Annexure – 2 : Technical Specifications & Scope of work

Technical Specifications:

1. SD-WAN

A. Architecture

Sl No	Description	Mandatory(M)/ Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	The network should be implemented as true software defined network architecture with a centralized control plane residing in the software defined network controller also the data plane and control plane should be separate.	M		
2	The software defined network controller should be capable of being installed as a physical appliance on-premises.	M		
3	The software defined network controller should be capable of running as a virtual machine in the data centre.	M		
4	The communication between the software defined network controller and the branch device running on the remote entity should be secure and encrypted.	M		
5	The tunnel creation should be automatic without any manual configuration on the edges and the controller.	M		
6	The Solution Should be able to configure dynamic routing on the edge devices to adapt to changes in network topology and traffic patterns.	M		
7	The WAN path Selection at the branch locations should be based on the near real time analytics of the WAN Links Capacity & Quality (Packet loss, Latency & Jitter).	M		

8	The WAN path selection should be dynamically selected based on the policy set from the software defined network controller.	M		
9	The architecture should allow for internet break out at the local at branch, centralized location, remote entity (remote location) and cloud based on the application (based on need) and the policy defined in the software defined network controller.	M		
10	The control plane element should not use classical routing protocols to make the traffic forwarding decisions at the branch office locations.	I		
11	The selection of WAN links to anchor the traffic flows for an application traffic should be dynamic and policy driven.	M		
12	The solution components should include Centralized Network Orchestrator, Software Defined Network Controller, Edge Devices running in the remote branch locations, in the virtual networks) and Hub or Gateway Devices at the Data centre.	M		
13	The solution should allow network service insertion & chaining to expand the agility and utility of the network.	I		
14	The system architecture should allow the use the most preferred link based upon Link characteristics (Latency, Jitter, PLR) for critical applications as defined in policy.	M		
15	The system should have the capability to establish communication with a traditional WAN using routing protocols exclusively from the central location (Data Center) during the transition period, or as needed in the future.	M		
16	The architecture should ensure that application flow is always anchored on a single WAN link terminated on the branch device at any point in time.	M		

17	The SD-WAN should be able to load balance across links simultaneously or leverage the secondary link/s for spill-over if the bandwidth required for one session exceeds the available bandwidth on the best link. This lets high bandwidth applications have as much bandwidth as they need to perform optimally.	M		
18	In the Proposed SDWAN Solution, all links deployed at the critical branches (branch with 2 routers) and normal branch (branch with single router) should be in active-active state.	M		
19	The software architecture of the solution should allow for running on multiple processor architectures without needing virtualization.	I		

B. Network Integration

The system should support multiple types of WAN links to be terminated on the branch device.

Sl No	Description	Mandatory(M)/ Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	The system should support multiple wired links on the branch device such that it binds multiple MPLS links and an MPLS link with public internet link.	M		
2	All devices should be fully populated. Remaining (in addition to minimum WAN and LAN ports) ports should be configurable as either LAN or WAN ports as per bank's requirement	M		
3	The system should support internet links that can be authenticated using PPPOE.	I		
4	The system should support termination of Internet Leased Line (ILL) on the branch device.	I		

5	The system should support Multi-Protocol Label Switching (MPLS), Internet Leases Line, DSL Broadband and Wireless WAN (3G and 4G/LTE) on the same branch device.	M		
6	The system should support termination of symmetric WAN links on the branch device.	M		
7	The system should terminate MPLS as well as Broadband links to device and must be able to use both the links for traffic. Any failure of a link must result in steering traffic on another link without any manual intervention.	M		
8	The system should support termination of asymmetric internet links the branch device.	I		

C. Virtual Private Network

The system should implement a secure virtual private network that connects the branch locations, virtual locations on the public cloud and data center on one single managed network.

Sl No	Description	Mandatory(M)/ Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	The system should allow creation of multiple virtual private networks as a collection of local area networks present at each branch location and DC HUB location.	M		
2	The system should allow creation of an encryption policy that has a unique encryption key or standardized encryption algorithm.	M		
3	The system should allow an encryption policy to be attached per virtual private network.	M		
4	The system should allow centralized generation of the encryption key/ standardized encryption algorithm.	M		

5	The system should allow automated and policy driven refresh of the encryption key / standardized encryption algorithm per virtual private network	M		
6	The system should allow time-based/scheduled manner refresh of the encryption key / standardized encryption algorithm for each virtual private network.	I		
7	The system should not store the encryption key / standardized encryption algorithm in disk on the remote device.	M		
8	The system should only allow dynamic tunnels to be created without any static overlays between branch devices and the hub device.	M		
9	The system should allow for full mesh connectivity between the Data Center, and the branch locations.	M		
10	The system should allow for hub-and-spoke connectivity between the data center (hub) and the branch devices (spokes).	M		
11	The system should allow for alternate hub destinations to be created for application specific traffic using a policy defined for it.	I		
12	The system should be able to retrieve the network information without any peering protocols like BGP, OSPF or any other routing protocol over WAN.	M		
13	The system should ensure that the virtual private network specific configuration is not be attached to physical or logical WAN or LAN Links or IP addresses or physical interfaces on the branch device.	M		

14	The system should ensure that any change in physical connectivity (Link 1 to Link 2 connectivity in case of multiple links being terminated on the branch device) or any change is physical connectivity type (Link 1 connectivity changed from internet broadband to MPLS or vice versa, in case of multiple WAN links being terminated on the Branch device) does not require any change in virtual private network configuration in the controller or physical/virtual device at location.	M		
15	The system must be able to make virtual private network paths dynamically on power on without using of any routing protocols on the WAN side.	I		
16	The system should support encapsulation types, but not limited to following: A. IPSEC B. GRE C. UDP D. No Encapsulation	M		
17	The system should be able to automatically pick the tunnel encapsulation type based on the application and based on the policy specified in the software defined network controller.	I		
18	The system should support the following minimum authentication algorithms for Data Integrity: a. SHA-512 b. SHA-384 c. SHA-256	M		
20	The system should support the following minimum encryption algorithms for Data Security: a. AES-128 b. AES-256	M		

21	The system should ensure that virtual private network configuration and policy is performed in the controller. The addition of one or more branch devices in to the network should not require any changes in the virtual private network configuration in software defined network controller.	M		

D. Network Performance, Traffic Management and Path Steering

The system should take into consideration the individual and total bandwidth capacity of all the WAN links terminated on the branch device, the quality of the WAN bandwidth on each individual link, nature of application and defined policy to ensure adequate network performance for the application traffic.

Sl No	Description	Mandatory(M)/ Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	The system should be able to prioritize inbound and outbound traffic.	M		
2	The system should be able to select the optimum path based on the network parameters like Latency, Jitter, PLR and network capacity.	M		
3	The system should enforce by default that the traffic flowing between two sites taking the same path in both directions.	I		
4	The system should be able to prioritize business critical applications and should prioritize this traffic over others during congestion.	M		
5	The system should support end-to-end packet classification, marking, and bandwidth allocation.	M		
6	The system should be able to automatically steer traffic flows to the optimum path, based on policy definition in the software defined network controller.	M		
7	The system should always ensure granularity at a flow level while steering traffic to a given path.	I		

8	The system should employ a centralized policy driven traffic management to steer traffic.	M		
9	The system should ensure that the session is not impacted when switching between paths.	M		
10	The system should be able to provide a centralized internet break out for all internet bound traffic.	M		
11	The system should load balance the application flows based on the nature of the application, priority of the application flow based on the quality of service and other policies specified by the centralized software defined network controller. The system should anchor such a prioritized application flow on the WAN link with the best quality (latency, jitter and packet loss ratio) metrics.	M		

E. Authentication, Authorization and Accounting (AAA)

Sl No	Description	Mandatory(M)/ Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	The system should authenticate every user on the network using Active Directory and/or Active Directory Federation Services (ADFS) to support single sign on for all applications hosted in the data center, in the Cloud and/or consumed as a software as a service.	I		
2	The central management system should authenticate and authorize every administrator accessing the branch device using the TACACS+ and Active Directory in the backend for the administrator user authentication and authorization.	M		

3	The system should be able to integrate with the TACACS+ service and Active Directory to pull and display the access logs across the network. This should be sortable and filterable on a per location basis and on a per administrator basis. The default storage period of these logs should be at least 30 days.	I		

F. Security

Sl No	Description	Mandatory(M)/ Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	The system should implement a stateful firewall on the branch device that can be centrally provisioned and managed from the software defined network controller.	M		
2	The system should be able to provide URL filtering with a URL blacklist and a whitelist at the branch device.	M		
3	The system should be able to block/filter Internet-bound traffic based on domain names on the branch device.	M		
4	The system should be able to integrate with 3rd Party Cloud Security Providers for end to end branch office security.	I		
5	The system should be able to integrate via a service chain on the hub device in the Data Center with a next generation firewall.	M		
6	The system should provide data and metrics to enable internal security teams to audit and analyze security-related incidents via SNMP traps (SNMP v3), Syslog that can be consumed by a 3rd Party SIEM system.	M		

7	The system should support Access Control Lists (ACL) to allow or deny traffic, DDoS mitigation functionality and protect DDOS attack like UDP Flood, Ping of Death etc. at Branch and DC Device.	M		
8	Controller and the device should be able to access only through web based for configuring and controlling. SSH, USB port and telnet should be disabled by default and console should be password protected.	M		
9	The System should have capability to white-list devices (i.e. PC, NW Switch.) MAC IDs available in the LAN at Branch and SDWAN device should not allow access to any unrecognized/unknown MAC ID(s). The control/management of MAC-ID white-listing and MAC-ID repository should be at central controller.	M		

G. Visibility, Analytics & Monitoring

The centralized controller should provide mechanism to get visibility in to what is happening in the software defined network.

Sl No	Description	Mandatory(M/ Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	The system should provide a mechanism to monitor the performance for Virtual Private Network.	M		
2	The system must be able to monitor ISP link parameters like link quality, link usage and link congestion and should be able to provide historical data on the same for a period of minimum 30 days.	I		
3	The system should support application-level monitoring and traffic control to improve business-critical application performance, facilitate capacity management and planning, and reduce network operating costs.	M		

4	The system should be able to dynamically steer traffic from one WAN link to another based on policy.	M		
5	The system should be able to track the reliability and performance of WAN links.	M		
6	The system should have the ability to provide visualization of traffic flows.	I		
7	The system should support the ability to automatically detect applications, report the application traffic, and allow for marking and filtering via policy.	M		
8	The system should be able to gather application and flow information.	M		
9	The system must measure the link capacity proactively while ensuring that it does not affect more than 10% of the link's capacity for the monitoring/probing traffic.	I		
10	The system should gather link information in real-time.	M		
11	The system should allow administrators of the network to be grouped with well-defined roles assigned to them. The system should support monitoring only user role, network change administrator role and an overall system administrator role with permissions to manage the software defined network controller.	M		
12	The system should allow monitoring of Packet loss ratio, Delay, Jitter, and Bandwidth utilization of each WAN link.	M		

H. Management & Orchestration

The system should support centralized management & orchestration of the software defined network.

Sl No	Description	Mandatory(M/ Important (I)	Complied (Yes/No)	If No, Bidder's Remarks

1	The system should offer the choice to deploy either on-premises or cloud hosting of all SD-WAN software components.	I		
2	The system should support a centralized single plane of management system to allow device configuration, policy provisioning, software updates and assurance capabilities.	M		
3	The system should support functionality to manage the performance of Internet links. The system should determine that Internet performance is degrading and notify the administrators.	I		
4	The system should support application visibility, application reporting, marking, filtering, and policy.	M		
5	The system should provide a dashboard that provides state of new appliances (Online, Offline, Not connected).	I		
6	The system should provide the ability to centralize management across cloud, SD-WAN, and wired/wireless LAN environments.	M		
7	The system should allow policies to be applied across WAN, LAN, and cloud-based resources.	M		
8	The system should enable a DevOps approach for network operations for the following: a. Rapid site provisioning. Rapid deployment of new applications in a way that is secure and offers high performance. Policies that follow the users, things, and workloads. Change management with ability to verify proper application of policies.	I		
9	The system should be able to notify external systems of events such as faults/alarms as Syslog messages, SNMP (SNMPv3) traps.	M		
10	The system must be able to send e-mail and SMS notification for events and alerts. The valid email addresses and numbers for receiving the SMS notifications should be configurable centrally.	M		

11	The System should be capable of exporting traffic statistics to AppFlow or NetFlow collectors.	I		

I. Network Wide Policy Enforcement

Sl No	Description	Mandatory(M) Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	The system should support centralized application of policies network wide or across subset of branch locations from the centralized software defined network controller.	M		
2	The system should allow definition and enforcement of traffic forwarding policies on the basis of application(s), application categories, direction of the traffic (from LAN to WAN or from WAN to LAN at the branch), from specific subnet(s), to specific subnet(s) and custom IP Address(es) for traffic from LAN to WAN on a branch.	M		
3	The system should support definition and enforcement of traffic forwarding policies that manage the steering of the traffic from the LAN to WAN at branch locations. The policy should include the traffic steering based on the WAN link type (MPLS, Internet, or any of the type of WAN link) available at the branch location.	I		
4	The system should allow definition and enforcement of traffic forwarding policies that allow encapsulation of the traffic with IPSEC or UDP or GRE or no Encapsulation for all traffic going from the LAN to WAN or from WAN to LAN.	M		

5	The system should allow definition and enforcement of traffic forwarding policies that allow traffic to be forwarded to a particular site (branch), all sites (full mesh topology), hub location (hub and spoke topology), at the same branch location or a to a custom location based on the traffic from specific subnet(s), to specific subnet(s) and custom IP Address(es) for traffic from LAN to WAN on a branch.	M		
6	The system should allow definition and enforcement of WAN link load balancing policies that allow steering of application flows on a WAN link with best quality (flow based and packet-based load balancing) with the quality defined in terms of latency, packet loss and jitter.	M		
7	The system should allow definition and enforcement of traffic load balancing policies that allow utilization of all the available WAN links simultaneously if the link latency is less than 50 milliseconds (Packet by Packet load balancing).	I		
8	The system should allow definition and enforcement of quality of service policies that allow traffic from the LAN to WAN and from WAN to LAN at a branch to be prioritized as the following: 1. CRITICAL 2. HIGH 3. MEDIUM 4. LOW Based on the basis of application(s), application categories, direction of the traffic (from LAN to WAN or from WAN to LAN at the branch), from specific subnet(s), to specific subnet(s) and custom IP Address(es).	I		
9	The system should allow definition and enforcement of traffic rate limiter on the traffic from LAN to WAN and WAN to LAN with policer (at a minimum with a flat rate policer).	M		

10	The system should allow definition and enforcement of access control lists (ACL) to allow or deny traffic from WAN, or to WAN or both ways based on the application category, application, from IP subnet and/or to IP subnet and the State of the connection. This should be also applicable in case the traffic is to be forwarded from one virtual private network to the other.	M		

10. Provisioning and Deployment

The system should support zero touch provisioning of remote branch locations.

Sl No	Description	Mandatory(M) Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	The system should also allow for plug and play installation of branch devices without requiring any manual configuration at the remote location.	I		
2	The system should allow automatic software upgrades from the software defined network controller across all deployed devices or a group of devices in the branch offices, data center and the cloud.	M		
3	The system should allow for modular upgrade of the software running on the branch devices from the centralized software defined network controller in order conservatively use the bandwidth at the remote branch locations for software upgrades.	I		
4	The system should be available and running when the software is being downloaded in to the branch device from the central software defined controller.	M		

K. Software Defined Network (SDN) Controller

The system should support software defined controller that can be deployed in the public cloud (Amazon Web Services, Microsoft Azure) or in the Enterprise Data Center.

Sl No	Description	Mandatory(M) Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	The software defined network controller must be able to generate notifications for the following: 1.Link Flaps at the remote branch location 2.ISP link quality degrade 3.Link utilization along with threshold 4. CPU, Memory and Disk Utilization of the Branch Device	M		
2	The notifications generated by the software defined network controller must be forwarded as email to a pre-configured email address.	I		
3	The notifications, events and alerts generated by the controller should be forwarded as SMS alerts to registered mobile numbers. The controller must allow specification of a SMS gateway for this purpose.	I		
4	The software defined controller must be able to scale more than 10K based upon customer requirements.	I		
5	The software defined network controller must have REST APIs available for 3rd party integration or integration with custom automation tools.	M		
6	The software defined network controller must be able to monitor the WAN links terminated on the device deployed at each branch location for link quality and capacity. The controller must store the data for a minimum of 30 days.	M		

7	The software defined network controller must monitor the WAN link for congestion. This data must store by the controller for a minimum of 30 days.	M		
8	The software defined network controller measures the link usage (WAN as well as LAN). The software defined network controller must store this data for a minimum of 30 days.	M		
9	The software defined network controller must monitor and report the WAN link flaps at branch location. This data should be stored for a minimum of 30 days.	M		
10	The software defined network controller should be able to monitor the traffic flows in the branch location.	M		
11	The software defined controller must be able to monitor, and report top 40 applications by usage across all branch locations, in a branch location along with the data rate and flow usage. This data must be stored by the controller for a minimum of 30 days.	I		
12	The software defined network controller should be able to monitor and report the top 40 LAN users in a branch location. This data should be stored by the controller for a minimum of 30 days.	I		
13	The software defined network controller must be able to report the total number of online and offline branch locations.	M		
14	The failure of the software defined network controller must not bring down the data path of the network.	I		
15	The software defined network controller should allow deployment as a single tenant / dedicated controller or a multi-tenant controller.	I		

L. Data Center Deployment

The system should allow for deployment at the data center as a central or a hub location.

Sl No	Description	Mandatory(M) /Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	The system should allow deployment of the SD-WAN Gateway appliance in the Data Center as a rack mounted physical appliance.	M		
2	The SD-WAN Gateway appliance deployed in the Data Center should be able to peer with the existing routers in the Data Center.	M		
3	The SD-WAN Gateway appliance should be capable of peering using standard routing protocols with the existing MPLS router in the Data Center.	M		
4	The SD-WAN Gateway appliance should be available as software that can be deployed on an existing hardware appliance (Intel x86 server) in the Data Center.	I		

M. High Availability

The system should allow for redundancy and deployment with high availability in the data center and remote branch locations.

Sl No	Description	Mandatory(M) Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	The system should allow the SD-WAN Gateway Appliance in the Data Center to be deployed in **Active/Active** redundant configuration for high availability.	M		
2	The system should allow the SD-WAN Gateway Appliance in the remote branch offices to be deployed in **Active/Active** redundant configuration for high availability.	I		

3	The software defined controller should be architecturally highly available with a redundant **active-active** deployment in both data center and in cloud.	I		

N. Scalability

The system and the solution should scale to support the current number of branch locations, data centers and the public cloud regions. The system should support the future expansions of the enterprise with the ability to scale without requiring a re-installation of the controller as new branch locations get deployed.

Sl No	Description	Mandatory(M)/ Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	Minimum number of branch locations supported by a single instance of software defined network controller should be at least 5000.	M		
2	Minimum number of concurrent VPN tunnels supported with a single instance of the software defined network controller should be at least 5000.	M		
3	The system should support at least 5000 network segments network segments (virtual private networks) with a single instance of a software defined network controller.	I		
4	The system should support at least 5000 locations connected to a network configured in a full mesh configuration.	I		
5	The system should support Internet Protocol version 6 (IPv6) dual stack from day one.	M		

O. Hardware Specification

Location Type A - For Branch locations / Regional Offices

Sl No	Description	Mandatory(M)/ Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	Proposed Solution must be of desktop form factor with fixed 4 10/100/1000 RJ-45 Ports, minimum of 4GB RAM, 16GB storage and USB2.0/3.0 Ports with a minimum MTBF 70000 hours.	M		
2	Proposed Solution must be available in virtual form factor to run as a VM either on Hypervisor like KVM or ESXi or Public/Private cloud.	I		
3	SDWAN solution must be capable of Active/Passive HA.	I		
4	SDWAN solution must be capable of terminating broadband, ILL, MPLS, 4G Dongle connectivity.	M		
5	SDWAN solution must have in build SIM slot capability.	I		
6	SDWAN solution must be able to use all WAN links together at same time.	M		
7	Device must have USB ports.	M		
8	Device must be able to support VLAN tagged packet transmission and receive over WAN as well as LAN interfaces.	M		
9	Device must have 4 10/100/1000T RJ45 ports. It must be able to change the role of these ports using system configurations and without re-imaging the software.	M		
10	Device must be able to support 2000 tunnels minimum and device must be able to support more number by increasing physical resources.	I		

Location Type B - For the Internet Routers/Head Office/Central Monitoring offices/Project office

Sl No	Description	Mandatory(M)/ Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	Proposed Solution must be of desktop form factor with fixed 6 10/100/1000 RJ-45 Ports, minimum of 8GB RAM, 32GB storage and USB2.0/3.0 Ports with a minimum MTBF 70000 hours.	M		
2	Proposed Solution must be available in virtual form factor to run as a VM either on Hypervisor like KVM or ESXi or Public/Private cloud.	I		
3	SDWAN solution must be capable of Active/Passive HA.	I		
4	SDWAN solution must be capable of terminating broadband, ILL, MPLS, 4G Dongle connectivity.	M		
5	SDWAN solution must be able to use all WAN links together at same time.	M		
6	Device must have USB ports.	M		
7	Device must be able to support VLAN tagged packet transmission and receive over WAN as well as LAN interfaces.	M		
8	Device must have 6 10/100/1000T RJ45 ports. It must be able to change the role of these ports using system configurations and without re-imaging the software.	M		
9	Device must be able to support 15000 tunnels minimum and device must be able to support more number by increasing physical resources.	M		

Location type C - For DC/DRC

Sl No	Description	Mandatory(M)/ Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	Proposed Solution must be of 1RU form factor.	M		
2	SDWAN solution must be capable of Active/Passive HA.	M		
3	SDWAN solution must be capable of terminating broadband, ILL, MPLS.	M		
4	SDWAN solution must be able to use all WAN links together at same time.	M		
5	Device must be able to support VLAN tagged packet transmission and receive over WAN as well as LAN interfaces.	M		
6	Device must have Fixed - 2x1G RJ45 Pluggable-4x1G RJ45/SFP ports. It must be able to change the role of these ports using system configurations and without re-imaging software.	M		
7	Device must be able to support 30000 tunnels minimum and device must be able to support more number by increasing physical resources.	M		

P. Support Requirements

Sl No	Description	Mandatory(M)/ Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	Technical and Solution Support (L1) should be available 7x24x365.	M		
2	Technical and Solution Support (L2) should be available on all working days of each bank.	M		

3	Hardware Replacement for Edge Location as per the service support clause mentioned in the RFP.	M		
4	Hardware Replacement for Hub-Data center location - On-site Spare	I		
5	Managed Services should be available directly by OEM or from Partners.	M		
6	Product usage training should be available directly from the OEM or from the Partners.	M		

2. NMS & Netflow Management

Sl No	Description	Mandatory(M)/ Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	The tool should provide complete Network monitoring & management system including:	M		
	1. IT Infrastructure Monitoring (Network, Server, Storage, Cloud, VMs, CCTV, Wireless, UPS etc.)	I		
	2. Traffic Flow Analysis with QoS Monitoring	M		
	3. SDWAN Performance Monitoring	M		
	4. Reporting & Dashboarding with integration	M		
2	The OEM should have a support center in India	M		
3	The solution should be scalable to monitor & manage more than 5000 plus devices and 6000 links.	M		
4	The organization should have ISO 270001 certification for their internal processes and certificate must be provided	M		
5	The solution should be available as Commercial-Off-The-Shelf (COTS) software	I		
6	The tool should be flexible to store the polled data based on customer's retention period	M		
7	The tool should be able to discover both IPv4 and IPv6 devices for monitoring	M		

8	The tool should be a unified system which can monitor the health and performance of network devices, servers, applications, databases and any IT device	M		
9	The tool should provide option to create specific views / dashboards for any type of device including Network devices, firewalls, servers, applications , Wi-Fi, VSATs, UPS etc.	M		
10	The solution should be completely multi-tenant where in every module and system being used can be assigned to a specific set of users or a group of users.	M		
11	The system should be capable to retrieve and show fault, performance , inventory and SLA data in a single dynamic view	M		
12	The system should have capability to add any additional information about the nodes via custom fields and it should be available on all filtering in other modules not limited to notification, dashboards, reports etc...	I		
13	The system should allow to create Node Tags for device grouping and resource/interface tagging for element grouping. Apart from Node Tags, system should also have option to do device grouping based on default fields.	M		
14	The solution should provide a mechanism to create multiple thresholds for each parameter which is being monitored	M		
15	Any fault, performance, views, reports should be configurable till node, component or parameter level. The tool should support granular level of control across the system	M		
16	The tool should provide the option to export the views into PDF, Word, Excel, HTML etc. formats depending on the need.	M		

17	The tool should allow each user account to have specific type of toolbar according to the administrator's requirement and each account should only be able to see/manage the list of equipment's for which they are authorized	I		
18	The tool should provides the option to have the portal account for the end customers with restricted views limited to their specific infrastructure. The tool should have the capability to be implement in DMZ and non-DMZ zone with adequate security.	M		
19	The tool should have proper segregation of admin users and portal users via separate logins and authentications. The system should also have capability to integrate with 3rd party authentication applications like TACACS, TACACS-2, Active Directory, PIM with option for session-based approvals	M		
20	The tool should have Role based Access Control and administrator should be able to create custom roles and assign module level privileges	M		
21	The tool must provide powerful connectivity to other data sources or 3rd party applications for data import and export using REST APIs	I		
22	The tool should provide REST APIs to integrate with IT Infrastructure Management, Configuration Management, Network Management, CRM tools to automate Events to Ticket	M		
23	The tool should also have an optional bi-directional integrated Network Configuration and Change Management tool with option to use NCCM features in future easily by enabling the license for it without having to do any additional installations. The integration should allow assets and topology to sync from the NMS module to the NCCM features for helping in Root-Cause-Analysis of faults	I		

24	The solution should be having single UI console rather multiple different UI console. If should be flexible enough to configure monitoring, configuration management and log management relevant data in a single dashboard and view together for all solutions.	M		
25	View all the licensed modules / system from the single console to avoid user switch over from one console to another. It shouldn't be SSO kind with different console it should be flawless and all the data will be available from single console rather multiple console.	I		
26	The tool should have option for CSV based discovery for bulk discovery and it should allow options to add customer fields to support customer specific data to upload during discovery	M		
27	The tool should have the option to fetch topology via SNMP for ARP tables from routers , MAC tables from layer 2 switches, cisco Discovery Protocol, Link Layer Discovery Protocol, Foundry Discovery Protocol or SynOptics Network Management Protocol. The discovery should be automated and continuous.	M		
28	The tool should have the capability to manually add any additional topology in the network. Options to add via GUI or tabular should be available. The system should also allow downloading of topology connections.	M		
29	Discovery has to work intelligently by identifying the device in the network by the given IP range and categorize into network devices and servers with vendor and model details.	M		
30	Automatically learn devices that supports SNMP, HTTP, Ping, SMTP, POP3, WMI,JMX, SOAP, REST API,PDC, SSH and Telnet along with any required protocol to communicate to the devices.	M		

31	The tool should be able to discover both the Primary and Secondary line of each branch connected to DC and monitor the connectivity with the link IP address for fault and performance.	M		
32	Doing discovery for one module / system should update the devices for the other modules as well instead of user doing the discovery again and again for the different modules / system. Like if the devices is discovered for the monitoring, it should automatically considered for the NCCM as well based on devices type	M		
33	The solution should be able to stop SLA calculation for every node in case of known downtimes. There should be a one click alarm masking capability in the system	M		
34	SLA calculation should be made for individual link wise as well as with the consideration of both the Primary and Secondary link together (for ISP Links) instead of individual link based. The downtime calculation will be measured when both the links are down for internal reporting and link based for ISP reporting. The tool should provide the flexible configuration in UI itself based on user needs	M		
35	SLA module should have the template based configuration where each branch measurement will be different for internal and ISP reporting. User should be able to configure multiple templates for the different need and assign the related branches to the template which will give the flexible and simple configuration for different needs.	M		
36	It is not only for the branch connectivity with primary and secondary link, system should provide the flexibility for grouping multiple resources as a single service and allows the SLA computation against the service instead of individual resource / component level SLA measurement.	M		

37	Different branches will have different working hours. Based on the work hours the SLA needs to be computed for the Branch Isolation and the ISP Links availability.	M		
38	The tool should support global threshold and it should have an option to define individual resource/interface statistics level threshold	M		
39	The tool should have build in algorithms to start the monitoring with zero threshold configurations	M		
40	The tool should have self learning algorithms to do auto baselining and should calculate the thresholds of components or nodes automatically.	M		
41	The tool should support configurable parameter like frequency, data duration, resolution duration, sigma based polarity value, reset points to should available to fine tuning the algorithm	M		
42	All thresholds within the tool should have a set point , reset point, polarity , set point message and reset point message for ease of use.	M		
43	The tool should also have anomalies detection and should be able to stop alarm flooding using dynamic thresholds	M		
44	Single threshold configuration should support all the severities rather for each severity needs different threshold configuration for the same stats.	M		
45	The tool be able to detect & highlight faults (abnormal situations) occurring anywhere within the network	M		
46	The tool be able to provide Filtering, De-duplication, Holding, Suppression and Correlation capability to let user focus on the critical event that affects the business and business processes	M		

47	The tool be able to provide multi-level (preferably six-level) Severity definition, will handle events automatically and inform the designated person as per operational requirement	M		
48	The tool should support separate Rule Engine based alarms apart from the generic threshold.	M		
	a. The tool should be able to have capability to configure Device Group based, Node Based, Resources/Interface based, and Aggregation link based.	M		
	b. On Selection of Nodes/Resources/Aggregation links it have flexibility to filter based on fields available in node information	M		
	c. Rules should have option to apply configuration on top of performance value or based on configured threshold alarms	M		
	d. Rules should have option configure the breach based on min, max and average values	M		
	e. The tool should be able to have option to configure rules n repeat counters	M		
	f. The tool should be able to have options to select custom alarm and clear alarm messages for individual configured rules	M		
	g. The tool should be able to have option to send severity levels like error, warning and information	M		
	h. Notifications support based on configured rules	M		
49	Provides alarm suppression with hold time and aid in prevention of flooding	M		
50	Sends alert via E-mail, SMS, Execute Batch file, SNMP Trap, XML notification, Pop-up window and Audio alert	M		
51	The tool should capture the SNMP traps from network devices and convert them to link down alarms automatically	M		

52	Provide Alarms Suppression capabilities so that any duplicated events can be tracked to provide just a single event notification	M		
53	Monitors all traffic from all the interfaces of the network device. Provides traffic Utilization based on individual interface level, nodes level or based on the group by location, branch, departments etc. as an Avg, Min and Max bandwidth, utilization, throughput or any custom monitoring parameters.	M		
54	Tool should have the provision to change the polling interval to any frequency depending on the priority till the individual component / resource level like each interface might have the different polling interval in the same device based of the criticality and importance of service customer	M		
55	Tool should be able to monitor SDWAN device performance parameters like Latency, Packet Loss, Jitter, BFD Sessions, Control Status, CPU Utilization, Memory Utilization etc.	M		
56	The tool should have capability to configure business, non-business hours or custom time polling. These configuration should be available for every device as well as every component in the device.	M		
57	Provision to disable and enable the polling of specific type of devices	I		
58	The tool should have capability to configure the maintenance period for any device. When device is in maintenance period there is no polling done and the SLA clock on the device is stopped.	M		
59	Provide a notification mechanism that allows administrator to define what notification channel to be used in different time of days, and able to trigger multiple notifications to alert multiple person and actions	M		

60	Provide escalation and acknowledgement function to provide the mechanism to ensure alternative personnel will be alerted when there is a critical situation and acknowledgement mechanism for generated alerts. The escalation should be available for any number of hierarchical sequence.	M		
61	Provide standard reports that display current status of nodes and interfaces. Reports could be viewed on daily graph (5 minute average), weekly graph (1 hour average minute average), monthly graph (1 hour average) and yearly graph (1 day average)	M		
62	Provide online and offline reports that allow the user to view the present usage of their devices. Reports generates should be exportable in the format of HTML, PDF, Excel and CSV	M		
63	Automatically generate daily reports that provide a summary of the network as well as custom Reports and that are automatically sent by email at a pre-defined schedule to any recipient or save into any specific folder or drive.	M		
64	Allows end-users to browse all reports using any web browser like Microsoft Edge(Internet Explorer), Mozilla Firefox, Google Chrome etc. without the need to install any report specific software	I		
65	Provides the option to get the required report as an all hours, business and non business hours for detailed analysis. Also Provide report on single or multiple statistical split based on the operation need as option during the configuration	M		
66	Provide correlation report between all major network devices to determine if there is any degradation in these devices	M		

67	Significantly reduce the potential of generating unwanted, non-business critical, alert floods that are symptomatic of many systems management tools by alerting based on a problem identified for an end-to-end, business transaction. Identifies the root cause of any IT problem detected and filters out irrelevant information to let the user concentrate on solving the problem	M		
68	Supports instant diagnosis of the node status through Ping, Telnet and SNMPwalk	M		
69	Support Real-Time report generation for checking continuous reachability of target device	M		
70	The tool should have capability to create a user level repository of all the issues being faced. Users should have the rights to add data to this repository and system should be intelligent to automatically retrieve back information from here based if same issue re-occurs	M		
71	The tool should have an option to highlight the Top Processes consuming Server CPU / Memory for any CPU Utilization High / Memory Utilization High alarm with a single mouse-click	M		
72	The tool should provide many different types of topology representation. To perform the following :	M		
	1. Display physical connections of the different devices being monitored in the system	M		
	2. Display flat maps of the entire network or networks in a single view	M		
	3. Display customer maps based on user configurations	M		
	4. Display maps based on geo locations	M		
	5. System should provide L2 and L3 topology of the complete network	M		
73	The tool should automatically learn IP Networks and their segments, LANs, hosts, switches, routers, firewalls etc. and to establish the connections and to correlate	M		

74	It should have the provision to search specific device or resources in a view, map to specific background for each level of the network, upload and change icons of devices/background of the network layers	M		
75	It should show the status of the connections based on the dependent connections and the utilization of the links by displaying connection with different width	M		
76	The tool should navigate to node page or interface page on click of respective node or link	M		
77	Filter topology view based on device group, node tag, vendor, model, IP address, host name etc.	M		
78	The tool should have option to display distance between devices in Topology Maps especially for branch gateway devices	M		
79	Have algorithmic auto arrangement capabilities. The tool should use standard algorithms like forceAltas2base , repulsion or barnerHut to makes sure the map views are non cluttered and arranged to the best non-overlapping method.	I		
80	The tool should use SVG Map based map view with drill down option is required. The tool should have capability to drill down views based on the office/branch location.	M		
81	Change Country/Region/State/City colour to Red/Orange/Green based on the device status, Red for all node down and orange for one or more node down and Green for all node up.	M		
82	Provides provision to draw & map user specific network diagram	M		
83	The tool should have Integrated Web based feature to build Network Diagram, No separate client window to configure network Diagram. The builder should be a Visio like system with all pre-loaded shapes and icons.	M		

84	The tool should support Drag & Drop based Network Diagram builder, Dynamically Upload Images, Customizable objects to support multiple vendors, capability to export maps in an XML format and upload to any other system.	M		
85	Any graph or network diagram configured should have functions to associate every component in the diagram to an existing node or resource. Additionally system should allow to associate any parameter being monitored to the specific element in the diagram. All network diagram's are user controlled and viewable to only specific configure users.	M		
86	The tool should be able to define Primary & back up line connection, so if primary line fails it should switch over to backup line & notify to administrator	M		
87	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 and also sampled NetFlow data. The tool should have capability to alternatively capture flow data via packet capture.	I		
88	The tool should be able to identify which users, applications, protocols, countries, AS numbers, top routers, and top interfaces are consuming the most bandwidth	M		
89	The tool must be able to store ALL flows without any rollups or loss for retention period - for security and audit purposes.	M		
90	The tool should be able to highlight the IP addresses of the top bandwidth consumers on the network and find out unwanted bandwidth usage	M		
91	The tool should be able to associate traffic coming from different sources to application names	M		

92	The tool should be able to be able to receive flows from non-SNMP-enabled devices, like VMware vSwitch	M		
93	The tool should be able to monitor Class-Based Quality of Service (CBQoS) to find out if traffic prioritization policies are effective and if business-critical applications have network traffic priority. The tool should be able to also support CBQoS Nested policies	M		
94	The tool should be able to monitor Type of Service (ToS), Differentiated Services Codepoint (DSCP), and Per-Hop Behaviour (PHB),BGP AS and NEXT HOP	M		
95	The tool should be able to have options to specify data retention periods	M		
96	The tool should be able to provide flow analysis with 1-minute granularity and The solution should be able to monitor up to 5 million flows per second, and should employs advanced optimization methods	M		
97	The tool should be able to provide real time flow and traffic analysis with 5 second granularity	M		
98	The tool must alert when traffic to known malicious domains are encountered	M		
99	The tool must provide tool to investigate if a security incident caused a breach or just a scanning	M		
100	The tool must provide way to list all Internal hosts that are impacted by a security incident	M		
101	The tool should be able to help in locating infected computers in case of virus outbreak	M		
102	The tool should be able to help to recognize DOS attack	M		
103	The tool should support VM, Hypervisor and Cluster monitoring from different vendors like VMWare, Nutanix, KVM, Linux etc.	M		

104	Cover geographically distributed networks through multi-level scalable distributed deployment architecture	M		
105	Ability to add new pollers at without any need for additional license.	I		
106	Integration should provide the option in both north as well as south bound integration on each module level. Any fault details should be able to send to third party CRM, Customer Portal, UNMS or even EMS if needed using the Trap, XML and even direct database query integration	I		
107	A completely integrated network management system which can monitor and management networks, servers, applications, WIFI, CCTV , VSAT etc from a single platform and should show an end to end visibility of all the services in your network.	M		
108	The NMS and NCCM solution should be integrated on real time basis using both NBI and SBI for sending and receiving required information. All the details should be available from the single console for the easy use of infromation and It should enable the two way communication / handshaking between NMS and NCCM.	M		
109	All the faults and threshold crossing alerts (TCA) should be synchronized from NMS to NCCM on real-time and all the configuration changes and auditing information should synced with NMS from NCCM on real time basis.	M		
110	The threshold should support two conditions for triggering an event and notification:	M		
	1. A specified number of consecutive polls must meet the condition.			
	2. Out of M poll points, at least N must breach the condition.			
111	This allows for flexible and robust monitoring, triggering events based on either consecutive breaches or a set number of breaches across all polls.	M		

112	Panel View Requirements	M		
	a. Realistic Representation: The panel view should resemble the actual device front panel.	M		
	b. Automatic Detection: The tool must auto-detect the device model and display the correct panel without additional configuration.	M		
	c. Comprehensive Monitoring: The panel should show all monitored interfaces with their statuses.	M		
	d. Dynamic Indicators: Include live fan icons and LED indicators for power status.	I		
113	Virtualization Monitoring Requirements	M		
	a. Guest OS Monitoring: Track all guest operating systems, including running processes and services.	M		
	b. Storage Utilization: Monitor storage at the virtualization layer, detailing total, free, and used space.	M		
114	Data collectors must store data locally and sync with the server during connectivity issues. This ensures no data is lost and maintains continuous data logging.	M		
115	Here are the communication methods using XML, CORBA, REST API, and SOAP for interacting with external software:	M		
	1. XML: Utilize XML for structured data exchange, ensuring compatibility via defined schemas (XSD/DTD).	M		
	2. CORBA: Implement CORBA for distributed computing, defining interfaces with IDL and using ORBs for heterogeneous system communication.	M		
	3. REST API: Develop RESTful APIs for lightweight and scalable interactions, using HTTP methods (GET, POST, PUT, DELETE) and JSON/XML data formats.	M		

	4. SOAP: Use SOAP for standardized messaging, defining service interfaces with WSDL and leveraging XML for message formatting over HTTP/SMTP.	M		
116	These methods enable diverse and efficient communication with external software systems, tailored to specific interoperability and integration requirements.	M		
117	Ensure all asset information is always synchronized between NMS and NCCM, either by using the same CMDB instance or via real-time synchronization. This guarantees consistent and up-to-date asset data across both systems.	M		
118	Ensure real-time correlation of faults, TCAs, and configuration changes, with immediate generation of root cause alerts.	M		
119	The correlation engine must identify root cause alarms from configuration changes in core or parent devices, affecting unreachable or down child devices.	M		
120	NMS should integrate with NCCM at the module level. Discovery processes should auto-update both systems. Topological connections and historical data should be shared from NMS to NCCM to trigger jobs based on topology changes.	M		
121	The correlation engine should analyze syslogs, flow data, fault data, and performance data to identify root causes.	M		
122	AI and machine learning streamline root cause analysis by correlating data from various sources like logs and configurations. This approach accelerates incident resolution by pinpointing underlying causes swiftly and accurately, even in complex scenarios.	M		
123	Anomaly Detection and Alerting: AI/ML systems monitor IT metrics, network traffic, and logs to swiftly detect and alert on deviations from normal behavior, ensuring prompt issue identification and response.	M		

124	Anomaly detection in performance data should clearly show predicted anomalies on graphs and effectively identify network issues.	M		

3. NCCM

Sl No	Description	Mandatory(M)/ Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	The solution should be GUI based	M		
2	The solution should be web browser-based system for easy access	M		
3	The solution should be OEM agnostic and it should support all market leading OEM network devices irrespective of their Model Et HW/OS Image Version.	M		
4	The solution should be able to Manage 5k plus network devices irrespective of Physical/Virtual/Software Blade i.e. Router, Switches, Firewalls, Load balancer, IPS etc. which are present in the market.	M		
5	The solution should Support SNMPv2, SNMPv3.	M		
6	The solution should Support IPv4 and IPv6.	M		
7	The solution should work on Intel Based platform on physical or Virtual Machines (VMware).	I		
8	The solution should have option to be deployed in HA mode	M		
9	The proposed solutions database version should not be under End-of-Sale and End-of-Support	M		
10	The bidder has to support, plan and perform all upgrade/update of version and patches during the contract period	M		

11	The solution should have internal workflow management for approval process or should be capable of integration with ITSM Ticketing tool. In case of any fault of the network devices, links, servers etc. on the real time basis, the auto ticketing to be triggered to the respective OEM.	M		
12	The solution should have a built in database to store structured data	M		
13	The solution should be able to display all type of jobs with appropriate or specific filters to the roles defined.	M		
14	The solution should have inbuilt version management of configurations with ability to compare two versions, revert to deleted version etc..	M		
15	The solution should have notification to provide alerts and notification using multiple channels with like	M		
	a. SMS	I		
	b. e-mail	M		
16	The solution should provide Notification if Critical job is not going to complete on defined time or Not started / expired within the scheduled time window due to Approval pending	M		
17	The solution should be able to build repository of software images and policies	M		
18	The solution should have audit and re-conciliation capability.	M		
19	The solution should be able to auto-discover network devices across WAN & LAN.	M		

20	During subsequent discoveries, the solution should be able identify and alert whenever any new device added or any device removed	M		
21	The solution should apart from auto-discovery, there should be option add/delete device manually, Through CSV upload and Through REST-API.	M		
22	The solution should be capable to discover device inventory of the devices	M		
23	The solution should have ability to discover Layer 2 and Layer 3 network topology relationships between devices to ensure configuration settings.	M		
24	The solution should network Topology Map should be available with connections and able to filter the maps based on Device IP , Device Group and Device Location	M		
25	The solution should have Device communications protocols support (for example, Telnet, SSH, TFTP, FTP etc.).	M		
26	The solution should be capable of Configuration multiple devices at a time.	M		
27	The solution should In real time, detect configuration and asset information changes, made across a multi-vendor device network, regardless of how each change is made.	M		
28	The solution should capable to detect, compare & alert on changes based on which decision could be made for rollback or implementation of changes with single click.	M		

29	The solution should support rollback to a previous configurations.	M		
30	The solution should maintain at least three previous versions and/or configurations and it should be configurable by users in the UI to extend the number of historical version required	M		
31	The Solution should support configuration deployment/rollback using ad-hoc commands, configuration templates	M		
32	The solution should support multiple commands with multiple parameters at a time for individual location to perform a task. The solution should be able to perform such task in multiple locations at a time.	M		
33	The solution should have the capability to create Multiple command set with hierarchy support (which order to execute) , Based on previous or parent command set result the next command set should execute or ignore, Wait time to start each command set should be provided	M		
34	The solution should have option to define whitelisted / blacklisted command sets for remote CLI sessions to target network devices per user	M		
35	The solution should have multiple options for blacklisted commands including:	M		
	i) Allow user to execute command but send notification to a senior stakeholder / manager	M		

	ii) Block the user from executing the blacklisted command but don't kill the remote session to target network device	M		
	iii) Terminate the remote CLI session when user tries to execute a blacklisted command	M		
36	The solution should provide option to schedule the Backup process.	M		
37	The Solution should have provision to Schedule the Task for specific date, weekly, monthly, and in case of any maintenance window.	M		
38	The solution should be able to track and detect any configuration changes and alert accordingly.	M		
39	The solution should Detect out-of-band configuration changes and trigger a configuration backup. Apply configuration changes to device configurations.	M		
40	The solution should support detecting the change dynamically and trigger the configuration backup in real time to identify the changes and notify the intended user with all the changes listed in the email content itself.	M		
41	The solution should have capability to automate routine network operations.	M		
42	The solution should support to execute the changes and do the provisioning in multiple devices at the same time	M		
43	The solution should have comprehensive Network configuration Back-up and Recovery for all network devices	M		

44	The solution should have capability to deploy and monitor IOS operating system images, network security patches for the supporting devices	M		
45	The solution should have the ability to push standard templates for newly deployed equipment's based on standard predefined policies	M		
46	The solution should have reusable templates for single or bulk changes.	M		
47	The device MUST support replacing current configuration with a new configuration without a reload.	M		
48	The solution should have capability to provision new network devices as per the compliance standard. System should alert policy failing commands before execution	M		
49	The solution should have provision to have approvals for all the jobs and configuration put up in the system	M		
50	The solution should be capable of automatically generate a script from a list of command lines that are input by the user.	M		
51	The solution should ability to upload entire archived configuration files to network devices	M		
52	The solution should allow a failed or success job to be resubmitted "x" number of times.	I		
53	The solution should ensure audit trail of activities being carried out.	M		
54	The solution should be able to load known solutions to the system for the vulnerabilities	M		

55	The solution should have the ability to resolve multiple vulnerabilities in one go.	I		
56	The system should have configuration to set the frequency of vulnerability check	M		
57	The solution should have out of the box policies for basic checks.	M		
58	The solution should allow user to configure multiple types of policies for the different devices in his network	M		
59	The solution should allow regular or specific scheduling of policies defined	M		
60	There should be a approval process of every config and policies being defined or executed.	M		
61	The solution should have capability for different alerts on policy violation to be defined at different levels of severity or urgency (for example, critical, severe or warning)	M		
62	Multiple session from a single account should not allowed	M		
63	The system provides strategic integration with companywide configuration & change processes & having compliance visibility across all network infrastructure components from single dash board.	M		
64	The system has to gather data on compliance to policies as a feedback mechanism to drive improvement &Capable of compliance reporting. Manage network compliance by comparing devices to Custom defined, best-practice standards, Gold Standard	M		

65	The system In real time should store a complete audit trail of configuration changes software made to network devices including critical change information.	M		
66	The system should maintain policy compliance using continuous configuration auditing and remediation.	M		
67	The system should ensure that devices are configured and operating in compliance with regulatory standards.	M		
68	The system should Automate audit cycles with built-in compliance reports and close the loop on compliance with integrated change management	M		
69	The system should be capable of automated remediation to bring devices back to policy compliance or to a default configuration status	M		
70	The system should have mechanism to Intelligently Remediate any Policy Violations.	M		
71	The system should have built in templates of PCIDSS, NIST etc..	M		
72	The system should have capability to configure granular, customizable user roles to control permissions on device views, device actions, and system actions.	M		
73	They should have capability to Manage device access and authorization through a centralized control model that is integrated with standard work flow and approval processes through mail notifications.	M		

74	The system should integration with TACACS, AD for Centralized Group / Role / User Management	M		
75	The solution should also integrate with Vendor Vulnerability Repository or Global Vulnerability Repository (like NIST) to automate the vulnerabilities identification on network devices	M		
76	The solution should integrate with market leading SIEM, SYSLOG tools	I		
77	The solution should integrate with market leading Incident Management a Ticketing	M		
78	The solution should have option to backup the Tool configuration	M		
79	The system should track All Actions According to Group / Role / User levels	M		
80	The system Should have provision to get feeds from OEM with regards to releases (version, patch) and notify	M		
81	The system Should have provision to get EOL / EOS from OEM and notify on expiry	I		
82	There should be a browser based customizable Executive dashboard widget/page showing Device Statistics & their Compliance	M		
83	The system should be able to Schedule and generate Report on all aspects of network device statistics and their compliance	M		
84	The system should be able to Schedule and generate custom report on all aspects of network device configuration & change management	M		

85	The system should have capability to created Reports quickly and brought together when upper management needs help in making important decisions on device upgrades, Compliance verifications.	M		
86	Reports can be retrieved in User friendly formats like Excel, CSV ,PDF	M		
87	All changes logged & generate in Reporting	M		
88	Help with audit compliance by comprehensive documentation and reporting.	M		
89	Archive with recording of activities performed	M		
90	Allow to generate reports to detail	M		
	1.task output analysis	M		
	2.security compliance	M		
	3.operational compliance	M		
	4.configuration differences	M		
	5.How many configuration updates were performed between certain time across all devices	M		
	6. Which operators performed configuration updates on which devices.	M		
	7.The number of unauthorised updates or policies violations detected	M		
91	Have ability to generate Custom dashboard for central monitoring	M		

92	The system should be Able to provide Event Summary Notification i.e. Daily summary notification option, which accumulates all the applicable alert conditions into a single notification, sent once a day. This allows recurring monitoring of alert conditions without the need for event storms or a flood of "too much data" to monitor and review.	M		
93	The Reporting in the system should be Role based	M		
94	The solution should dynamically manage configuration and provisioning, automatically resolving dependencies within templates.	M		
95	The solution should include a REST API for external applications to:	M		
96	The solution should automatically identify device vulnerabilities and offer firmware upgrade capabilities.	M		
97	The solution should suggest remedies for vulnerabilities.	M		
98	The solution should regularly update and monitor vulnerabilities from OEMs for new issues.	M		
99	The solution should regularly backup configuration data in plain text format for accessibility during NCCM tool downtime or disasters.	M		
100	The solution should correlate problem detection, policy violations, and topology relationships to pinpoint network problem root causes effectively.	M		

101	Administrators should view current SSH and Telnet CLI sessions, including commands and responses on all network devices, and perform command searches within these sessions.	M		

4.Log Management

Sl No	Description	Mandatory(M)/ Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1	Log management should cover the log collection from the complete infrastructure like Servers, Network Devices, Firewalls, Virtualization Platforms, Cloud environment, Containers, Web, DB and Security Applications / appliances, User directories etc…	M		
2	System should support the easy way of parsing to support any new vendor, applications even in-house build applications	M		
3	System should be scalable vertically as well as horizontally as per the need. All the components should have scalable option like log collectors, Log store, Presentation layer etc…	M		
4	The log management system should have tight integration with other modules like fault, performance, configuration management etc…	M		
5	All the modules information mentioned above should be available from the common portal	M		
6	Logs should be available as part of the correlation engine along with Fault, Performance TCA to do the higher-level root cause analysis	M		
7	All the received logs should be converted as Alarms based on the rules mapping and follow the common format in the alarms.	M		
8	Also, it should provide option to overwrite the severity from the received logs based on user need and color code accordingly.	I		

9	Should provide the option to view the detailed logs information with all the fields as per received / collected.	M		
10	It should supress the repetitive matched alarms and instead of making the entry again in alarm page it will show the counts	M		
11	User should have option to configure the notification for the converted alarms in multiple format and not limited to email, sms, script execution, whatsapp, slack channels, MS teams channel, telegram, rest api call, push to Rabbit MQ / Active MQ etc…	M		
12	System should support well established pattern matching and comprehensive rule engine to fulfil the requirement to match combination of filtering and various type rules.	M		
13	The simple rule matching will be any fields in the logs should be allowed to make the match pattern and convert as alarms.	M		
14	Should allow to define the list of fields and matching patterns and conditions. Matching patterns and expected values should be one or more and allow to take it from the file. Based on the match condition should provide the flexibility of Blacklisting and whitelisting like match the blacklist will be in alarms condition and does not match the whitelisted also an alarm condition	M		
15	System also should allow the user to define the specific fields in the logs should not be changed for the specific timeline. Like if the user login in one location and location will not be changed for the duration for subsequent logins. Location change within few minutes will be detected as unusual behaviour and raise an alert.	M		
16	System should provide the option to have hold of pattern matched logs for the specific duration and based on the count match of similar logs should raise an alarm.	M		

17	System should raise an alarm for unusual increase in logs as well decrease in logs received from the host level / location level / any group to point the anomaly.	M		
18	Rules should be flexible to detect any new values in the critical fields which never seen before.	M		
19	System must provide the default rules set to cover most the common scenarios required in the market and also flexible enough to configure the new rules set required for policy, compliance and new requirements	M		
20	System should be flexible enough to configure the data retention duration based on the type / host group logs. Based on the storage user can have retention for any longer duration without any limitation.	M		
21	The collected logs should be stored in the archived form for the audit and forensic purpose for the required duration.	M		
22	System should support the extensive search operation for the selected type of log collections. All the fields in the logs should be available as part of the search options and multiple fields selection should be possible with and / or condition to make the search more effective.	M		
23	Log page will be displayed with selective group type of logs and should have flexibility of choosing what the fields to be displayed are.	M		
24	Should provide the option to display all the fields of the logs collected by clicking an icon on the same log display page	M		
25	The solution should support archiving and compression to ensure the reduced storage usage for the longer duration.	M		

26	System should provide the widget-based dashboards and reports. It must provide the default widgets for Servers, Network Devices, Firewalls, Virtualization Platforms, Cloud environment, Containers, Web, DB and Security Applications / appliances, User directories etc…	M		
27	Base modules like Dashboards, Reports, Rules engine, alerting etc… needs to work for any new vendors, applications and in-house build applications seamless without need of any custom development	M		
28	System should provide the options to configure the archival process and schedule also the format on which the historical logs to be kept.	M		
29	It should support the automated archival in desired format and location automatically	M		
30	The solution should allow rule-matched alarms to be converted into ITSM incidents either automatically or manually with a single click, streamlining incident management processes. In case of any fault of the network devices, links, servers etc. on the real time basis, the auto ticketing to be triggered to the respective OEM.	M		
31	The solution should allow creation of any number of widgets in graphical, textual, detailed, or summary formats, offering flexibility to meet specific operational needs.	M		

5.Hardware Specifications:

Sr. No	Description	Mandatory(M)/ Important (I)	Complied (Yes/No)	If No, Bidder's Remarks
1.	Software vendor must certify the HCI platform and hardware. Bidder should submit certification for the same from the corresponding software OEM.	M		
2.	The Hyperconverged	I		

	Infrastructure (HCI) appliance should have seamless integration of Compute, Storage, Networking, Security, Virtualization and Management functionalities within a single appliance.			
3.	The HCI appliance should have an integrated web management interface for overseeing the entire life cycle of Virtual Machines, encompassing Creation, Updating, Deletion, Backup, Point-in-time Snapshot, Cloning, Templates, Migration, Monitoring, VM Console access, HCI Health Metric Visualization and Security Management.	I		
4.	The Web Management interface should have graphical visibility into hardware resource utilization (including CPU, RAM and network) at both the server and virtual machine levels. At a minimum, the graphs should display real-time, 5-minute, hourly, daily, weekly, monthly, and overall details of the aforementioned parameters.	I		
5.	HCI solution shall have automated High Availability capabilities for the virtual machines without dependency on external server/VM. In case one server/Node fails all the Virtual machines running on that server shall be able to migrate to another physical server running same Hypervisor.	I		
6.	The Proposed solution shall support future addition of nodes with different CPU models and memory capacity/configuration in the same cluster.	M		
7.	Hyper Converged platform should support scalability in terms of adding additional server nodes without any downtime to business	I		

	services.			
8.	HCI solution should support Active directory and LDAP servers integration.	I		
9.	HCI solution should support Virtual Machines of commonly available Operating Systems like Windows, Linux with 64 bit and 32 bit architecture.	I		
10.	Proposed HCI solution should be supplied with AHV/vSphere/Stacbloc hypervisor. Bidder should quote with perpetual license for the hypervisor. Bidder should submit declaration from the Hypervisor OEM that the quoted license is perpetual.	M		
11.	HCI solution should support creation of unlimited workloads (VM's). The only limitation should be the underlying hardware resource.	I		
12.	HCI platform should support minimum 32 nodes in the cluster.	M		
13.	HCI solution should have built-in backup solution for virtual workloads. The backup solution should support live mode backup, suspend mode back and stop mode backup for virtual machines.	M		
14.	HCI solution should have built-in Software Defined Storage services. SDS should have capability to create multiple tiers of virtualized storage. SDS should support RF2 and RF3 from day-1.	M		
15.	HCI solution should have ability to configure multiple storage backends like Software Defined Storage Cluster, iSCSI interfaces, File services interfaces for NFS, SMB. The Storage backend should support industry standard VM disk types viz., VMDK, QCOW2, RAW.	M		

16.	Proposed HCI solution should have file sharing services. File sharing services should provide File Services supporting Windows (CIFS / SMB), FTP and Linux systems (NFS). File sharing services should not have storage capacity limitation. File sharing services should provide mechanism for CIFS/SMB and NFS shares to allow/deny the users based on the IP address for Storage service access.	M		
17.	HCI platform should support infrastructure automation and self-service operations as mentioned below: Create virtual machine Stop virtual machine Delete virtual machine Performing clone, backup, snapshot operations.	M		
18.	HCI platform should support application automation and life cycle management. It should support following activities on VMs with Windows and Linux operating systems: Application installation, Starting application, Stopping application, Removing application and corresponding VMs. Data collections: Collecting installed application list from VMs.	M		
19.	HCI solution should have capability to implement following Security Guidelines of Indian Computer Emergency Response Team (CERT-In) for the virtual machine operating system, application and database in an automated way. OS hardening for Windows and Linux Web Server Security Database Server Security	M		

20.	HCI Automation solution shall have built in security modules to enable hosts comply to standards and industry benchmarks - CIS. Should provide support for Windows & Linux operating system flavors.	M		
21.	HCI solution should provide VM OS Health management services like memory clearing, swap space, dentries, inodes, page cache preventing potential failures. These services should be performed in an automated way.	M		
22.	HCI solution should create local repositories for VM operating system (OS) images and application packages.	M		
23.	Deployment support: The proposed HCI solution should be able to support a single node deployment in standalone mode, with multiple data replica copies for staging environment. HCI Solution should be able to deploy and support 2 Node cluster with automated High Availability (HA) without any external support for production workloads.	M		
24.	HCI solution should be factory pre-integrated with HCI software and appliance. Entire HCI solution should be from single OEM and that OEM shall take responsibility of warranty and support for HCI platform and hardware. The bidder should submit declaration from OEM stating the same.	M		
25.	The HCI OEM must conduct necessary proactive health checks for the HCI solution. During the warranty period, the HCI OEM is required to perform a proactive health check each quarter and submit the health check report within 15 days on the HCI OEM's	M		

	letterhead. The bidder should submit declaration from OEM stating the same.			
26.	The HCI appliance must be certified by the Bureau of Indian Standards (BIS), with the BIS certificate issued in the name of the HCI OEM. The bidder should submit BIS certificate from the OEM.	M		
27.	Perpetual License to be provided for the entire HCI environment. However, time to time updates, patches and upgrades should be provided without any additional cost during the warranty period.	M		
28.	All the components of HCI appliance like HCI management layer, Hypervisor, hardware and all HCI features should be from the same OEM, factory installed for better compatibility and ready for fast deployment. HCI OEM has to provide Make in India declaration on their letter head stating their local content percentage. Bidder has to submit MAF from HCI OEM. If bidder is a OEM, self declaration certificate with tender reference number to be submitted.	M		
29.	The HCI OEM should provide 5 years comprehensive warranty and onsite support for the complete HCI solution & add on components.	I		
30.	Bidder has to size the HCI hardware specifications based on the software requirements. Total two sites - DC & DR. HCI solution should be designed with minimum 3 HCI nodes at each site (total minimum 6 nodes). In each site it should be deployed in 2+1 mode or higher (2	I		

	production nodes and 1 failover node). DC and DR should have same Hardware configuration. Minimum hardware specification for each HCI node: 2 x 28 Core, HT, Intel Xeon scalable processor or latest or equivalent, Dual socket server motherboard, 384 GB ECC Memory or higher, 2 x 480 GB Enterprise flash disks with RAID-1 using 1gb cache or higher hardware raid controller for Hypervisor, 3 x 7.68 TB Enterprise flash disks for virtual machines data, 6 x 10Gbps RJ45 ports, 1 x 1G RJ45 port for management, Dual (Redundant) Power Supply, 2U rack with 8 bay hot swappable bays and rack mounting kit.			
31.	HCI solution should be supplied with two numbers of layer-2 or above network switches per site, total four switches. Each switch should have minimum 24 numbers of 10G ports. Bidder should provide all required patch cables, DAC cables and modules.	I		
32.	Proposed HCI solution should be a matured and production ready HCI solution. The HCI OEM should be operating in the Indian Market for a minimum of 9+ years and should have deployed minimum 100 HCI nodes in State/Central Government/PSU organizations in India. OEM certificate of incorporation and PO copies, invoice copies with self declaration to be submitted.	M		

GENERAL SCOPE OF WORK

Sl No	Description	Acceptable (Yes/No)	If No, Bidder's Remarks
1	Bidder has to supply and install the Hardware & Software along with required licences at Banks Data Centre locations. Bidder has to take back-to-back OEM support for All software, licenses etc. Bidder also have to share the list of Bill of Materials for technical evaluation. Implementation will be done for all necessary Hardware Software License and Cabling.		
2	Bidder has to plan, design, integrate, implement, roll out, manage and migrate the all solutions for the contracted period.		
3	Bidder has to document the detailed solution architecture, design, traffic flow etc. System Integrator (SI) after consulting with the Bank team should finalize the solution/architecture by understanding Bank's existing architecture and also on the basis of that provide a solution for integration/implementation of all solutions.		
4	Bidder has to own the responsibility of making the solution run as desired by the bank		
5	Bidder shall ensure that during the various phases of implementation, the performance, security etc of the existing network setup is not compromised.		
6	If some components are missed out or not properly sized, onus is on the bidder to supply and replace it without any cost to bank however appropriate penalty will be levied by the bank.		
7	In case of need, the bidder has to integrate the software with AD, NTP server, TACACS, VAS tool, and any other new API /tool deployed in Banks environment which can be integrated with the proposed solution without any additional cost and solution requirement considering the 5 years period of contract.		
8	All necessary entitlements, papers of license for software should be provided to bank		
9	Support should be provided for 24*7*365.		
10	The bidder has to design, lay and test the solution to cater to the requirements. The solution has to be deployed at DC &DR locations for the bank & any other locations as decided by the Bank		

11	The bidder has to submit project and support escalation matrices and keep bank informed, if any changes take place.		
12	Design and implementation have to be done by the SI and reviewed by the OEM and seamless integration should be carried out. (If needed onsite for OEM)		
13	All product updates upgrades & patches should be provided by the selected bidder free of cost during the warranty period and it should be updated then and there to enforce the security compliance.		
14	Bidder should inform Bank about all release/ version change of patches /upgrades/update of software/OS/ middleware etc. as and when released by the successful bidder		
15	For the network establishment, central place at DC, Bangalore and DRC place at Mumbai. For log management establishment, DC as well as DR will act as an independent management.		
16	The bidder is required to participate and comply with various audits regulatory requirements and certifications conducted by bank, RBI, NABARD, Sponsor Bank and various legal entity and other agencies.		
17	Bidder has to provide hands on OEM training to 10 people in 2 batches of identified bank officials which should cover in depth operational and troubleshooting features of the solutions. The training should be held in Bengaluru. Bidder has to provide user manual and technical documentation both in hard copy and soft copy to bank.		
18	Bidder should keep the bank explicitly informed about the end of support dates on hardware and software and related products and should ensure support during warranty period. Wherever possible extended support should be provided for the solutions/deliverables supplied.		
19	Bidder has to prepare and supply the standard configuration/ back-ups/compliance/reporting etc. template as per Bank's requirement		

20	The successful bidder has to ensure the availability of resident engineers at Project Office, Bengaluru and DC & DR locations for 3 years from the date of acceptance of the solutions as per RFP clause on all working days as well as beyond office hours or on holidays, if required. L2 Resident engineer/s must have relevant solution certification and working experience of at least four years. The L1 Resident engineer/s must have working experience of at least two years. Certificate from that organisation to be submitted as a proof of experiences while On boarding. The onsite resource support should be available 24*7*365. The dress code will be formal for the onsite support personnel on all days. If bank requires onsite support personnel to be available on holidays or extra hours at no cost to the bank. All infrastructure required for the support personnel like desktop PC email etc. shall be provided by bank.		
21	The successful bidder (SB) will ensure onsite availability of experience engineers in case of any urgent requirement of bank in addition to the existing onsite resident engineer without any extra cost to the bank, till the time the issue is resolved or the bank feels so.		
22	The resident engineer stationed at banks Project office will be exclusively for the project and cannot be shared by the bidder for any other purpose. Granting leave/absence to the engineer posted at our site, should be prior intimation to the bank and suitable replacement should be arranged in his/her absence without fail.		
23	Selected Bidder (SB) has to provide substitute support personnel in case posted support personnel remains absent or on leave. Holidays of support personnel shall be governed as per Bank's holidays. In case no substitute provided for the absent period or report not provided for any working day then a penalty of 200% of the proportionate per day rate will be levied. It is the responsibility of the SB to monitor the actions/performances of the onsite support personnel. The penalty shall be deducted from any of the amount payable to the successful bidder.		

24	Bank reserves it right to engage/disengage the service of the resident support personnel by giving one month notice to the successful bidder.		
25	The proposed NCCM Solution should cover all the existing network devices as well as the proposed SD-Wan routers		
26	**RESPONSIBILITY FOR FAULT FREE OPERATION**		
26.1	The Successful Bidder (SB), following the execution of the Contract, will assume total responsibility for the fault free operation of solution during contract period (Comprehensive Onsite Warranty & AMC period).		
26.2	The successful bidder has to guarantee a minimum uptime of 99.90% on monthly basis for the total solution (including hardware, software and other components) during the warranty and AMC period. (Any planned shutdown will not be considered for calculating SLA).		
26.3	In case the bidder fails to meet the agreed uptime as mentioned above, penalty shall be levied as mentioned in the RFP.		
26.4	The amount of penalty will be recovered from the vendor from any payment to be made to them as per clauses mentioned in the RFP.		
26.5	During comprehensive on-site warranty/ comprehensive annual maintenance contract of the solution, the bidder will accomplish preventive and breakdown maintenance every quarter for the Solutions at DC and DRC, to ensure that all hardware functions without defect or interruption. Prior clearance from the Bank should be obtained and records for having done the preventive maintenance have to be furnished to Network Team, Project Office, Bengaluru.		
26.6	The Bank will normally approach successful bidder, for any problem relating to the products supplied under this purchase order. The Bank however reserves its right to take up directly with the Original Equipment Manufacturer of products supplied under this purchase order and this condition shall be incorporated by successful bidder, in their contract / agreement with the Original Equipment Manufacturer.		
27	**ONSITE SUPPORT ENGINEER'S ROLE**		

27.1	The devices has to be configured & hardened as per requirement of Bank.		
27.2	Support Engineer shall provide support for configuration of device as and when needed by BANK		
27.3	Overall management and monitoring of the solution, including the H/W, S/W and application health and utilisations.		
27.4	Maintain the inventory of all IP Address along with present location, the port numbers used for connectivity, MAC		
27.5	Addition/ Deletion/ Modifications in configuration/ rule sets/ user policies as per bank's requirement.		
27.6	Applying regular updates/ upgrades/ patches/ fixes etc.		
27.7	Keep back up of log, configuration, data etc.		
27.8	Prepare and submit regular reports as required by the bank.		
27.9	Call log, follow up and escalation for resolution of all types of h/w or application issue for the solution.		
27.10	Promptly alert bank's team in case of any discrepancy observed or any security threat and initiate necessary action		
27.11	Engineer should do any configuration changes requested by bank.		
27.12	Engineer should take care of configuration change and roll back as per bank person request.		
27.13	Engineer should do the solution fail over testing on critical devices during preventive maintenance period.		
27.14	Engineer should take back up for all network and security devices on daily basis.		
27.15	Engineer should be capable of creating any new configuration/ configuration template/job/tasks etc as and when required by Bank		
27.16	Engineer should do the DC/DR/Branch devices hardening configuration changes as per banks network		
27.17	Engineer should do the syncing of DC & DR supplied servers.		
27.18	Engineer should monitor the solution intimate banks on any compliance breach & rectify based on bank team request as and when required.		

27.19	Engineer should share compliance report on monthly basis.		
27.20	Engineer should inform banks team in case of any alert /error observed in any device configuration and act accordingly to solve the issue.		
27.21	Engineer has to do the failover testing of critical devices as per bank team's request.		
27.22	Engineer has to ensure that all backups are happening correctly and need to maintain and submit the checklist on monthly basis		
27.23	Engineer has to prepare and submit day to day activity report on monthly basis.		
27.24	Engineer has to do the periodic discovery of all the network devices & share the list of noncompliance devices and do the required changes to make it compliant only after bank's team permission.		
27.25	The engineer has to conduct planned and unplanned DR Drill activity as and when required by the bank and submit the appropriate reports to the Bank.		

Authorized Signatory Name and Designation Office Seal

Place:
Date: