

1. Objective of proposed solution:

TSCAB would interpret a Cyber Security Operation Center (SOC) as a centralized unit identified in an organization that delivers IT Security Services and deals with security issues at organizational and technical level. It attempts to thwart unauthorized access and manage security related incidents using processes and procedures and that it has distinct modules for event generation, event collection, message database, analysis engines, and reaction management, and preferably uses reputed & standard SIEM, security analytics tools.

TSCAB intends to build a Cyber Security and network Operation Centre (C-SOC) to monitor, assess and defend TSCAB and DCCB's (10 Banks) information systems. The proposed SOC and NOC facility is to be equipped with set of tools such as Security Information and Event Management Tool (SIEM),ARM, Incident Ticket Management, Advance Endpoint,, Network management, Network configuration management ,Server Application monitoring, Ticketing, Incident management, SLA management, Helpdesk tools, etc. given in detail under this RFP and Security Intelligence feeds, for better security monitoring and Network monitor and response capabilities.

Bidders are expected to design, implement and operationalize Cyber Security Operations centre (C-SOC) and other security solutions to provide comprehensive information security monitoring and network management for TSCAB and DCCB's (10 Banks). The selected Bidder will be responsible for designing and implementing **onsite TSCAB campus, TSCAB Buildings, Troop bazar, Hyderabad.** The onsite resources from TSCAB data centre will carry out the C-SOC activities. Selected Bidder will also supply and install other security solutions and all required infrastructure, services for operations of the C-SOC as per the broad objectives outlined in this RFP.

2. Essential business requirements for SOC, NOC and other security solutions:

The C-SOC should cover proposed solutions and existing information assets at Primary data centres Hyderabad, DR data centre, Noida.

TSCAB expects bidders to provide full-fledged Services including but not limited to Supply, design, implementation, configuration, customization, integration, monitor, backup, documentation, training, warranty support, post warranty maintenance support, back to back arrangement with OEM and any other activities and services related to or connected to the Information Technology , Monitoring, Cyber security & related solutions. The bidder is expected to do following but not limited to:

a. Supply, design, implementation, and monitor SOC and NOC and other security solutions.
b. Supply, installation and configuration of LED screens, desktop workstations, TOR switches, video matrix switches, etc. required for setting up of C-SOC centre at TSCAB campus, Hyderabad.

c. Security monitoring of attacks into/on/against TSCAB's IT assets.
d. Manage security, configuration, availability, performance and fault management, advisory for the security devices and its software stipulated in scope.
e. Design and implement SIEM by integrating various devices (Firewall,server,router and etc) and including threat intelligence feeds among them.

f. Provide feeds in threat intelligence ON SIEM
g. Ensure malware scanning, protection, presentation, and reporting as required by TSCAB.
h. Dashboard for reporting and SLA management.
i. Monitoring entire network, links, systems, devices, applications, etc. for availability, performance, SLA and other parameters using tools.
j. Provide helpdesk, ticketing tools to facilitate proper governance of helpdesk activities.
k. Manage and maintain all the proposed security devices/solutions with the help of dedicated onsite team.
l. Fix and comply with all the audit observations with respect to C-SOC and other security solutions on time bound manner.

3. Requirements for Design and Implementation of SOC and NOC

The C- SOC model intended to setup by TSCAB and DCCB's (10 Banks) is Onsite model, where entire C-SOC will be setting up at TSCAB campus Hyderabad. Bidder will be responsible for designing the C-SOC architecture. After getting approval from SEBI, bidder will implement the said architecture. Bidder/OEM will also review the said architecture periodically, suggest, and implement any changes if required to SEBI.

A. The bidder shall implement other security solutions such as SIEM /security monitoring l, vulnerability monitor, etc. covering entire offices and data centers of TSCAB and DCCB's. The Onsite and remote resources(if any) (People, Process and Technology) support required to run and manage the C-SOC by TSCAB resources and other security solutions shall be deployed

B. **Bidder should quote all the latest versions (current line) of products, software's, hardware, servers, appliances, etc. The quoted products, software, hardware, servers, appliances, etc. should not be declared as end of sale, end of support during next 5 years from the date of issue of purchase order.**

C. **The bidder should provide required reporting tools, helpdesk tools, ticketing tools, SLA monitoring** tools, Case management tools, backup and archival solution for storing logs, data, configurations, etc. for C-SOC and other security solutions proposed as part of this project.

D. The bidder should configure all the existing, proposed and newly procured network, security devices, servers, etc. for network monitoring, performance, uptime, etc. to carryout seamless NOC operations. Bidder should provide all the licenses, software, API's, tools required for successful configuration of existing , proposed and newly procured devices , applications, solutions, etc.

E. Bidder should provide upgrades, updates, patches, bug fixes and carry out its implementation without additional cost to TSCAB during the implementation period. The bidder should ensure that after patch installation the integrated C-SOC set up, integrations among other products, security orchestration should function properly.

F. All the components of C-SOC and other security solutions proposed should have back to back support agreement from the OEM for a period of 5 years from the date of acceptance of complete solution.

G. The licenses /activation keys for all the components of C-SOC, other security solutions proposed as per the scope of work should be valid for a period of 1-year at least from the date of acceptance of complete solution. The bidders should suitably factor the license validity accordingly.

H. The proposed IT helpdesk, incident management, ticketing and SLA management tools should be configured for both NOC & SOC and should be integrated properly .The roles, responsibilities, workflow automation, authorization, etc. should be defined properly for each set of users, teams (onsite SOC team, onsite NOC, team, onsite device management teams, other service providers teams within TSCAB, end users, etc.). The access to such helpdesk, ticketing and SLA tool should be provided to other system integrators helpdesk teams stationed at TSCAB for handling other projects (such as portal ,network , IMSS, DMS, website, helpdesk teams, etc.) in TSCAB for call logging, monitoring, call resolution etc.

I. The bidders should configure all the SLA parameters (as mentioned in this RFP) in the SLA monitoring tool.

J. Bidder should also configure SLA parameters, reports in the proposed SLA monitoring tool for other project components of TSCAB managed by other service providers.

K. All the components of NOC, SOC and other security solutions should support IPV6 address from day one. The required licenses for supporting IPV6 should be provided from day one. Bidder should configure IPV6 addresses if needed.

L. All the existing components and proposed solution components' clock should be synchronized with latest version of NTP. Also the bidders should regularly check whether NTP is functioning properly or not.

M. The bidder should provide product/solution wise Architecture diagram for all the proposed products/solutions and services.

N. Bidder should provide consolidated architecture diagram consisting of all products, solutions and services for C-SOC.

O. If TSCAB/DCCB's procures, new devices/applications during the intial support period (1 Year) then bidder should configure and monitor these devices/applications under SOC and NOC operations without additional cost to TSCAB/DCCBs.

Brief Scope

The selected vendor needs to supply, implement and support **state wide Cyber Security Operations Centre (CSOC) for 10 Banks, which are Telangana State Cooperative Apex Bank (TSCAB) and 9 (Nine) District Cooperative Central banks (DCCB's) of Telangana state and associated Primary Agriculture Cooperative Credit Societies (PACS).**

The Selected vendor needs to take the **full responsibility of Implementation, Configuration, integration, training and support for Cyber security operations Centre**.

Vendor is required to respond to this tender for the required material & Services as per the detailed scope/Bill of Material as mentioned.

Hardware, networking:

- Vendor should be in a position to supply, implement and support **state wide Cyber Security Operations Centre (CSOC) for Telangana State Cooperative Apex Bank (TSCAB) and 9 (Nine) District Cooperative Central banks (DCCB's) of Telangana state and associated Primary Agriculture Cooperative Credit Societies (PACS).**

- Server Hardware for CSOC Components implementation as per technical specifications given in **the same document.**

4. SCOPE of work for SOC and other security solutions:

The broad scope of work for SOC and other security solutions includes:

A. **Supply, install, implement, integrate, customize, manage, upgrade and maintain security solutions, tools, technologies and services as mentioned below to meet TSCAB and DCCB's requirements:**

a. SIEM with threat intelligence feeds
b. Network performance and configuration management
c. Network traffic Analyzation.
d. Vulnerability Scanning Solution
e. Advanced End Point Protection solution for endpoints and servers
f. log Capture solution
g. Authentication response manager.
h. Setting up and implementation of NOC& SOC

SOC SOLUTION –DETECTION and RESPONSE

Bidder is expected to perform the following SOC operations but not limited:

1. Perform security gap analysis for existing security and Network architecture and help TSCAB/DCCBs to plug those security gaps or mitigate the same using proposed security products/solutions. This should be done pre and post project implementation.
2. Identification and classification of all systems in TSCAB based on criticality.
3. Develop, update and maintain log baselines for all platforms at the TSCAB that are required to be monitored.
4. Configure all systems to generate detailed event logs.
5. Design and configure security orchestration model for advance threat detection and mitigation, threat hunting by integrating various security devices and sharing threat intelligence feeds among themselves using API integrations,
6. Collect, store, analyse and act on logs generated by systems
7. Collect and store configuration data from various C-SOC and targeted devices/systems and use it for detailed analysis, identifying gaps, correlation, forensic and reporting.
8. Proposed solutions Monitor security logs to detect malicious or abnormal events and raise the alerts for any suspicious events that may lead to security breach in TSCAB/DCCB's environment
9. Manage and coordinate response to such incidents and provide personnel for managing the security monitoring service.
10. Configure need based access to systems, databases, networks, etc.
11. Review, patch, update /upgrade of proposed systems on a continuous basis.
12. Coordinate the activity of monitoring the Internet to proactively identify spam/phishing emails, web sites and other threats in the name of the TSCAB/DCCBs and facilitate coordination
13. Offered solutions should detect security attacks on IT infrastructure, bidders should also monitor for security events on business applications, databases and also identify user entity behaviour analysis.
14. Bidder should configure action rules to monitor, detect and manage incidents for the following minimum set of IT infrastructure security events but not limited to:
    a. Buffer overflow attacks

b. Port & vulnerability scans
c. Password cracking
d. Worm/virus outbreak
e. File access failures
f. Unauthorized server/service restarts
g. Unauthorized changes to firewall rules
h. Unauthorized access to systems
i. SQL injection
j. Cross site scripting
k. Anonymous Web Traffic
l. Auditable Events Change Policy Violation
m. Authentication Attempt - Default Account
n. Authentication Attempt from Potential Threat from Threat Intelligence Feed
o. Authentication Traffic but No Agent
p. Continuous Excessive Logon Failures
q. Correlated File Deleted
r. Critical Account Logon Failures
s. Database User Change
t. File Audit Failure with Restricted Information Inference File Audit with Restricted Information Inference Firewall Logon Failure with Inference
u. Generic Worm Behaviour
v. InternalUserLogonFailure with Inference
w. Machine Removed from Group
x. Machine Removed from OU
y. MSSQL Critical Account Logon Failure
z. MSSQL Database Change Attempt
aa. MSSQL DB Error or Exception
bb. MSSQL DB Object Change Attempt
cc. MSSQL DBCC Command Issued
dd. MSSQL Duplicate Connection Attempt
ee. MSSQL Security Error
ff. New Critical Group Member
gg. New Machine Created-Enabled
hh. New User Created-Enabled
ii. Non-Admin Server Logon
jj. Policy View-Change
kk. PortScans
ll. Remote Windows Server Logon
mm. SQL Injection Attempt
nn. SSH Logon Failure with Inference
oo. SSH2 Brute Force Tool
pp. Suspicious DNS Traffic
qq. Time Synchronization Failure
rr. Unpatched Vulnerability Found
ss. User Account Created
tt. User Account Deleted

uu. User Account Events
vv. User Account Lockout
ww. User Account Properties Update
xx. UserLogonFailure with Inference
yy. Vendor - Account Logon Failure
zz. Virus Attack - Bad State
aaa. VPN Logon Failure
bbb. Windows Batch Logon Failure with Inference
ccc. Windows Event Log Cleared
ddd. Windows Logon Failure with Inference
eee. Windows Network Cleartext Logon Failure with Inference
fff. Windows New Credentials Assigned Logon Failure with Inference
ggg. Windows Workstation Unlock Logon Failure with Inference
hhh. Worm Activity

15. Proposed solution should carry out correlations amongst the logs from multiple sources to detect multi-vector attacks using security analytics tool.
16. Should detect and mitigate advance real time attacks using Decoy and Deceptive technologies.
17. Bidder's should showcase alerts with details of mitigation steps to designated personnel within TSCAB/DCCBs and any identified service provider of TSCAB/DCCBs.
18. Bidder should provide coordinated rapid response to any security incident. Bidder should contain attack & coordinate restoration of services. While vendor personnel will enlist support of other service providers in TSCAB/DCCBs, primary responsibility for incident response will be with the bidder.
19. Bidder should display on how to maintain a knowledge base of alerts, incidents and mitigation steps and this knowledge base should be updated with evolving security events within and outside TSCAB/DCCBs.
20. Evidence for any security incident should be maintained in tamper proof manner and should be made available for legal and regulatory purposes, as required.
21. Bidder should display add/delete/modify rules, reports and dashboards based on requirements; however, track of these rules needs to be maintained in tamper proof environment.
22. Bidder provided solution should have MIS reports to TSCAB/DCCBs on daily, weekly and monthly basis. Reporting requirements will be finalized with the selected bidder. Bidder provided solution should also have the provision to provide reports on demand whenever required by TSCAB/DCCBs.
23. Bidder should educate teams on conduct forensic analysis for security incidents to enable identification of perpetrators and their methodologies.
24. Perform vulnerability scanning on regular basis or as per the TSCAB/DCCBs requirements. Fixing these vulnerabilities in coordination with respective asset owners.
25. Bidder should configure and provide training on ARM solution for all the existing, proposed and newly procured devices.
26. Bidder should implement DLP, UEBA solution to detect and prevent sensitive data loss and detect insider threats.
27. Detect and respond TSCAB/DCCBs IT resources from denial of service type of attack, etc.
28. Detect and respond TSCAB/DCCBs from all DNS related attacks.
29. Design, implementation and management of encryption for desktops, servers and removable devices using Microsoft bit locker solution.
30. Bidder should bring workflow processes. Bidder should integrate the workflows including incident management, escalation management, reporting etc. with the process management system in existence at the TSCAB/DCCBs from time to time.

31. Bidder should showcase manage the log storage including online, offline and archival systems for the logs.
32. Bidder should display how to carry out system administration tasks including regular backup of system, restoration, installation, health check and other maintenance activities for the supplied systems.
33. Bidder should manage any faults in the proposed solution by trouble shooting and coordinating with the OEM/principle on call basis.
34. Bidder should support implementation of proposed solution with the following activities: Review of architecture, program management of implementation, skill acquisition on the tool. Bidder should support such activities any time that it is required during the contract period.
35. All deliverables including reports should undergo quality assurance process. Bidder team lead should define quality metrics, measurement frequency and reporting periodicity in consultation with TSCAB/DCCBs.
36. Team lead should review reports, operating procedures, administrative activities on a daily basis to identify quality issues.
37. Solution should have periodic quality assurance reports to TSCAB/DCCBs as per the reporting frequency designed.
38. Bidder should provide backend support to the TSCAB/DCCB team. Such support at the minimum include:
    - for adding new/updated threat scenarios and other best practices in TSCAB/DCCBs proposed solution for detection & response based on bidder's visibility & experience across other customers
    - development of new connectors for TSCAB/DCCBs business applications and new devices
39. Bidder should ensure continuous training and best practice updates for TSCAB/DCCBs team from its backend resources.

General Instructions, Terms and Conditions

The Tender document meant for the exclusive use of Tendering as per the stated specifications, terms and conditions. The intended tender shall not be transferred, reproduced or used for any purposes.

TSCAB holds the copyright for this document. Any dissemination, copying, reproduction, transfer [digital/non-digital] and/or distribution of the same by any means including digital transmission over the networked telecom infrastructure, to other than to whom this document is meant or using it for any purpose other than for the purpose for which it is meant is strictly prohibited.

The tender is not an offer but an invitation to receive Tenders' response. No contractual obligation whatsoever shall arise from the tender process unless and until a formal contract is signed and executed by duly authorized officers of the Bank and the Vender.

The Bank shall not be responsible for the accuracy or completeness of such information and/or interpretation.

Any information related with this 'process' beginning from the issuance of this document till the process is fully accomplished (till the finalization of vendor) will be informed through e-mail, so give valid e-mail ids & contact numbers of the authorized persons.

The bidders may be in touch with the Bank for latest updates through email.

The Bank reserves the right to stop or cancel whole or part of the process at any time without notice to Vendors and the Bank is in no way liable to the vendor or anyone coming across this document, or participating in the process.

General Information

Bank is looking for well-proven OEM branded software/hardware products, which is volume produced and are used by a large number of users in India. All products quoted should be associated with specific model numbers and names and with printed literature describing configuration and functionality. Any deviations from the printed specifications should clearly identifiable in remark column. The same will verify under technical evaluation.

Requirements and Specifications

- Security information and event management
- Network performance monitoring
- NetFlow traffic analysation,
- IT Incident ticketing management
- Network configuration management
- Syslog management
- Vulnerability Assessment
- Advanced End point protection.
- Access rights management

- The proposed components will have to supply with all the software drivers, if any, and manuals. The version of software delivered with the equipment should be the latest one available in the market. All pre-requisites required for running equipment proposed should be included in the proposal.
- For details of software/hardware/Networking requirements at Datacentre, vendors should refer to Bill of Material mentioned in this tender document.

Other Instructions

1. All proposals submitted for products and services requested herein must include a detailed description. **Vendors should clearly spell out the associated warranties, support and any other relevant information**.

2. Bank reserves the right to consider special or unique features, which may be included in the proposal. Bank also reserves the right to determine selection process.

3. Bank reserves the right to enter into a contract based upon proposals received without further discussion of such proposals. Accordingly, proposal should submit with the Vendor's best price, delivery and service capabilities. Bank will select proposals with which to negotiate and reserves the right to enter into a contract with a Vendor that may not necessarily be lowest in fees charged.

4. The vendor must provide complete installation of the hardware and its related software, ensure proper system performance, and complete acceptance testing of the various systems as per Acceptance Testing Procedure acceptable to the Bank.

5. The Vendor shall, defend, indemnify, and hold harmless the Bank, their officers, and agents from and against any and all claims, demands, causes of action, orders, decrees, or judgments for injury, death, damage to person or property, loss, damage, or liability of any kind (including without limitation liability under any law occasioned by, growing out of, or arising from
   (a) the performance of any product or service to be supplied by the Vendor, or
   (b) by any act, error or omission on the part of the Vendor, its agents, employees, or subcontractors, and or
   (c) any failure to fully comply with all applicable laws and regulations by the Vendor, its agents, employees, or subcontractors. The Vendor shall also indemnify Bank from any claims arising out of any Intellectual Property

Dispute arising out of the usage of any software supplied by the Vendor. The Vendor shall provide complete information of the Vendor's corporate structure and chain of liability for Software or any other components of the Solution or infrastructure. Expenses for developing the proposals and answering Bank's questions are entirely the responsibility of the Vendor and shall not be chargeable, in any manner, to Bank.

6. Vendor will abide by all applicable Indian laws and regulations and will obtain (or demonstrate current possession of) any and all permits, licenses, certifications or other approvals that may be required and/or appropriate for performing services hereunder.

7. A Committee formed by Bank for the purpose of evaluation will review all proposals. Trade secrets, test data, or other similar proprietary information will remain confidential on a best effort basis provided such material is clearly marked as such. Any portion of the proposal, which can consider a trade secret in the context, should be so marked.

8. Vendors must identify by name, title, and telephone number and e-mail address of the person(s) in their organization to whom Bank can address questions during the evaluation of proposals.

9. Vendors must provide specific information on any warranties/guarantees provided and state the terms and conditions of the warranties/guarantees that offered. It is important for Vendors to note that Bank will require appropriate guarantees for timely completion of the project as well as guarantee of on-going support for maintenance as well as major and minor upgrades, Patch releases, product changes etc.

10. The Vendor is and shall perform these services as an independent contractor, and as such, shall have and maintain complete control over all of its employees, agents, and operations. Neither the Vendor nor anyone employed by it shall be, represent, act, and purport to act or deemed to be the agent, representative, employee or servant of the Bank.

11. The Vendor selected because of this Request for Proposal will be working as an independent contractor and will be required to take out and keep in force all permits, licenses, certifications, other approvals, and or insurance that may require by the Bank, any local or regional governmental agency, or the Union of India. Failure to comply with any of these items would be grounds for immediate cancellation of the contract.

12. Applicable warranties to any products purchased because of this proposal request must be clearly specified. The location or agent responsible for servicing this account must be clearly stated. In addition, the vendor must provide complete information and pricing on maintenance agreements available and recommended for this system after the warranty period. The vendor's policy on equipment, software upgrades, enhancements, and on-going support shall also be addressed. **Warranty and maintenance terms and costs may be taken into consideration in the award.**

13. Bank shall be saved harmless by the vendor from payment of any and all claims arising out of any infringement, alleged infringement, or use of any patent or patented device, article system, arrangement, materials, or process used by them in the execution of this contract.

14. In the event that information or pricing submitted by the vendor is unclear, Bank may request additional explanation and/or pricing breakdowns from the vendor for the purpose of evaluation and decisions. The vendor shall answer requests for additional information or clarification in writing, and these responses will become part of the vendor's proposal. Vendors failing to provide adequate information on any issue in a timely manner to allow a comprehensive evaluation by Bank shall be considered unresponsive, and their proposal subject to rejection.

Eligibility of Bidder

The bidder must evidence each applicable criterion by submitting the photocopies and/or original legal-evidential documents, which are clear, visible, in English language. The proposals submitted, if do not satisfy these criteria, as applicable to the proposals being submitted in response to the Tenders will be rejected outright.

Only those bidders who fulfill the following criteria are eligible to respond to the Tender.

Eligibility Criteria:

1. The bidder must be a Registered Company and having IT Operations for minimum period of 5 Years.
2. It is mandatory for the bidder to quote for all the items mentioned in the RFP, failing to do so would result in the disqualification of proposal/vendor.
3. The bidder should have support/service centre in Hyderabad.
4. The bidder should be OEM/Authorized Partner of the software and hardware components as per BOM.
5. Tender includes software, Hardware and Networking components. Only OEM/Authorised Partner of software and hardware components (servers) can apply for the tender.
6. All servers, & Software's mentioned in BOM must be quoted as single tender.

Cost of Tendering:

The Vendor shall bear all costs associated with the preparation and submission of its Tender. The Bank shall in no case be responsible or liable for these costs, regardless of the conduct or outcome of the Tendering process.

The Tender responses of unsuccessful vendors will not be returned.

The Vendor should carefully study all instructions, forms, terms and conditions and specifications in the Tender Document. Failure to furnish full information prescribed in the Tender Document or submitting a Tender not substantially responsive to the Tender Document in every respect may result in the rejection of the Tender.

The Vendor shall not, without the Bank's prior written consent, make use of any document or information enumerated in the Tender Document except for the purposes of performing the Contract.

Any publicity by the Vendor in which the name of the Bank is to be used should be done only with the explicit written permission from the Bank.

Clarification of Proposals

For purposes of scrutiny, evaluation and comparison of offers, the Bank may, at its discretion, ask vendors for

clarifications on any of the clauses in their proposals. The Bank has the right to disqualify the vendor who does not respond to its request for clarification or whose clarification renders the proposal unsuitable for the proposed project. The decision of the Bank in this regard shall be final and no correspondence on this matter will be entertained.

Tender Price

Prices quoted by the vendor shall remain fixed during the Contract period and shall not be subject to variation on any account, including exchange rate fluctuations, changes in taxes, duties, levies, charges, etc. A Tender submitted with an adjustable price quotation will be treated as non-responsive and will be rejected.

All proposals must include taxes, duties, octroi, levies, etc. of any kind that may be applicable. Any such amounts shall be shown separately. If not shown, they will be considered an expense of the Vendor. No additional charge will be considered unless specifically mentioned in the offer. Prices quoted will be inclusive of transportation and comprehensive insurance till the equipments reach at the respective sites as specified by the Bank. The offer should be only in Indian rupees and should be inclusive of supply, installation and commissioning of the equipment. All prices should be itemized. Unit prices should be given for every item or part offered.

Warranty and Annual Maintenance Contract (AMC):

All equipment delivered under this contract shall be warranted for trouble free performance for a period of 36 months starting from the date of commissioning. The word warranty in this document refers to “Comprehensive Onsite Warranty” offered by OEM.

The vendor shall warrant that all goods supplied under the contract are new, unused and of the most recent or current models and shall incorporate all latest improvements in design and materials.

The vendor should indicate the Annual Maintenance Charges for the equipment along with the terms and conditions and should be committed for a period of 3 years from the date of expiry of warranty.

Tender Security (EMD)

The Vendor shall furnish Refundable Tender Security (EMD) by way of demand draft in favour of The Telangana State Cooperative Apex Bank Limited (TSCAB), issued by a nationalized bank or Schedule Bank for a sum of Rs. 1, 00,000/- (Rs. One lakhs only) and shall remain valid for sixty (60) days beyond the validity of the Tender.

Unsuccessful Vendors' Tender Security (EMD) will be discharged or returned after the expiration of the period of Tender validity prescribed by the bank.

The successful Vendor's Tender security will be discharged upon the vendor signing of the Contract, furnishing the successful implementation, and training document.

The Bank on Tender security amount will pay no interest

Any contravention of the terms of this Tender will result in forfeiture of the Tender security apart from other legal remedies that may be sought

Tender Currency

Tenders are to be quoted in INR - Indian Rupee only.

Tender Forms

The Vendor shall complete the Tender Response Forms and the Commercial Response Forms furnished in the Tender Document.

Period of Validity of Tenders

Tender shall remain valid for a period of 60 days from the date of opening of the technical Tender. The Bank shall reject a Tender as non-responsive if it is valid for a shorter period.

In exceptional circumstances, the Bank may solicit the Vendors' consent for an extension of the period of validity. The request and the responses thereto shall be made in writing. The Tender security provided shall also be suitably extended. However, a Vendor may refuse the request for extension without forfeiting its Tender security.

Signing and Submission of Tender

The technical offer of the RFP response should be submitted in two copies.

Participation in the Tendering process implies giving consent to all the terms, conditions and other requirements contained in any part of the Tender document.

The Tender shall be typed or written in indelible ink as instructed in respective parts and shall be signed by the vendor or person or persons duly authorized to bind the vendor to the Contract. The person or persons signing the Tenders shall initial all pages of the Tenders.

Any interlineations, erasures, or overwriting shall be valid if only they are authenticated by full signature of the person signing the Tenders.

Proposals for Technical Bid and Commercial Bid are to be sealed in separate envelopes and submitted to the address given below. All the envelopes must be super-scribed with the following information:

- Type of Offer (Technical or Commercial)
- Due Date
- Name of Vendor

ENVELOPE – I (Technical Offer-T.O.):

The Technical offer should be complete in all respects and contain all information asked for, except prices. The T.O. should include all items asked for in the attached Annexure. The technical offer should not contain any price information. The T.O. should be complete to indicate that all products and services asked for as quoted. Where available, the vendor should clearly indicate the product code/part no. For example, the Technical Offer should mention that AMC charges are included in the Commercial Offer, without mentioning the actual amounts in the T.O.

ENVELOPE-II (Commercial Offer-C.O.):

The Commercial Offer (C.O.) should give all relevant price information in Indian Rupees and should not contradict the T.O. in any manner.

These two envelopes containing the Technical and Commercial Offer should be simultaneously submitted. Please note that if any envelope is found to contain both technical and commercial offer, then that offer shall not be considered.

If the envelopes are not sealed and marked as indicated above, the Bank will assume no responsibility for the Tender's misplacement or premature opening.

The envelopes duly sealed should be submitted on or before 1.00 PM on 25.07.2019 at the address given below:

To
CIO Office
Telangana State Cooperative Apex Bank Limited (TSCAB),
4-1-511/3, Street Number 5,
Troop Bazaar, Abids,
Hyderabad, Telangana 500001

Proposals may not be withdrawn after submission and shall be valid for a period of 60 days from the date of submission as mentioned above.

Vendors submitting the Tenders through postal/courier services should ensure that the Tenders are received in the Bank's office well before the deadline set for receiving of the tender proposals.

The Bank is not responsible for Postal/Courier delay, non-receipt, non- delivery of documents/proposals, loss of documents in transit etc., whether it is supposed to sent/received, by the Bank or the vendor or supposed to be transmitted electronically, including loss of documents/information during transit/transmission.

Late Receipt of Tenders

Any Tender received by the Bank after the prescribed deadline for submission of Tenders will be rejected.

Opening of Technical Tenders by the Bank

The technical proposals will be opened by the banks internal committee on the date mentioned above. The vendors, if they wish, may remain present on the day of opening of Technical Response. The internal committee as per eligible criterion will inform the eligible vendors for further process after the post technical evaluation.

Evaluation and comparison of Tenders

Only those Tenders, which have been determined to be substantially responsive and meet the eligibility criteria and are complete in all respects, will proceed to the stage of being fully evaluated and compared.

The Bank may, at its discretion, waive any minor non-conformity or any minor irregularity in the offer. This waiver shall be binding on all the vendors and the bank reserves the right to exercise such waivers.

The evaluation criteria, which will be adopted by the Bank to evaluate the complying responses, will include (illustratively only):-
The content, clarity, completeness, transparency and quality of the responses vis-à-vis its veracity with system demo

- The Vendor's ability to supply and deploy & support the required components within the project schedule expected by the Bank.

- Vendor's proven track record in providing and implementing similar solutions
- Vendor's financial stability and capability to sustain in this critical competitive business environment.
- Vendor's capabilities in delivering projects on time and on budget, without disrupting normal ongoing business activities.
- The ability to provide support the solution effectively.
- The technical qualifications and reputation of the Vendor.

Evaluation of Technical Tenders

The Bank may require the Vendors to make technical demonstration regarding the various aspects of the proposed solution. This process will also enable the Bank to clear up issues that may be identified from the Tenders' response. All expenses for such demonstrations will have to be borne by the Vendors.

Technical evaluation will have multiple phases' viz., detailed study of proposals, the technical tender responses, solution presentation and/or site visit analysis. Those who qualify technically may be invited for a presentation. The site visit of only those vendors may be conducted who have qualified in the result of technical presentation.

The Bank will prepare a short-list of technically qualifying vendors and the commercial offer of only short-listed vendors will be opened.

Evaluation of Commercial Tenders

The Commercial offer of only short listed technically qualified bidders will be opened and evaluated by the Bank.

The evaluation will be done based on techno-commercial response.

If, during evaluation of the financial/commercial Tenders, there is a discrepancy between words and figures, the price expressed in words shall prevail over the price stated in figures. If the Vendor does not accept the price expressed in words, its Tender will be rejected, and its Tender security shall be forfeited.

Bank may negotiate with the short-listed bidders responding to the Tender, to serve the best interests of the Bank. In the event if the Bank is unsuccessful in negotiating a contract with the apparent best vendor within a reasonable time frame, Bank may begin negotiations with another vendor. Vendors are cautioned, however, to submit proposals initially on a most favorable basis, since an award decision may be made without any negotiation, based on price and terms of the original proposal.

Contacting the Bank

All contacts with Vendors will be documented in a transparent and unbiased manner.

No Vendor shall contact the Bank and or its technical advisors on any matter relating to its Tender after the opening of the Tender until the contract is awarded to the successful Vendor.

Any effort by a Vendor to influence the Bank in its decisions on Tender evaluation, Tender comparison or contract award shall result in disqualification of the Vendor.

Notification of Award

After negotiating with the short-listed vendors & prior to the expiration of the period of Tender validity, the Bank will notify to the successful Vendor in writing or by facsimile that its Tender has been accepted.

The notification of award will constitute the formation of the Contract. The vendor should respond within 5 days from the date of acceptance of tender.

Upon signing of the contract by the successful Vendor, the Bank may promptly notify each unsuccessful Vendor.

No correspondence will be entertained from the unsuccessful vendors and Bank's decision for selecting the vendor will be final and binding on all the vendors.

Bank reserves the right to select or reject all proposals if they do not match with the Bank's expectations.

Signing of the Contract

The bank and the successful Vendor may negotiate on the Contract form and service level agreements before signing the contract.

The Bank shall send to the successful Vendor the Contract Form incorporating all the terms of the agreement based on which the Bank and the successful Vendor will negotiate terms of Service Level Agreement. Final agreed SLA will be signed by both parties.

Performance Security (Bank Guarantee)

Within thirty (30) days after the Vendor's receipt of Notification of Contract Award, the Vendor shall furnish Performance Security to the Bank for an amount of Rs. 5,00,000 (Five Lakhs Only) for the due and punctual performance and fulfilment of the contract.

Failure of the successful Vendor to comply with the requirement of signing of contract and performance Security shall constitute sufficient grounds for the annulment of the award and forfeiture of the Tender security, in which event the bank may make the award to the next lowest negotiated evaluated Vendor or call for new Tenders.

The Performance Bond may be discharged by the Bank upon being satisfied that there has been due performance of the obligation of the Vendor.

The Bank shall notify the Vendor in writing of its invocation of its right to receive such compensation within Fifteen (15) days, indicating the contractual obligation(s) for which the Vendor is in default.

The proceeds of the performance security shall be payable to the Bank as compensation for any loss resulting from the Vendor's failure to complete its obligations under the Contract.

The Performance Security shall be denominated in INR only, and shall be in one of the following forms: a) A bank performance guarantee issued by a schedule bank or b) A banker's cheque / demand draft favoring the Bank **and payable at Hyderabad.**

The performance security/EMD will be discharged by the Bank and returned to the Vendor not later than 30 days following the date of completion of the Vendor's performance obligations, including any warranty.

Payment Terms

Payment shall be made in INR - Indian Rupee on submission of commercial invoices.

- 70% the tender value will be released on delivery and installation of the components/equipment
- 20% of the tender value will be released on complete configurations, providing training along with documents and commissioning.
- 10% of the order value to be retained until submission of the performance guarantee for a period of 1-year.

Prices

Amount payable to the Vendor as quoted in the Price Schedule shall be firm and not subject to adjustment during performance of the Contract, irrespective of reasons whatsoever, including exchange rate fluctuations, changes in taxes, duties, levies, charges, etc. All prices will be valid during the currency of the Agreement.

Delivery of Material

Vendor shall deliver all the Hardware/networking equipment at the respective sites within 5-6 weeks from the date of receiving the Purchase Order. Bank would communicate the vendor for delivery of the material if any delays in DC build.

Vendor shall install and commission all the Hardware equipment within 2 weeks after the delivery/powered-on. The vendor shall provide packing of goods in such a manner as to prevent their damage or deterioration during transit to the final installation site. The packing shall be sufficient to withstand, without limitation, rough handling during transit and exposures to extreme temperatures, humidity, sleet and precipitation during transit and open storage.

The vendor will make provision for the entry permits on site basis wherever applicable and the vendor will pay any tax that will be required to borne for allowing the goods to enter the city in which the site is located.

At the discretion of the Bank, there will be acceptance test conducted by the vendor in presence of the Bank officials and or its nominated consultants. In case of serious discrepancy in hardware/software supplied, Bank may cancel the entire purchase order and return the equipment back to the vendor.

Delivery locations for hardware:

DC Address: CtrlS Datacentre, Hyderabad.

To start with, DC hardware should be delivered/mounted/installed @DC location only. Vendor should take all the necessary measures including expenditure required for the safe and secure shifting.

In case of short shipment of hardware or networking or media etc on delivery, payments would be delayed till the completion of short shipment.

Penalty for non-adherence to the Time Schedule

The time schedule for each item of deliverables will be annexed to the agreement. The Vendor shall be responsible for maintaining timeliness in implementation of the project.

Penalty for delays in completion of the project will be levied @ Rs. 50,000/- (Rupees Fifty thousand only) per week of delay, subject to a maximum of 10% of contract value, after which the Bank reserves the right to appropriate the performance security in portions or in full.

Installation of Material

Vendor shall complete the installation, configuration & operationalisation of the operating system and all other related system software required for the performance of the servers and equipment supplied as per this tender at the DC or any other alternative locations as stipulated in the Purchase Order within 15 days of getting clearance for commissioning from Bank. Bank will provide the clearance for commissioning, within a period of 30days from the delivery of the Equipment defined in the tender.

Vendor shall submit a Completion Report duly signed by authorized representatives of the Bank, to Information Technology Services Department (ITSD) of the Bank. The report should contain inter alia, date of delivery, date of installation at the specified location and date of start of warranty for all the Equipment defined in the tender, installed at the stipulated locations, as soon as the entire installation is completed.

The Bank reserves the right to stop or cancel whole or part of the process at any time without notice to Vendors and the Bank is in no way liable to the vendor or anyone coming across this document, or participating in the process

After submission of responses, any material change in the membership of such above third parties/vendors in the proposal, or in their responsibility or commitments the same is subject to approval by the Bank.

The Bank intends that the Vendor appointed/selected under this Tender shall be single point of contact, and responsibility to fulfil all the obligations, notwithstanding the fact that the Vendor may appoint/procure services of third party suppliers to perform all or part of the obligations under this Tender or subsequent agreements.

Such Vendor is expected to co-ordinate with the Bank's existing or future other Vendor's, including their third party vendor/s, especially hardware and software. The Bank does not expect any Vendor to point towards another for any type of failures or deficiencies.

Vendor must co-operate with any of the Service Provider's/vendors or vendors whom the Bank may appoint during

the contract period. Vendor's must provide required information or required technical assistance to such vendors including assisting them in any type of interface requirements, without any additional costs to the Bank.

Each Vendor can submit only one proposal for this Tender. Similarly, only any one of the group companies including sister concerns of Vendor can submit proposals under this Tender. If it is found that any two Vendor are part of the same group or sister concerns, both the Vendors will be disqualified at any stage of this process as deemed fit by the Bank.

Taxes and Duties

The Vendor shall be entirely responsible for all applicable taxes, levies, charges, license fees, royalties, etc. payable to any government or agencies or co-vendors or any sub-contractor.

Income / Corporate Taxes in India

The Vendor shall be liable to pay all corporate tax, income tax and any other tax that may be levied in accordance with Indian law. The Bank's liability is restricted to the payment of charges to the Vendor as per SLA.

Wherever the laws and regulations of India require deduction of any taxes at the source of payment, the Bank shall effect such deductions from the payment due to the Vendor. The Bank shall remit such monies to the competent authority and furnish certificate of deduction as provided in the relevant law under which such deductions are made.

Integrity

The Vendor is responsible for carrying out all activities in accordance with the agreement using latest machinery, programs and economic principles and using all available means to achieve full and complete performance of its obligations under the agreement.

Vendor's obligations

1. The Vendor is obliged to: (a) work closely with the Bank's staff and other agencies involved, (b) act within its own authority, and (c) abide by directives issued by the Bank for the execution of the Agreement. The Vendor shall follow industry 'Best Practices'.

2. The Vendor shall abide by the job safety measures prevalent in India and will exonerate the Bank from all demands or responsibilities arising from accidents or loss of life caused by the negligence of the Vendor. The Vendor will pay all indemnities arising from such incidents and will not hold the Bank responsible.

3. The Vendor is responsible for managing the activities of its personnel and will be held answerable for any misdemeanours of its staff. The Bank shall not be responsible for the misconduct of the Vendor's employees. Under no circumstances shall the Vendor's employees be treated as employees of the Bank.

4. The Vendor shall promptly provide any information relating to the outsourced work as may be required by the Bank.

Documentation

The Vendor to provide all relevant documentation in respect of all the products, services. Illustratively these can be user manual, troubleshooting manual etc. All such documents/manuals should detail the operational procedure and possible consequences of the deviation from such operational procedure.

Vendor should supply one set of copies of each and every software / OS, which are installed by them in the branches/offices in CDs for every branch / office. Paper licenses are also to be issued to each and every branch/office.

Vendor must deliver the installation, maintenance and troubleshooting manuals, which generally come with respective hardware and peripheral components, network and power components to the office where such equipments are being installed.

Any performance tuning required for any components (hardware, software and / or Network) delivered by the Vendor must be carried out by the Vendor with no additional cost during warranty, ATS.

Vendor should carefully go through above, while arriving at the project cost.

Patent Rights

If a third party claims any infringement of copyright, patent, trademark, industrial design rights, etc. arising from the use of the hardware/ software in India by the Vendor in the performance of its obligations, the Vendor shall act expeditiously to extinguish such claim. If the Vendor fails to extinguish such claim and the Bank pays compensation to such third party as a result of such infringement, the Vendor shall indemnify the Bank for all such payments, including court and lawyer fees and all other expenses in connection with such claim. The Bank will give notice of any such claim to the Vendor immediately and the Vendor shall reimburse such monies expeditiously.

Resolution of Disputes

The Bank and the Vendor shall make every effort to resolve amicably any disagreement or dispute arising from the SLA through direct informal negotiation.

If, after 30 (thirty) days from the commencement of such informal negotiations, the Bank and the Vendor are unable to resolve any dispute amicably, either party may refer the matter to be settled in accordance with the provisions of Telangana Coop Societies Act. The jurisdiction of the settlement of disputes will be Hyderabad only.

Governing Language

The governing language of the Tender process shall be English.

Notices

The following shall be the address of the Bank for serving notice:

To,
Telangana State Cooperative Apex Bank Limited (TSCAB),
4-1-511/3, Street Number 5,
Troop Bazaar, Koti,
Hyderabad, Telangana 500001

The Vendor shall be served with notice, if any, at its registered office address.

A notice shall be effective when delivered before or on the stipulated last date of notice.

Applicable Law

The Contract shall be interpreted in accordance with the laws of the India and the Vendor shall agree to submit to the courts under whose exclusive jurisdiction the Head Office of the Bank falls.

Bank's Right to Accept or Reject any Tender

The Bank reserves the right to accept or reject any or all Tenders received in response to tender without assigning any reasons. It may also cancel the entire process at any time prior to awarding of the contract at its sole discretion and without incurring any liability to the Vendors.

The Bank shall neither be bound to offer any reasons for acceptance or rejection of the Tenders nor entertain any correspondence with the unsuccessful Vendors in this matter.

Disclaimer

As the information stated in this document is not an offer, the Bank will not be bound by any of its terms

BILL OF MATERIALS & SCOPE OF WORK

S.No	Description	Qty
1	Server Hardware	2
2	Network Performance Monitor (up to 500 elements) - License with 1st-year Maintenance	1
3	NetFlow Traffic Analyzer Module for Network Performance Monitor License with 1st-year Maintenance	1
4	Server & Application Monitor (up to 75 nodes with unlimited app monitoring) - License with 1st-Year Maintenance	1
5	Security Information and Event Manager (up to 250 nodes core log sources for servers/firewalls/syslog) - License with 1st Year Maintenance	1
6	Network Configuration Manager (up to 100 nodes) - License with 1st-year Maintenance	1
7	Web Help Desk Per Technician License (6 to 10 named users) - License with 1st-Year Maintenance	10
8	Syslog Server - Country License (50 max) with 12 Months Maintenance	1
9	ARM Access Right Manager for Single Organizational in AD	1
10	Advanced End point Protection for agents, 1-Year Included Premium Support	200
11	Nessus Professional - On Premise - Annual Subscription 1 year	1

12	Installation , Configuration and Implementation Charges	1
13	50 Inches LED screens with controller	12
14	Support charges from 2nd year onwards for all relevant products	

Product Specifications

Performance Monitoring

S.No	Description	Compliant/ Non-compliant	Remarks
1	**Core Monitoring Capabilities**		
1.1	The proposed monitoring solution should be able to monitor: (a) Routers (b) Switches (c) Firewalls (d) Wireless devices (e) Servers (e) Other SNMP-enabled devices		
1.2	Should automatically provide real-time, in-depth network performance statistics after discovery/configuration of devices, including but not limited to, (a) CPU load (b) Memory utilization (c) Interface utilization (d) packet loss		
1.3	Should show statistics like interface bandwidth, current traffic in bps, total bytes received/transmitted etc.		
1.4	Should be able to discover and troubleshoot network paths hop-by-hop for both on premises and cloud environment for specific TCP connections		
1.5	Should display information including alerting for major routing protocols (BGP, OSPF , RIP, EIGRP) with options to view and search routing tables including VRFs, changes in default routes and flapping routes, router topology and neighbor statuses		
1.6	Should help with multicast traffic information monitoring, alerting including topology information, multicast information, route information, multicast errors etc.		
1.7	Should display device status and interface status by different colors to represent warning and critical status		
1.8	Should monitor hardware health for popular vendors like Cisco, DELL, F5, Juniper, HP etc. and should allow alerting and reporting on hardware health monitoring		
1.9	Should show both real-time details and historical details in form of charts with option to choose the time periods		

1.10	Should be able to discover and monitor both IPv4 and IPv6 devices		
1.11	Should have options to poll using SNMP v1, v2c and v3 and WMI		
1.12	Should have options to configure polling intervals as needed		
1.13	Should have options to specify data retention periods		
1.14	Should have the option to determine device availability using SNMP only		
2	**Network Discovery**		
2.1	The proposed monitoring solution should be able to discover devices in the network with SNMP and ICMP capabilities automatically, on input of, (a) IP address ranges (b) subnets (c) individual IP addresses (d) Active Directory		
2.2	Should not add devices with multiple IP addresses as duplicate nodes but should list all known IP addresses for the node		
2.3	Should allow interface filtering on discovery results to exclude virtual interfaces and access ports and select interfaces based on pattern matching		
2.4	Should have option to automate and schedule discovery process		
2.5	Should be able to automatically imports discovered devices		
2.6	Should prompt in web console on discovery of new devices in network		
2.7	Should use discovered information for creating topology maps		
3	**Graphical User Interface and Customization**		
3.1	The proposed management solution Should provide a high-quality graphical user interface with asynchronous view refreshing		
3.2	This web console should be accessible centrally or remotely		
3.3	The web console should allow multiple users to log in at the same time		
3.4	It should have horizontal scaling options available if too many users login at same time		
3.5	It should allow customization by having options to add/remove sections in web pages as necessary		
3.6	It Should provide a unified view of alerts, traps, events, syslog messages in a single page		

3.7	It should give a single unified view of multicast information, route information and device information for a device.		
3.8	It should quickly highlight devices with issues, based on different properties like response time, cpu load, memory usage, high interface usage etc.		
3.9	It should allow creation of custom dashboards and restrict views for users based on devices or interfaces, i.e. it should have role-based access		
3.10	It should log user actions and events in the web console for audit purposes and they should be available for alerting and reporting		
3.11	It should allow interactive charting for node, interface, volume charts etc.		
3.12	It Should provide a dynamic dashboard that allows in-depth visibility and correlates disparate historical data points across different part of the infrastructure. The result should be exportable in tabular format		
3.13	It should allow export of any web page in console to PDF format		
3.14	It should integrate with Active Directory for user login purposes		
3.15	It should be easy to use and intuitive with drill-down features		
4	**Advanced Reporting**		
4.1	The proposed monitoring solution Should provide current and historical out-of-the-box reports for various statistics monitored		
4.2	Should be able to generate / create the report via the web console		
4.3	Should be able to generate statistical reports that can be used as reference for future planning or troubleshooting		
4.4	Should allow customization of reports by adding/removing columns, setting filters, specifying timeframes, grouping columns etc.		
4.5	Should allow advanced customization by providing options to enter custom queries to query the database directly		
4.6	Should have options to save the customized reports permanently and have them accessible in web console		
4.7	Should allow reports to be sent out on schedule as daily, weekly, monthly reports		
4.8	Should allow emailing of dashboards created in web console		

4.9	should be able to configure both charts and tables into a single report.		
4.10	Should have options to import/exports reported created by other users		
4.11	Should support multiple formats such as pdf, HTML and CSV		
5	**Advanced Alerting**		
5.1	The proposed monitoring solution should be able to manage and display events/alerts in the web console		
5.2	The alerts and events information should be logged into the database for future reference		
5.3	The alerting mechanism should allow complex conditions and condition groups to be specified for narrowing down the alert condition		
5.4	It should allow custom queries to be entered to create rules against the database		
5.5	It should allow creation of new alerts from scratch and also customizable threshold limits		
5.6	It should allow creation of alerts based on sustained states		
5.7	Should have various actions that can be taken, including but not limited to, sending out emails, forwarding SNMP traps, running executables, sending SMS text alerts, playing sound, emailing a web page etc.		
5.8	Should have support for variables in alert email message to make the content more self-explanatory		
5.9	Should have the ability to dynamically baseline statistics and automatically set Warning and Critical threshold		
5.10	Should allow alerts suppression during scheduled maintenance		
6	**Grouping**		
6.1	The proposed monitoring solution should allow grouping of devices by various properties -- by department, by location, by name and by other properties gathered		
6.2	Should also allow adding members to groups on-the-fly by specifying a property which can dynamically change values, like volumes reaching low free space		
6.3	Should be able to define dependencies and relationships between connected devices and interfaces to avoid false-positive email alerts in case of outage.		
6.4	Should be able to calculate group availability by averaging the availability of the group members.		

7	**Network Maps**		
7.1	The proposed monitoring solution should be able to represent the network pictorially and display performance details of devices in real time		
7.2	Should allow customization of background, icons etc. and should allow multiple network maps to be nested with drill-down capabilities		
7.3	Should be able to display not just the device status on the map but also status of any other detail obtained through custom MIB polling		
7.4	Should have the capability to display the status of nodes or an aggregated group of nodes over dynamically updated street data.		
7.5	Should be able to automatically connect devices by means of topology information gathered during discovery, like Cisco Discovery Protocol or Link Layer Discovery Protocol		
7.6	Should be able to view multicast topology using upstream and downstream device list information		
7.7	Should be able to display devices location on the geographical level and down to street level		
7.8	Should have the ability to show the link utilisation as a 'weather map'		
8	**Multi-vendor Support**		
8.1	The proposed monitoring solution should not be vendor-specific		
8.2	The discovered devices should be detected as that of a specific vendor and categorized automatically		
9	**Extensibility**		
9.1	The proposed monitoring solution should allow gathering of custom properties from SNMP-enabled devices by specifying the OID of the properties		
9.2	Should be able to fetch properties from devices without need to import device MIBs into MIB database		
9.3	Should be able to get real-time values, charts and also alerts on these custom properties		
9.4	Should have APIs available to programmatically import/export nodes and do similar functionality		
10	**Application Aware Network Performance Monitoring**		

10.1	Should be able to provide Network Response Time (NRT) and Application Response time (ART) for critical applications		
10.2	Should be able to identify and classify ~1200 applications out of the box		
10.3	Should have the ability to display aggregate volume metrics per application / node		
10.4	Should have the ability to create custom HTTP applications		
10.5	Should be able to contextually provide QoE data for nodes in Node Details subview		
11	**Additional Components**		
11.1	Should have utilities to view the database, to stop and start application services		
11.2	Should have options to receive, display and alert on syslog messages and traps from devices		
11.3	Should have wireless reporting option to display wireless thin and autonomous access points and their associated clients		
11.4	Should have customized mobile views of console for administrators' immediate viewing		
11.5	Should be able to monitor Cisco switch stack, with the ability to display invidual member switches, power stack and data stack rings		
11.6	Should be able to report on technologies like Cisco UCS, Energywise feature		
11.7	Should be able to report on virtualized Cisco Nexus 1000V switches, VSAN, Fibre Channel switches like Cisco MDS, Brocade, McData devices		
11.8	Should be able to monitor cloud-based Meraki wireless infrastructure		
11.9	Should be able to monitor entire VMware and Hyper-V virtual infrastructure, including Virtual Centers, Datacenters and ESX clusters, and automatically track VM performance		
11.10	Should be able to monitor individual components in F5 BIG-IP load balancing environment		
11.11	Should be able to monitor individual components in Cisco ASA firewall, including but not limited to: connection count, site to site and remote access VPN tunnels, interface identity and utilization, high availability status and configuration synchronization status.		
11.12	Should be able to monitor Cisco Nexus with VDC awareness, including vPC specific view for configured vPC and peer vPC.		
11.13	Should be able to monitor SDN environment (e.g. Cisco ACI), including but not limited to: APICs, tenants, application profiles, endpoint group and physical entities.		

12	**Integration**		
12.1	Should be able to integrate with modules serving other monitoring purposes and provide a single-pane-of-glass view		
12.2	Should allow integration with third-party applications at user-interface layer, through message exchanges and also through APIs		
12.3	Should be able to integrate with ServiceNow, with the ability to automatically create incidents and synchronize the acknowledgement of incidents bidirectionally		
12.4	It should support SAML 2.0 for integration with Active Directory Federation Services (AD FS) or Okta for Single Sign-On (SSO)		
13	**Enteprise Scalability**		
13.1	The proposed monitoring solution should be able to accommodate growth through addition of load-balancing applications		
13.2	Load-balancing engines should handle interruptions in the connection between the engines and the main application		
13.3	Should allow information from multiple instances of application to be consolidated into a single view		
13.4	Should support multiple deployment options: (a) Centralized deployment (b) Distributed deployment (c) Hybrid deployment With a centralized operations console view, alert acknowledgement and reporting interface		
14	**High Availability**		
14.1	Should have options for ensuring high-availability of application, with/without use of failover products		
15	**Platform Security**		
15.1	Should be fully compatible with TLS 1.2, without any dependency on TLS 1.1 or 1.0		
15.2	Should support Microsoft Device Guard with all binary signed to ensure code integrity		
16	**Deployment**		

16.1	Should be deployable within one hour and should not require consultants for deployment, implementation, configuration or customization		
16.2	Should support agentless deployment		
16.3	Should support deployment on Amazon EC2 and Microsoft Azure (optional)		
16.4	Should support centralized upgrade for all remote components (e.g. remote data collectors, web consoles) without additional management operation on the remote servers		
16.5	Should include actionable dashboard that provide self check functionality for the monitoring platform and display remediation advice for non-compliant item		
17	**Frequency of Updates**		
17.1	New features to be added to product versions frequently, preferably twice every year or more		
17.2	Should notify availability of new versions in the web console		
18	**Product Support**		
18.1	Should provide 24x7 support		
18.2	Active support through forums and community would be a welcome feature		

Bandwidth Monitoring

S.No	Description	Compliant / Non-compliant	Remarks
1	**Core Monitoring Capabilities**		
1.1	The proposed monitoring solution should be able to monitor network traffic by capturing flow data from network devices, including Cisco NetFlow v5 or v9, Juniper J-Flow, IPFIX, sFlow, NetStream data, sampled NetFlow data and Cisco ASA NetFlow		
1.2	Should identify which users, applications, and protocols are consuming the most bandwidth		
1.3	Should highlight the IP addresses of the top bandwidth consumers on the network and find out unwanted bandwidth usage		

1.4	Should be able to associate traffic coming from different sources to application names		
1.5	Should be able to receive flows from non-SNMP-enabled devices, like VMware vSwitch		
1.6	Should monitor Class-Based Quality of Service (CBQoS) with nested policies to find out if traffic prioritization policies are effective and if business-critical applications have network traffic priority		
1.7	Should also support Cisco NBAR2 classification		
1.8	Should monitor Type of Service (ToS), Differentiated Services Codepoint (DSCP), and Per-Hop Behavior (PHB)		
1.9	Should monitor BGP information		
1.10	Should show both recent and historical details in form of charts with option to choose the timeperiods		
1.11	Should have options to specify data retention periods to avoid strain on database and server resources		
1.12	Should provide flow analysis with 1-minute granularity		
2	**Network Discovery**		
2.1	The proposed monitoring solution should be able to automatically add flow sources which are already being monitored for performance		
2.2	Should notify the flows coming in from unmanaged devices and/or unmanaged interfaces and allow to add them for monitoring with minimum effort		
3	**Graphical User Interface and Customization**		
3.1	The proposed management solution Should provide a high-quality graphical user interface		
3.2	It Should provide diverse views categorized by user, application, department, conversation, interface, protocol, type of service, Autonomous System Networks		
3.3	It should allow creation of personalized views of network traffic by providing list of parameters from which we can pick and choose to set filters		
3.4	It should have ability to save customized filtered views as new links in web page for easy access later, with options to search for IP ranges/CIDR etc		

3.5	Should provide a dynamic dashboard that allows in-depth visibility and correlates disparate historical data points across different part of the infrastructure. The result should be exportable as tabular format.		
3.6	This web console should be accessible centrally or remotely		
3.7	The web console should allow multiple users to log in at the same time		
3.8	It should have horizontal scaling options available if too many users login at same time		
3.9	It should allow customization by having options to add/remove sections in web pages as necessary		
3.10	It should allow export of any web page in console to PDF format		
3.11	It should allow creation of custom dashboards and restrict views for users based on devices or interfaces, i.e. it should have role-based access		
3.12	It should integrate with Active Directory for user login purposes		
3.13	It should be easy to use and intuitive with drill-down features		
4	**Advanced Reporting**		
4.1	The proposed monitoring solution Should provide current and historical out-of-the-box reports for various statistics monitored		
4.2	Class-Based Quality of Service reports should give details on Pre-Policy, Post-Policy and Drops		
4.3	Should be able to generate statistical reports that can be used as reference for future planning or troubleshooting		
4.4	Should allow customization of reports by adding/removing columns, setting filters, specifying timeframes, grouping columns etc.		
4.5	Should allow advanced customization by providing options to enter SQL queries to query the database directly		
4.6	Should have options to save the customized reports permanently and have them accessible in web console		
4.7	Should allow reports to be sent out on schedule as daily, weekly, monthly reports		
4.8	Should allow emailing of dashboards created in web console		
5	**Advanced Alerting**		

5.1	The proposed monitoring solution should be able to display events and alerts in the web console		
5.2	Class-based Quality of Service alerts should be fired when the traffic processed exceeds threshold settings for Pre-Policy, Post-Policy and Drops.		
5.3	The alerts and events information should be logged into the database for future reference		
5.4	The alerting mechanism should allow complex conditions and condition groups to be specified for narrowing down the alert condition		
5.5	It should allow SQL queries to be entered to create rules against the database		
5.6	It should allow creation of new alerts from scratch with customizable threshold limits		
5.7	Should have various actions that can be taken, including but not limited to, sending out emails, forwarding SNMP traps, running executables, sending SMS text alerts, playing sound, emailing a web page etc.		
5.8	Should have support for variables in message to make the content more self-explanatory		
6	**Grouping**		
6.1	The proposed monitoring solution should allow to create custom IP address groups to categorize flows by geography, department, device type etc.		
6.2	Should be able to use these groups while creating customized views of network traffic		
7	**Multi-vendor Support**		
7.1	The proposed monitoring solution should not be vendor-specific and should be able to monitor devices from Cisco, Foundry, Juniper Networks, Extreme Networks, HP, Riverbed etc.		
7.2	It should be able to provide a unified summary view taking into account all the monitored devices from different vendors		
8	**Extensibility**		
8.1	The proposed monitoring solution should allow gathering of flow information from devices which are not flow-capable when used with third-party flow exporters		
9	**Additional Features**		
9.1	Should help in locating and isolating infected computers in case of virus outbreak		

9.2	Should help to recognize malicious traffic, including but not limited to: TCP and UDP traffic on port 0, DOS attack		
9.3	Should give importance to the most bandwidth-intensive conversations to improve database performance, reduce page load times and increase reporting speed.		
9.4	Should compress data in database for optimal performance of application		
9.5	Should ensure database maintenance happens in background to prevent overwhelming of database with flow traffic data		
9.6	Should allow NetBIOS and DNS resolution of endpoint domain names		
9.7	Should have utilities to view the database, to stop and start its own services		
10	**Integration**		
10.1	Should be able to integrate with modules serving other monitoring purposes and provide a single-pane-of-glass view		
10.2	Should allow integration with third-party applications at user-interface layer, through message exchanges and also through APIs		
11	**Enteprise Scalability**		
11.1	The proposed monitoring solution should be able to monitor up to 3 million flows per second, and should employs advanced optimization methods		
11.2	Should be able to accommodate network growth through addition of load-balancing applications		
11.3	Should allow information from multiple instances of application to be consolidated into a single view		
11.4	Should support multiple deployment options: (a) Centralized deployment (b) Distributed deployment (c) Hybrid deployment With a centralized operations console view, alert acknowledgement and reporting interface		
12	**High Availability**		
12.1	Should have options for ensuring high-availability of application, with/without use of failover products		

13	**Security**		
13.1	Should be fully compatible with TLS 1.2, without any dependency on TLS 1.1 or 1.0		
13.2	Should support Microsoft Device Guard with all binary signed to ensure code integrity		
14	**Deployment**		
14.1	Should be deployable within one hour and should not require consultants for deployment, implementation, configuration or customization		
14.2	Additional repository database should not be required for storage of Flow data, it should be able to utilize the same database as the monitoring platform		
15	**Frequency of Updates**		
15.1	New features to be added to product versions frequently, preferably twice every year or more		
15.2	Should notify availability of new versions in the web console		
16	**Product Support**		
16.1	Should provide 24x7 support		
16.2	Active support through forums and community would be a welcome feature		

Network Device Configuration Management

S.No	Description	Compliant/ Non-compliant	Remarks
1	**Core Capabilities**		
1.1	The proposed management solution should be able to automatically backup configuration (text based, XML and binary configuration files) for routers, switches, firewall, access points and other network devices		
1.2	Should be able to make bulk configuration changes. For example, change community strings, update ACLs etc. across multiple devices		
1.3	Should send real-time alerts when network configuration changes happen, with the comparison of which configuration lines were added, deleted and modified		

1.4	Should allow comparison of startup and running configuration files to troubleshoot device configuration issues		
1.5	Should allow comparison of current configuration with that of past to understand the changes that have happened over time		
1.6	Should allow comparison of configuration for multiple devices against a common baseline configuration		
1.7	Should help automate repeated tasks by defining series of commands as templates and executing them with or without parameters		
1.8	Should detect configuration policy violations to ensure compliance with federal regulations and corporate standards		
1.9	Should automate change approval process by enabling administrator to review changes submitted by uploaders before they are executed on the devices		
1.10	Should provide inventory of network device hardware and should have out-of-the-box reports for assets and serial numbers		
1.11	Should keep devices current as part of the procurement and maintenance with End of Life and Support tracking		
1.12	Should support multiple protocols including SNMP v1/v2c/v3, Telnet, SSH v1/v2 and TFTP		
1.13	Should allow specification of login information, transfer protocols, transfer ports at global level and also at device level		
2	**Network Discovery**		
2.1	The proposed management solution should be able to discover devices in the network on input of, (a) IP address ranges (b) subnets (c) individual IP addresses		
2.2	Should have option to enable/disable automatic addition of discovered nodes		
3	**Graphical User Interface and Customization**		
3.1	The proposed management solution Should provide a high-quality graphical user interface		
3.2	This web console should be accessible centrally or remotely		
3.3	Should provide End-of-Life/End-of-Support (EoL/EoS) information to help keep devices current with regards to procurement and maintenance of the deployment		

3.4	Should provide a dynamic dashboard that allows in-depth visibility and correlates disparate historical data points across different part of the infrastructure. The result should be exportable with a tabular format.		
3.5	Should allow remote access to job-related features and functions, and show also allow remote access to eite and update device configurations		
3.6	It should allow multiple users to log in at the same time		
3.7	It should have horizontal scaling options available if too many users login at same time		
3.8	It should allow customization by having options to add/remove sections in web pages as necessary		
3.9	It Should provide separate sections for configuration management tasks, inventory and reports on policy violations		
3.10	It should quickly highlight devices which have policy violations, those which have not been backed up for configuration, those with conflicts in configuration etc.		
3.11	It should allow creation of custom dashboards and restrict views for users based on devices or interfaces, i.e. it should have role-based access		
3.12	It should allow export of any web page in console to PDF format		
3.13	It should integrate with Active Directory for user login purposes		
3.14	It should be easy to use and intuitive with drill-down features		
4	**Advanced Reporting**		
4.1	The proposed management solution Should provide out-of-the-box reports for various statistics monitored		
4.2	Should have policy reports designed for regulations specified in HIPAA, SOX, CISCP, Cisco Security Audit etc.		
4.3	Should allow customization of reports by adding/removing columns, setting filters, specifying timeframes, grouping columns etc.		
4.4	Should allow reports to be sent out on schedule as daily, weekly, monthly reports		
4.5	Should allow emailing of dashboards created in web console		
5	**Advanced Alerting**		

5.1	The proposed management solution should be able to display events and alerts in the web console		
5.2	The alerts and events information should be logged into the database for future reference		
5.3	Should be able to backup configuration, execute config script, show last configuration changes as alert actions		
5.4	Should have various actions that can be taken, including but not limited to, sending out emails, forwarding SNMP traps, running executables, sending SMS text alerts, playing sound, emailing a web page etc.		
5.5	Should have support for variables in message to make the content more self-explanatory		
6	**Grouping**		
6.1	The proposed management solution should allow grouping of devices by various properties -- by vendor, machine type, OS image, OS version, last login result and other custom properties		
7	**Multi-vendor Support**		
7.1	The proposed management solution should not be vendor-specific and Should provide built-in configuration management support for network devices from Cisco Systems, Nortel Networks, Extreme Networks, Dell, HP, Adtran, Riverbed, 3Com, Aruba Networks, Juniper Networks, Foundry Networks etc.		
7.2	The discovered devices should be detected as that of a specific vendor and categorized automatically		
8	**Extensibility**		
8.1	The proposed management solution should allow creation of device command templates for devices not supported out-of-the-box		
8.2	Should allow creation of custom device templates to automate repeated configuration tasks		
8.3	Should be able to create custom policy reports by specifying what content should/should not be present in configuration. The content could be specified either as a string or as a regular expression		
9	**Additional Components**		
9.1	Should have utilities to create device templates for devices which are not supported out-of-the-box		

9.2	Should have options to receive, display and alert on syslog messages and traps from devices		
9.3	Should be able use external authentication server like RADIUS/TACACS		
9.4	Should provide firmware vulnerability information for Cisco and Juniper devices. Information should be provided by trusted sources (e.g. NIST)		
9.5	Should be able to perform Cisco IOS, ASA and Nexus firmware upgrade for multiple devices at a time		
9.6	Should be able to discover all security contexts on Cisco ASA and individually handles configuration backup and restore		
9.7	Should be able to visualize ACLs configured on Cisco ASA, with the ability to detect and notify on changes on ACLs, display rules hit count, identify shadow and redundant rules		
9.8	Should be able to discover VDC on Cisco Nexus and individually handles configuration backup and restore		
9.9	Should be able to visualize ACLs configured on Cisco Nexus, with the ability to detect and notify on changes on ACLs, display rules hit count, identify shadow and redundant rules, display configs for vPC and its member interfaces		
10	**Integration**		
10.1	Should be able to integrate with modules serving other monitoring purposes and provide a single-pane-of-glass view		
11	**Enteprise Scalability**		
11.1	The proposed management solution should be able to manage even 10,000 devices and accommodate network growth through addition of load-balancing applications		
11.2	Should support multiple deployment options: (a) Centralized deployment (b) Distributed deployment (c) Hybrid deployment With a centralized operations console view, alert acknowledgement and reporting interface		
12	**High Availability**		
12.1	Should have options for ensuring high-availability of application, with/without use of failover products		

13	**Deployment**		
13.1	Should be deployable within one hour and should not require consultants for deployment, implementation, configuration or customization		
14	**Frequency of Updates**		
14.1	New features to be added to product versions frequently, at least twice every year		
15	**Product Support**		
15.1	Should provide 24x7 support		
15.2	Active support through forums and community would be a welcome feature		

Application Monitoring

S.No	Description	Compliant/ Non-compliant	Remarks
1	**Core Monitoring Capabilities**		
1.1	The proposed monitoring solution should be able to monitor: (a) Application status (b) Appilcation performance statistics (c) Services and processes (d) OS performance (e) Hardware		
1.2	Should automatically provide real-time view of processes running in systems and in-depth application performance statistics after discovery/configuration of applications		
1.3	Should be able to manage the processes, services running in systems and in-depth application performance statistics after discovery/configuration of applications		
1.4	Should automatically provide real-time view of windows event logs including the level of the event logs, Event ID, and source.		
1.5	Should have expert monitoring methods that point out the status and performance of key parameters (like services, queue length in case of Exchange, sql queries in case of databases etc.) of applications based on best practices		

1.6	Should be able to put together important parameters of an application, into one single monitoring template that can be uniformly applied to applications on different servers		
1.7	A customization made in one application's monitoring template should be propagated immediately to all other servers having that application		
1.8	Should allow use of custom scripts with various scripting engine options like VBscript, Perl, Powershell etc.		
1.9	Should have options for user experience monitoring for various applications and services like HTTP, FTP, DHCP, DNS, SQL Server, Oracle, JSON, etc. to find out issues even before users notice them		
1.10	Should be able to report on hardware details (like CPU, memory, fan state, power etc.) of servers from popular vendors like IBM, HP, DELL and also VMware Hosts		
1.11	Should have options to poll using SNMP, WMI and other methods		
1.12	Should display application status and status of important services by different colors to represent warning and critical status		
1.13	Should show both realtime details and historical details in form of charts with option to choose the timeperiods		
1.14	Should have options to configure polling intervals as needed		
1.15	Should be able to get Disk I/O Performance Metrics for Processes & Services Monitored via WMI		
1.16	Should have options to specify data retention periods		
1.17	Should be able to provide User Audit Event Logging including Terminated Processes, Stopped/Started/Restarted Services, Nodes Rebooted Newly Created/Edited/Deleted Credentials & Application Templates Assigned, Removed, Managed, and Unmanaged Applications		
2	**Cloud Monitoring Capability**		
2.1	Discover and monitor EC2 cloud instances and EBS volumes in AWS via API		
2.2	Discover and monitor Azure cloud service via API		
2.3	Automatically discover and monitor new instances		

2.4	Consolidate view for cloud, hybrid, and on-premises systems		
2.5	Monitor application performance and OS metrics on cloud instances		
2.6	Should be able to monitor Docker, Docker Swarm, Kubernetes, and Apache Mesos container deployments, with the ability to automatically discover containers running on the orchestrator.		
3	**Application Discovery / Monitoring**		
3.1	The proposed monitoring solution should be able to discover applications in the chosen servers, apply monitoring for them and start report statistics in few minutes		
3.2	Should have option to find processes either through WMI or SNMP, Performance Counter Monitors, WMI Monitors, VMware Performance Counter Monitors etc.		
3.3	Should be able to discover application dependencies and connections between application servers, with the ability to monitor both incoming and outgoing connection information on a per process level.		
3.4	Should have option to discover JMX monitors for monitoring Java-based applications like JBoss, Tomcat, WebLogic etc.		
3.5	Should be able to discover email and directory servers, databases, network services, operating systems, VMware ESX servers etc. automatically by means of inbuilt monitoring templates		
3.6	Should be able to create and set automatic Calculation of Warning & Critical Thresholds From Baseline Data		
3.7	Should provide indepth monitoring of Microsoft SQL out of the box with the following SQL Error Logs, Individual Database Details Views, Status of SQL Agent, Job Results, Index Fragmentation, SQL Server Connections		
3.8	Should provide indepth monitoring of Microsoft Exchange mailbox role servers including performance of Information store, database, storage, replication, etc. It should also trend the sent and received emails and attachments for every mailbox user.		
3.9	Should provide indepth monitoring of Microsoft Internet Information Service (IIS) including services, processes, individual website connections and response time, individual application pool, other statistic like cache and connection.		

3.10	Should provide indepth monitoriing of Microsoft Office 365 products including Exchange Mailboxes, mail Traffic, security, subscription status and mobile device statistics.		
4	**Graphical User Interface and Customization**		
4.1	The proposed management solution Should provide a high-quality graphical user interface		
4.2	This web console should be accessible centrally or remotely		
4.3	The web console should allow multiple users to log in at the same time		
4.4	It should have horizontal scaling options available if too many users login at same time		
4.5	It should allow customization by having options to add/remove sections in web pages as necessary		
4.6	It Should provide a unified view of alerts, traps, events etc. in a single page		
4.7	It should quickly highlight applications with issues, based on different properties like down applications, applications with problems, parameters with high CPU, memory usage etc.		
4.8	It should allow creation of custom dashboards and restrict views for users based on applications, i.e. it should have role-based access		
4.9	It should allow interactive charting		
4.10	It should allow export of any web page in console to PDF format		
4.11	It should integrate with Active Directory for user login purposes		
4.12	It should be easy to use and intuitive with drill-down features		
4.13	It should have integration options to automatically visualize relevant virtual infrastructure objects such as datastores and storage objects such as LUNs		
4.14	Should provide a dynamic dashboard that allows in-depth visibility and correlates disparate historical data points across different part of the infrastructure. The result should be exportable with a tabular format.		
5	**Advanced Reporting**		

5.1	The proposed monitoring solution Should provide current and historical out-of-the-box reports for various statistics monitored		
5.2	Should be able to generate / create the report via the web console		
5.3	Should be able to generate statistical reports that can be used as reference for future planning or troubleshooting		
5.4	Should allow customization of reports by adding/removing columns, setting filters, specifying timeframes, grouping columns etc.		
5.5	Should allow advanced customization by providing options to enter custom queries to query the database directly		
5.6	Should have options to save the customized reports permanently and have them accessible in web console		
5.7	Should allow reports to be sent out on schedule as daily, weekly, monthly reports		
5.8	Should allow emailing of dashboards created in web console		
5.9	should be able to configure both charts and tables into a single report.		
5.10	Should have options to import/exports reported created by other users		
5.11	Should support multiple formats such as pdf, HTML and CSV		
6	**Advanced Alerting**		
6.1	The proposed monitoring solution should be able to manage and display events/alerts in the web console		
6.2	The alerts and events information should be logged into the database for future reference		
6.3	The alerting mechanism should allow complex conditions and condition groups to be specified for narrowing down the alert condition		
6.4	It should allow custom queries to be entered to create rules against the database		
6.5	It should allow creation of new alerts from scratch and also customizable threshold limits		
6.6	It should allow creation of alerts based on sustained states		

6.7	Should have various actions that can be taken, including but not limited to, sending out emails, forwarding SNMP traps, running executables, sending SMS text alerts, playing sound, emailing a web page etc.		
6.8	Should have support for variables in alert email message to make the content more self-explanatory		
7	**Grouping**		
7.1	The proposed monitoring solution should allow grouping of applications by various properties -- by department, by location, by name and by other properties gathered		
7.2	Should also allow adding members to groups on-the-fly by specifying a property which can dynamically change values, like volumes reaching low free space		
7.3	Should be able to define relationships between servers and applications to avoid false-positive email alerts in case of outage.		
8	**Topology Maps**		
8.1	The proposed monitoring solution should be able to represent the applications pictorially and display performance details of applications in real time		
8.2	Should allow customization of background, icons etc. and should allow multiple maps to be nested with drill-down capabilities		
9	**Multi-vendor Support**		
9.1	The proposed monitoring solution should not be application-specific		
9.2	The discovered applications should be monitored with inbuilt monitoring templates created based on best practices		
10	**Extensibility**		
10.1	The proposed monitoring solution should allow custom scripts to be included to extend application monitoring capabilities		
10.2	Should be able to get realtime values, charts and also alerts on these custom properties		
10.3	Should have APIs available to programmatically import/export nodes and do similar functionality		

11	**Additional Components**		
11.1	Should have utilities to view the database, to stop and start application services		
11.2	Should have customized mobile views of console for administrators' immediate viewing		
12	**Integration**		
12.1	Should be able to integrate with modules serving other monitoring purposes and provide a single-pane-of-glass view		
12.2	Should integrate with virtualization monitoring software to provide end-to-end application performance view from the application to the VM to the host.		
12.3	Should allow integration with third-party applications at user-interface layer, through message exchanges and also through APIs		
12.4	Should be able to integrate with ServiceNow, with the ability to automatically create incidents and synchronize the acknowledgement of incidents bidirectionally		
12.5	It should support SAML 2.0 for integration with Active Directory Federation Services (AD FS) or Okta for Single Sign-On (SSO)		
13	**Enteprise Scalability**		
13.1	The proposed monitoring solution should be able to accommodate growth through addition of load-balancing applications		
13.2	Load-balancing engines should handle interruptions in the connection between the engines and the main application		
13.3	Should allow information from multiple instances of application to be consolidated into a single view		
13.4	Should support multiple deployment options: (a) Centralized deployment (b) Distributed deployment (c) Hybrid deployment With a centralized operations console view, alert acknowledgement and reporting interface		
14	**High Availability**		

14.1	Should have options for ensuring high-availability of application, with/without use of failover products		
15	**Platform Security**		
15.1	Should be fully compatible with TLS 1.2, without any dependency on TLS 1.1 or 1.0		
15.2	Should support Microsoft Device Guard with all binary signed to ensure code integrity		
16	**Deployment**		
16.1	Should be deployable within one hour and should not require consultants for deployment, implementation, configuration or customization		
16.2	Should support agentless deployment		
16.3	Should include optional agent for Windows, Linux (x86), Linux (ARM) and AIX		
17	**Frequency of Updates**		
17.1	New features to be added to product versions frequently, preferably twice every year or more		
17.2	Should notify availability of new versions in the web console		
18	**Product Support**		
18.1	Should provide 24x7 support		
18.2	Active support through forums and community would be a welcome feature		

Security Information & Event Management

S.No	Description	Compliant/ Non-compliant	Remarks
1	**Core Capabilities**		

1.1	The proposed monitoring solution should be able to immediately spot abnormalities in the network by looking into data from millions of files and events		
1.2	Should perform proactive log analysis and real-time event correlation across the infrastructure to quickly identify attacks, highlight threads and detect policy violations		
1.3	Should be able to correlate millions of events from network, systems, applications, virtual machines and storage infrastructure using real-time, in-memory, non-linear and multi-dimensional correlation facilities		
1.4	Should store terabytes of log data without need to purchase additional storage using high performance, high compression data model which should data at at least 60:1 ratio		
1.5	Should monitor both devices and systems. For example, monitor Windows Domain Controllers for brute force hacking attempts, monitor firewalls for port scans and malformed packets, monitor antivirus software for not-cleaned viruses, monitor proxy servers for suspicious URL access, monitor SQL databases for changes to tables and schema etc.		
1.6	Should ensure reliable and secure delivery of log messages, ensuring chain of custody, along with buffering and encryption of messages from endpoint to appliance		
1.7	Should help create incidents report by monitoring security audits		
2	**Compliance**		
2.1	The proposed monitoring solution should be able to ensure compliance with PCI, HIPAA, NCUA, GLBA, NERC-CIP, FISMA, SOX or custom corporate policies		
3	**Alerts and Active Responses**		
3.1	The proposed monitoring solution should be able to mitigate threats with active responses to devices and systems		
3.2	It should have many inbuilt rules for immediate use and for customization		

3.3	It should automatically and interactively take action to protect infrastructure by quarantining, blocking, routing, and controlling services, processes, acccounts and privileges		
4	**Graphical User Interface**		
4.1	The proposed management solution Should provide a high-quality graphical user interface accessible through standard browsers		
4.2	It should have real-time console for live event monitoring		
4.3	It should help visualize search data and understand how to take action on it with intuitive search interface, using options like Word Cloud, treemaps, bubble charts, histograms etc.		
4.4	It should have drag-and-drop options to create filters, rules and searches		
4.5	It should make searching for rules simpler, preferably by tags or categories instead of folders		
4.6	It should have option to show both original and normalized log information in the same search interface		
4.7	It should have Top 10 views to highlight common issues		
4.8	This web console should be accessible centrally or remotely		
4.9	The web console should allow multiple users to log in at the same time		
4.10	It should quickly highlight abnormalities in the network		
4.11	It should be easy to use and intuitive with drill-down features		
5	**Reporting**		
5.1	The proposed monitoring solution should be able to generate compliance reports quickly		
5.2	Should have many inbuilt reports (around 300 or more) and out-of-the-box compliance packs that would help with audit purposes		
5.3	Should allow customization of reports by adding/removing columns, setting filters, specifying timeframes etc.		

5.4	Should have reports that show database usage information too		
6	**Multi-vendor Support**		
6.1	The proposed monitoring solution should not be vendor-specific		
6.2	Should be able to monitor dozens of manufacturers, hundreds of products and thousands of models		
7	**Deployment**		
7.1	Should enable quick deployment, like a virtual appliance, on popular hypervisors like VMware or Hyper-V, and should not be hardware-based		
7.2	Should support deployment on Microsoft Azure (optional)		
8	**Additional Components**		
8.1	The proposed monitoring solution should protect sensitive data with real-time detection and ejection of USB drives		
8.2	Database archival should allow archival of newly-created data alone		
9	**Integration**		
9.1	The proposed monitoring solution should share and correlate log and event data from network monitoring solutions, application monitoring solutions and virtualization monitoring solutions through data sharing integration		
9.2	It should be able to accept traps from network monitoring, application monitoring and other monitoring solutions		
9.3	It should support the use of Lightweight Directory Access Protocol (LDAP) Kerberos based authentication credentials to access Microsoft Active Directory for Single Sign-On (SSO)		
9.4	It should allow export of syslog messages to a dedicated syslog server in their original (raw) format		
10	**Enteprise Scalability**		

10.1	The proposed monitoring solution Should provide with the capacity for long-term storage and retrieval of original log messages.		
11	**Frequency of Updates**		
11.1	New features to be added to product versions frequently		
12	**Product Support**		
12.1	Should provide 24x7 support		
12.2	Active support through forums and community would be a welcome feature		

Access Rights Management

S.No	Description	Compliant/ Non-compliant	Remarks
1	**Core Capabilities**		
1.1	The proposed monitoring solution should be able to automate access rights management, analysis and identify insecure accounts while providing audit trails for users who have access to critical and sensitive data		
1.2	It should monitor, analyse and audit access rights to Active Directory (AD) and AD Group Policy		
1.3	It should monitor, analyse and audit access rights to Microsoft Exchange on-prem/Exchange Online		
1.4	It should monitor, analyse and audit access rights to Microsoft SharePoint on-prem/SharePoint Online		
1.5	It should monitor, analyse and audit access rights to Windows file share		
1.6	It should track all resource access activities and display in an easy-to-comprehend UI in real-time for AD, file share, and Exchange		
1.7	It should track all changes made outside the access rights management tool used, e.g. Windows native tools		

2	**Permission Analysis**		
2.1	The proposed monitoring solution should provide visual graphical representation of AD user and group permissions relationship including nested groups		
2.2	It should interactively display the relationships between resources, its structure, user accounts/groups, and permissions		
2.3	It should support multiple AD domains		
2.4	It should provide insights into top risk factors with the highest security impact: Non-compliant user accounts		
2.5	It should provide insights into top risk factors with the highest security impact: Accounts with password that never expire		
2.6	It should provide insights into top risk factors with the highest security impact: Directories with deviating access rights		
2.7	It should provide insights into top risk factors with the highest security impact: Unresolved SIDs in directories		
2.8	It should provide insights into top risk factors with the highest security impact: Globally accessible directories		
2.9	It should provide insights into top risk factors with the highest security impact: Inactive accounts		
2.10	It should provide recommendation and steps to resolve identified security risks		
3	**Permission Management**		
3.1	The proposed monitoring solution should be easy to manage user permissions with automated and role-specific templatised user account provisioning and deprovisioning		
3.2	It should provide scheduled user provisioning e.g. grant access rights for a certain time period and revoke given rights automatically on the desired date		
3.3	It should provide simple easy to use self-service web portal to employees to order their access rights that goes to the designated data owner		
3.4	It should provide delegation of access rights management to the data owners via a simple easy to use self-service web portal to approve resource access rights request		

3.5	It should provide periodic review of access rights of all employees that can be used to maintain correct access rights to the resources		
3.6	It should provide a web-based management portal to delegate standard account management operations to the help desk such as password reset.		
3.7	It should provide mandated commenting feature for every changes made manually for documenting purposes		
4	**Compliance**		
4.1	The proposed monitoring solution should be able to help demonstrate an organisation's PCI DSS compliance		
5	**Alerts and Active Responses**		
5.1	The proposed monitoring solution should be able to display alerts on both authorised and un-authorised access or changes to resources such as AD, Exchange and Windows file shares in real-time		
5.2	It should detect credential misuse and other unauthorized/suspicious activity		
5.3	It should detect and alert on potential credential risks, e.g. accounts with insecure configurations		
5.4	It should support actions such sending email, writing into Windows Event Log, and executing scripts when the alert is generated		
6	**Graphical User Interface**		
6.1	The proposed management solution Should provide a high-quality graphical user interface		
6.2	This console should be accessible centrally or remotely		
6.3	The web console should allow multiple users to log in at the same time		
6.4	It should integrate with Active Directory for user login purposes		
6.5	Provide comprehensive view of all AD, file servers, Exchange, SharePoint resource from single UI		
7	**Reporting**		
7.1	The proposed monitoring solution should be able to generate comprehensive user access reports for regulatory compliance and audits		

7.2	It should support reports in various formats such as PDF, CSV, XLSX		
7.3	It should support custom management and audit reports		
7.4	It should support automated schedule report generation		
8	**Deployment**		
8.1	Should enable quick deployment, like a virtual appliance, on popular hypervisors like VMware or Hyper-V, and should not be hardware-based		
9	**Integration**		
9.1	The proposed monitoring solution should be able to integrate with 3rd party applications such as ServiceNow or Matrix42		
10	**Enterprise Scalability**		
10.1	The proposed monitoring solution should be able to scale from small (<100 users) to large (40K+ users) environment		
11	**Frequency of Updates**		
11.1	New features to be added to product versions frequently		
12	**Product Support**		
12.1	Should provide 24x7 support		
12.2	Active support through forums and community would be a welcome feature		

Help Desk

S.No	Description	Compliant/ Non-compliant	Remarks
1	**Core Helpdesk Capabilities**		
1.1	The proposed helpdesk solution Should provide easy to use ticketing system that automates the creating, tracking and closing of tickets as well as tracking data over time		

1.2	Should have a highly configurable workflow engine to ensure change management policies and procedures are adhered to		
1.3	Should provide hardware and software asset management for licensing, warranties, maintenance and more		
1.4	Should have flexible and schedulable reporting		
1.5	Should be able to automate links to related knowledgebase articles or self help tools for specific issues or requests		
1.6	Should have options for actions to be performed before and after package deployment to ensure that complicated patches get deployed without scripting		
1.7	Should have Dashboard view of data, with drill down capabilities		
1.8	Should have Web based console providing easy access to the application and critical data from any internet ready location		
1.9	Should have interface to manage approval requests		
2	**Graphical User Interface**		
2.1	Should have a web user interface that provides ease of configuration through simple to understand, point-and-click configuration.		
2.2	Should provide dynamic, real-time access to your service desk through the convenience of virtually any webkit enabled mobile device such as Microsoft® Windows Mobile®, RIM® Blackberry®, and Apple® iPhone® devices		
3	**Service Request fulfillment**		
3.1	Should have an agentless architecture to avoid additional agent software on each machine		
3.2	Should be aligned with the ITIL v3 methodologies in the processes of Incident, Problem, Knowledge, and Configuration Management.		
3.3	Should allow the service desk to easily configure multiple tiers & groups of IT staff.		
3.4	Should be able to dynamically route and assign help desk tickets to a specific technician or group of technicians		
3.5	Should be able to create customized form elements with ease		

3.6	Should be able to create ticket checklists and checklist templates		
3.7	Should have a quick and easy audit trail for each completed service request.		
3.8	Should be able to optimize staff assignment of incoming requests via round robin distribution, or in a triage approach		
3.9	Should be able to automatically convert a service request email into a trouble ticket		
	Should provide flexible, dynamic business rules allow for virtually unlimited routing and ticket update automation capabilities for inbound and existing tickets		
4	**Integration**		
4.1	Should have asset database integration with networking monitoring or configuration management or server monitoring solutions		
4.2	Should have native integration to receive alerts directly from other monitoring solutions and record them as tickets		
5	**Ease of Deployment**		
5.1	Should be simple to deploy without outside assistance and consultants.		
5.2	Should have a wizard that will guide through the deployment process.		
5.3	Should create sample request type out-of-the-box for the ease of use by user		
6	**Account Management**		
6.1	Should be able to integrate with eixsting standard LDAP and Microsoft's Active Directory		
6.2	Should have a that contains built-in logic to weigh technician availability vis-a-vis ticket assignment		
6.3	Should provide a self-registration option for clients to complete and engage in customer support.		
6.4	Should provide options to configure individual technicians or groups with similar permissions to restrict options for efficiency or security reasons		
6.5	Should be able to create logical groups for ticket routing, visibility & escalations		
7	**Scalability**		

7.1	Should be able support a large number of client users		
8	**Discovery and Inventory assests**		
8.1	Should provide automated asset discovery based on subnet or IP range using WMI		
8.2	Should be able to associating an end user with a specific asset or group of assets		
8.3	Should have scheduling feature to automatically add or remove assets at predefined intervals		
9	**Dashboard and Reporting**		
9.1	Dashboard should show at-a-glance charting provides an instant overview of the help desk's service fulfillment.		
9.2	Should provide robust graphic reporting tools that can easily monitor technician performance, customer support needs by location, real-time billing data, and incidence frequency.		
9.3	Reports should be fully customizable to allow addition of fields as needed		
9.4	Should be able to create new reports from scratch within few minutes		
9.5	Ability to execute reports immediately or on a schedule		
9.6	Ability to configure report export formats and send email reports		
10	**Notifications**		
10.1	Ability to configure and set automatic email notifications		
10.2	Should be able to configure Apple Push Notification (APN) to Apple iOS devices		
11	**Service Level Agreement Management**		
11.1	Should provide Rules allow your team to create automated escalations based on virtually any service ticket related field and SLA due date		
11.2	Should be able to configure tiered date-specific reminder notifications via email and visual queuing.		
11.3	Should have a different reminder intervals may be configured based on the service ticket's SLA priority.		

11.4	Should provide key performance indicators and custom reports allow you to pinpoint bottlenecks, promoting efficiency and automation.		
12	**Licensing**		
12.1	Licensing should be simple, preferably licensed based on number of helpdesk users and the quantity of client end user accounts is always unlimited.		
13	**Cost of Maintenance**		
13.1	Maintenance and administration of the product should consume only about 10% of one person's time and should not require one full-time person to manage		
14	**Frequency of Updates**		
14.1	New features to be added to product versions frequently, preferably twice every year or more		
15	**Product Support**		
15.1	Should provide 24x7 support		
15.2	Active support through forums and community would be a welcome feature		

Advanced Endpoint Protection

1 Introduction

1.1 The proposed Advanced Endpoint Solution shall be able to:

1.1.1 Prevent all exploits, including those utilizing unknown Zero-Day vulnerabilities;

1.1.2 Prevent all malicious executable, without requiring any prior knowledge;

1.1.3 Provide detailed forensics against prevented attacks on the endpoint;

1.1.4 Be effective in preventing Exploits and Malwares without connectivity or updates from Management Server(s) and/or cloud-based resources.

2 Scope of Work

2.1 The Tenderer shall propose the following for implementation in ORGANIZATION environment:

2.1.1 Advanced Endpoint Protection (xxxxx Workstations, xxxx Servers)

2.2 Refer to subsequent paragraphs for detailed requirements.

3 Advanced Endpoint Protection Functional Requirements

3.1 Endpoint

3.1.1 The Tenderer shall propose solution supporting at least XXXX THOUSAND (XXXXX) Advance Endpoint Solution for endpoints and XXX THOUSAND (XXXX) Advance Endpoint Solution for Servers.

3.1.2 The proposed solution shall co-exist with the existing endpoint security solution (i.e. Anti-Virus, Host-based Intrusion Prevention Systems, Software Delivery, etc.) in the ORGANIZATION environment in terms of threat and malware prevention.

3.1.3 The proposed solution shall support following end-points

i. Windows XP, Windows Vista, Windows 7,Windows Embedded, Windows 8, Windows 10, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Mac OSX,
ii. Virtual environments - VMware ESXi, Citrix XenServer, Oracle Virtualbox, Microsoft Hyper-V
iii. Virtual Desktop infrastructure - VMware Horizon View, Citrix XenDesktop, Microsoft Virtual PC
iv. Linux Enterprise Environment – Oracle, Cent OS, Ubuntu, SUSE, RedHat, Debian, Amazon Linux

3.1.4 The proposed solution shall support anti-exploit and anti-malware prevention capabilities across both the Windows, Mac and Linux Operating Systems.

3.1.5 The proposed solution shall be recognized as a security solution (AntiVirus/AntiMalware) by Windows Security Center.

3.2 Management

3.2.1 The proposed solution shall be managed from Web-based Graphical User Interface (GUI).

3.2.2 The proposed the solution is able to export its logs out in syslog format to any log management solution.

3.2.3 The proposed solution shall provide one common management platform for both the Windows, Mac and Linux agents.

3.2.4 The proposed solution shall provide the ability for all agents to draw from a common license pool.

3.2.5 The proposed solution's management server shall be able to support at least 30,000 agents per management server and 1,50,000 per Database.

3.3 Exploit Prevention

3.3.1 The proposed solution shall support process protection and applications with the capability to add in other third party and proprietary/customized applications to that list.

3.3.2 The proposed solution shall provide a function to specifically perform monitoring or learning of the ORGANIZATION environment (i.e. processes and applications installed and running on the end-points). This is for initial deployment and the pilot phase (with test users).

3.3.3 The proposed solution shall be able to provide real-time prevention against exploits of any application vulnerabilities by blocking exploit techniques not limited to Software Logic Flaws, Memory Corruption, e.g. DLL Hijacking etc w/o dependency for Vendor patches.

3.3.4 The proposed solution shall be capable of preventing pre-exploitation snooping attacks on the endpoint.

3.3.5 The proposed solution shall also be able to prevent post-exploitation attacks on the endpoint i.e. privilege escalation, Keylogging etc.

3.3.6 The proposed solution shall be able to prevent zero-day or undiscovered exploits of any application vulnerabilities by blocking exploits techniques.

3.3.7 The proposed solution should provide the capability to perform exploit monitoring and prevention based on a number of exploit techniques without requiring a connection to the Management Server and/or Cloud Service and without relying on signatures.

3.3.8 Once the proposed solution prevents or blocks an exploit technique, it shall freeze the process, collect forensic information (not limited to process name, file source and path, time stamp, memory dump, OS version, User ID, vulnerable application version, etc.) and terminate only this particular process.

3.3.9 The proposed solution shall utilize exploit technique modules to prevent or block. It shall not be based on signatures, reputation and heuristics of file. The exploit technique modules can be applied to known and popular applications as well as authorized unknown or in-house developed applications.

3.3.10 The proposed solution shall not use end-point resource intensively

3.3.11 The proposed solution shall update the exploit technique modules not more than once in SIX (6) months, as to minimize administrative and operational overheads when downloading the updates.

3.3.12 The proposed solution shall be able to simultaneously protect all applications and processes against exploit techniques.

3.3.13 The proposed solution shall be able to create exclusion rules to exclude specific endpoints for specific processes from the security threat event log from the proposed solution management console.

3.3.14 The proposed solution should allow whitelisting of process and legitimate application.

3.3.15 The proposed solution should verify command Parameter in Macros and Scripts.

3.3.16 The Proposed solution should have behavior knowledge of spawning malicious child process.

3.4 Malware Prevention

3.4.1 The proposed solution shall support protection against the execution of malicious executables.

3.4.2 The supported malware shall include but not be limited to:

i. Windows Executables
ii. Macro-enabled Office documents
iii. Mach-O
iv. DLL
v. ELF

3.4.3 The proposed solution shall provide a function to specifically perform monitoring or learning of the ORGANIZATION environment (i.e. processes and applications installed and executing on the end-points). This is for initial deployment and the pilot phase (with test users).

3.4.4 The proposed solution shall provide the capability to control what is allowed to be executed on the ORGANIZATION endpoints (such as be not limited to, folder location, network location, removable media)

3.4.5 The proposed solution shall provide the capability to do control and restrict the parameters on how executables can run (not limited to file location of execution, external media, network location, spawning of multiple child processes etc.).

3.4.6 The proposed solution shall be able to prevent the execution of malware by using malware modules to target common process behaviors triggered by malware.

3.4.7 The proposed solution shall not use end-point resource intensively (i.e. not more than 1% CPU and not more than 50MB memory)

3.4.8 The proposed solution shall not rely on hardware specific exploit analysis technique such as local software virtualized sand-box or virtualized container.

3.4.9 The proposed solution shall provide the capability to configure global whitelists to allow certain executable files to be run within a certain scenario within the ORGANIZATION.

3.4.10 The proposed solution shall provide the ability to enforce whitelist/blacklist controls of a parent-child process creation tree. The whitelist or blacklist shall be configurable.

3.4.11 The proposed solution shall be able to create exclusion rules to exclude certain endpoints from the protection capability from the security threat event log.

3.4.12 The proposed solution shall provide ransomware prevention capability by being able to detect and prevent ransomware behavior or activity on the endpoint i.e. Unauthorized encryption of data files

3.4.13 The ransomware prevention capability shall not have to rely on any file backup and restoration feature.

3.4.14 The proposed solution shall have the ability to prevent file-less malware by employing techniques such as preventing unauthorized use of scripting engines and child processes.

3.4.15 The Proposed solution should have Behavior based Ransomware prevention no dependency on Signature or update.

3.4.16 The Proposed solution should have validation on all process running in Kernel and validating their existence.

3.4.17 The Proposed solution should have a “0” Trust Architecture and prevent any unknown execution on the system.

3.5 Unknown Malware Analysis

3.5.1 The proposed solution shall have the capability to query the Threat Intelligence solution for hash values to verify whether it is malicious or benign.

3.5.2 The proposed solution shall have the capability to submit potential malicious files to the Threat Intelligence solution through the endpoint management server not more than 100 MB.

3.5.3 The proposed solution shall have the capability to view the malware analysis report natively from the endpoint management server.

3.5.4 The proposed solution shall not analyze files that have already been submitted previously. It will indicate that the file is identical and has been submitted earlier.

3.5.5 The proposed solution is able to provide prevention for unknown Malware by using APT sandbox technology with Dynamic, Static and Bare Metal Analysis. Furthermore, it is able to provide verdict with full analysis report after submission.

3.5.6 The proposed solution should provide the capability to manually change or override a decision taken by the Threat Intelligence for a particular verdict.

3.5.7 The proposed solution should provide the capability to prevent execution of a file when its statistic\attributes is unknown from the vendor Cloud Services or no connection.

3.5.8 The proposed solution should provide the capability to prevent execution of a file when the endpoint cannot query the Cloud Services for and the statistic\attributes is locally unknown.

3.5.9 The proposed solution shall minimally support analysis of the following file types

i. Windows Executables
ii. Macro-enabled Office documents
iii. Mach-O
iv. DLL

3.5.10 The proposed solution should provide the capability to perform static analysis (machine learning) in offline mode.

3.5.11 proposed solution shall provide the capability to perform analysis locally on the endpoint and provide an immediate verdict.

3.5.12 The Local Analysis capability shall be available for both Windows and Mac.

3.5.13 The proposed solution should provide cohesive protection w/o constant connection to internet and take local decision on suspicious activity.

3.5.14 The proposed solution should have technique based Ransomware prevention without any update.

3.5.15 The proposed solution should have mechanism to detect unknown threats using behavioral analysis

3.6 Reporting

3.6.1 The proposed solution shall have the following natively built dashboards to monitor the security posture and status of the ORGANIZATION:

a. Endpoint Security Manager Dashboard
b. Security Event Dashboard
c. Threat Details Dashboard
d. Provisional Mode Details Dashboard
e. Security Error Log Details Dashboard

3.6.2 The proposed solution shall have the following natively built dashboards to monitor the health of the individual endpoints in the ORGANIZATION:

a. Endpoint Health Details Dashboard
b. Endpoint Status Details Dashboard
c. Endpoint Rule History Dashboard
d. Endpoint Security Policy Change Dashboard
e. Endpoint Service Status History Dashboard

3.6.3 The proposed solution is able to provide a Web-based view of the threats and malware and also provide exporting of the data logs for threats or endpoint health in CSV format.

3.7 Forensics

3.7.1 The proposed solution shall support the collection of forensic data captured by the advanced endpoint solution to a centralized location.

3.7.2 The proposed solution shall support the collection of the following forensic information for further investigation purposes:

i. Memory Dump
ii. Accessed Files
iii. Loaded Modules
iv. Accessed URI

v. Ancestor Processes

3.7.3 The proposed solution should support the use of web-based Background Intelligence Transfer Service (BITS) and utilizes idle network bandwidth to upload forensic data.

3.7.4 The proposed solution shall support the tuning of the forensic policies within the management server to dictate the type of forensic information to collect when a threat occurs.

3.7.5 The proposed solution shall have the capability to view high level system information about the endpoint after the threat has been detected and also provide the capability to retrieve the prevention data for further analysis and investigation.

3.7.6 The proposed solution shall have the capability to automatically create an exclusion value and exclusion rule from the detected threat report to allow the process to run on a particular endpoint.

3.8 Response

3.8.1 The proposed solution should provide option to remotely isolate the machine from the network.

3.8.2 The proposed solution should support process termination from the management interface

3.8.3 The proposed solution should support live remote shell for performing advance response activities

3.8.4 The proposed solution should support remote file manager to perform advance response activities.

Proposed Components: Hardware

Vendors should provide detailed explanation of the Hardware, as proposed along with the specifications of environmental equipment. Vendors are also requested to include optional additional equipment recommended by them with proper justifications.

All hardware should be provided with the latest server models only.

Item	Description of Requirement (Preferably HPE Brand)	Compliance (Yes/No)	Reference documents
Make & Model	**Specify**		
Chassis	2 U Rack Mountable		
CPU	2 * Intel Xeon Gold 5128 (2.3 GHz, 16 Core) Processor		
Memory	24DIMM slots. 128 GB memory scalable upto 3.0 TB using DDR4 Load Reduced DIMM (LRDIMM) operating at 2666 MHz (depending on processor model) Should be capable of identifying and reporting whether genuine OEM memory is installed for system reliability		
Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance		
HDD Bays	Upto 8SFF bays The drive carrier should have intutive icon based display along with "DO NOT REMOVE" caution indicator that gets activated automatically in order to aviod dataloss/downtime due to wrong drive removal.		
Hard disk drive	4*600GB SAS 10K RPM HDD's		

Host Bus Adapter	Dual Port HBA with 16Gbps		
Controller	Server should support Onboard SATA software RAID controller supporting SSD/HDD and at least two M.2 drives In addition, server should support one of the below controllers supporting Mixed Mode which combines RAID and HBA mode, PCIe 3.0 based 12Gb/s SAS Raid Controller with RAID 0/1/1+0/5/50/6/60/1 Advanced Data Mirroring/10 Advanced Data Mirroring (onboard or on a PCI Express slot) Storage controller should support Secure encryption/data at rest Encryption		
Networking features	1Gb 4-Port Network Adaptors		
Interfaces	Serial - 1 Micro SD slot - 1 USB 3.0 support With Up to 5 total: 1 front, 2 rear, 2 internal (secure)		
Bus Slots	3 PCI-Express 3.0 slots, atleast one x16 PCIe slots		
Power Supply	Should support hot plug redundant low halogen power supplies with minimum 94% efficiency		
Fans	Redundant hot-plug system fans		
Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support Energy Star ASHRAE A3/A4 UEFI 2.6 SMBIOS Redfish API SNMP v3 TLS 1.2 DMTF Systems Management Architecture		

System Security	UEFI Secure Boot and Secure Start support Security feature to ensure servers do not execute compromised firmware code FIPS 140-2 validation Common Criteria certification Configurable for PCI DSS compliance Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser Tamper-free updates - components digitally signed and verified Secure Recovery - recover critical firmware to known good state on detection of compromised firmware Ability to rollback firmware Secure erase of NAND/User data TPM (Trusted Platform Module) 1.2 TPM (Trusted Platform Module) 2.0 Smart card (PIV/CAC) and Kerberos based 2-factor Authentication Configurable for PCI DSS compliance Secure erase of NAND Chassis Intrusion detection		
Operating Systems and Virtualization Software Support	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware ClearOS		
GPU support	System should support NVIDIA's latest computational accelerators and graphics accelerators		
System tuning for performance	1. System should support feature for improved workload throughput for applications sensitive to frequency fluctuations. This feature should allow processor operations in turbo mode without the frequency fluctuations associated with running in turbo mode 2. System should support workload Profiles for simple performance optimization		
Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encyption deployment.		
Provisioning	1. Should support tool to provision server using RESTful API to discover and deploy servers at scale 2, Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows PowerShell		
Firmware security	1. For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable 2. Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also		

	store Factory Recovery recipe preloaded to rollback to factory tested secured firmware		
Server Management	Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resources user is authorized to view.		
	The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware • Appliance alerts		
	The Systems Management software should provide Role-based access control		
	Management software should support integration with popular virtualization platform management software like vCenter, and SCVMM		
	Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.		
	Should provide an online portal that can be accesible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contrats and status. The Portal should also provide a personalised dashboard to monitor device heath, hardware events, and contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).		
	Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.		
	The Server Management Software should be of the same brand as of the server supplier.		
Cloud Enabled Monitoring and Analytics	1. Offered servers shall have cloud enabled monitoring and analytics engine for proactive management. All required licenses for same shall be included in the offer. 2. Cloud Enabled Monitoring and analytics engine shall have capability to provide following: a. Providing Firmware upgrade and patch upgrade recommendations proactively. b. Providing power and support entitlement status. c. Recommendations to eliminate performance bottlenecks and		

	critical events, based on Analytics engine having capability of proactive recommendation for arresting the issues / problems.		
Warranty	3 Year 24*7 with 4Hr Response		

Chief Information Officer (CIO)

FORMATS ENCLOSED FOR TECHNICAL RESPONSE

Annexure 1: Covering/Forwarding letter by vendor on their letter head

[To be submitted on letter head of bidder as first page in the following format)

Date:

Ref Number:

To
The ……..
Telangana State Cooperative Apex Bank Limited (TSCAB),
4-1-511/3, Street Number 5,
Troop Bazaar, Koti,
Hyderabad, Telangana 500001

Dear Sir

SUB: RFP/Tender Reference:

Having read/understood the subject tender documents, we, the undersigned, confirm that we are eligible to submit the proposal under the tender and offer to supply, deliver, install and support the **'Hardware Software and Services** as per Tender, in conformity with the above tender documents as per Schedule of Prices attached in the commercial offer.

If our tender offer is accepted, we will submit the performance guarantee from any Bank as acceptable to the Bank for the amount mentioned as in the clause 'Performance Security" for the due performance of the Contract.

We agree to abide by this tender offer till 60 days from the closing date of tender and our offer shall remain binding upon us and may be accepted by the Bank any time before the expiration of that period. Until a formal contract is prepared and executed, this tender offer, together with the Bank's written acceptance thereof and the Bank's notification of award, shall constitute a binding contract between us. We also understand that the Bank is not bound to accept the lowest or any offer the Bank may receive.

Yours Truly

Authorized signatory of bidder

[Seal, Name, Signature and authority]

Commercial Response

Date:

Ref Number:

To

To
The ……..
Telangana State Cooperative Apex Bank Limited (TSCAB),
4-1-511/3, Street Number 5,
Troop Bazaar, Koti,
Hyderabad, Telangana 500001

Dear Sir

SUB: RFP/Tender Reference:

1. Supply, Installation & Commissioning of Cyber Security Operations Centre Software and Hardware.

Description	Make	Model No.	Unit Price	Qty	Taxes	Total Amt
x^{th} Year AMC/Support						
y^{th} Year AMC/Support						
z^{th} Year AMC/Support						

Yours Truly

Authorized signatory of bidder

[Seal, Name, Signature and authority]

MAF (Manufacturers Authorization Form)

Date:

Ref Number:

Dear Sir,

SUB: RFP/Tender Reference

We _____who are established and reputable Manufactures/Developers of _____ [mention the name of equipment, name of software, server/printer/Windows etc.] having factories/development centres at_____ and _____ do hereby authorize M/s

_____ (Name and address of Vendor) to offer their quotation, negotiate and conclude the contract with you against the above invitation for tender offer. We confirm that our company (as a single unit, not the group) has had a turnover exceeding Rs. __in last three fiscal years. We also confirm that in each of these three financial years, our company has made profit. We hereby extend our full guarantee and warranty as per terms and conditions of the tender and or the contract for the equipment and services offered against this invitation for tender offer by the above vendor. We hereby commit to the tender terms and conditions and will not withdraw our commitments during the process and or the period of contract.

We have also issued MDAF to …… who might be participating in this tendering process.

Yours Faithfully,

Authorized signatory of the Manufacturer/Developer of proposed solution components

[Seal, Name, Signature and authority]

Thank you all for participating in the Pre-bid meeting held on 17th July,2019 at 4 PM at our TSCAB HO and raised your valuable queries, below are the answers for all the queries raised by all the members.

1. Primary NOC, SIEM, INCIDENT/Ticketing Tools should be Perpetual License.
    a. Yes NOC tools and SIEM, ICIDENTINET Ticketing tools on perpetual basis only
2. SIEM License Based on devices or Log sources .not based on EPS Count.
    a. Yes SIEM based on devices we will add all of our Primary log sources(firewall ,AV, Servers, routers, syslog server to SIEM)
3. More than 300 correlation rules need to be created during installation.
    a. Yes
4. NOC alerts needs direct integration with ticketing.
    a. NPM, NCM, SAM, NTA tool alerts- Automation integration with Ticketing tool
5. SIEM should have threat intelligence feeds to identify malicious IP.
    a. Yes
6. NOC Alerts need to convert as Tickets.
    a. Yes, more than 200 alerts' scenarios need to be configured on NOC tools
7. Network configuration manager need to identify configuration and firmware vulnerabilities.
    a. Yes
8. All the tool implementation from TSCAB Head Office.
    a. Yes, but hardware delivery should be at our datacentre which is CrtlS Hyderabad.
9. Post implementation 1-year onsite support on call basics.
    a. Yes
10. How many syslog servers required? Minimum 20.
    a. 25

Also as discussed in the Pre-Bid meeting below three points are mandatory requirement for bid eligibility.

The proposed solution SIEM Solution should in the Gartner Magic quadrant.
The proposed solution Network Performance Monitoring Solution should in the Gartner Magic Quadrant

1. NPMD offerings should be— Network Performance Monitor (NPM), NetFlow Traffic Analyzer (NTA), Network Configuration Manager (NCM),

All the products should be provided with Manufacturer Authorization form including hardware.

Any deviation in the documentation will be disqualified during technical validation itself.

Note: no queries will be considered after pre-bid meeting