Technical Specification – 2 _Enterprise Network management system (NMS)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
	General Requirement				
1.	The Solution must support ITIL Version 4 and above framework including terms and definitions. Solution must have the capability to upgrade to ITIL Version 4 and above.	M			
2.	The Solution must have a process driven workflow which will incorporate routing of request, setup of service desk, service level agreement (SLA) management, electronic request approvals by actionable e-mail, SMS alerts etc.	M			
3.	The Solution should support a web-based client for user and administrative functions with auto sign-off facility after a predefined idle time.	M			
4.	The Solution shall have the capability to adapt and maintain custom workflows as per LIC-defined processes	M			
5.	The Solution should support mobility devices to allow for role-based views that can be accessed while away from the office.	M			
6.	The Solution should be able to configure the graphical using drag and drop for all fields	M			
7.	Product should be able to import user data from LDAP, AD or from other 3rd party systems identity management system. It should also have option to manually upload user data.	M			
8.	The Solution should be able to enable rapid creation of new users and administration of existing users.	M			
9.	The proposed Solution must have option to define announcements for notifying end users / requesters about any important information with option to schedule it for certain time period	NM			
10.	The proposed Solution should allow the admin user to create custom work streams for the user interface & can hide, show, edit, or delete these custom work streams.	NM			
11.	The Solution must be compatible with various Server and network types, including but not limited to leased lines, MPLS, VPN, and SDN, SDWAN, etc.	M			
12.	The Solution should be compatible with a wide range of protocols and interfaces for third-party integration, including REST APIs/ SOAP/ PowerShell / SQL / FTP, SFTP / SSH and other standard methods.	M			
13.	The Solution should support API integrations to enable seamless data exchange with third-party Solutions like SIEM, IAM, ERP, monitoring platforms, etc.	M			
14.	Must allow secure API access with role-based control, supporting OAuth2, API keys, MFA and token-based authentication.	M			
15.	The solution should provide ability to support 3rd party integration and have open API/interfaces for integration.	M			
16.	The solution should provide ability to correlate events across the spectrum of infrastructure components and should support events from components including Network, hardware, multiple-platform servers, database, etc.	M			
17.	The Solution should support multi-level administrative delegation by enabling the creation of distinct administrative domains. Each administrator should be assigned specific roles and resources, ensuring accountability within their defined scope of responsibility.	M			

Technical Specification – 2 _Enterprise Network management system (NMS)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
18.	The solution should provide ability to generate web based real-time reporting and historical reporting of elements in the infrastructure, providing the ability to format and present data in a graphical and tabular display.	M			
19.	The solution should provide the ability of integrating events to automatically create trouble tickets in Service desk system for in-time problem resolution for supported service desk tool	M			
20.	Ability to perform event correlation, sending alerts to administrators, real-time and historical analysis with trend and ad-hoc reporting.	M			
21.	The solution should support all types of networks like Leased lines, MPLS, VPN, SDN etc.	M			
22.	Solution should include pre-built connectors and API for faster integration and automation enablement.	M			
23.	The Solution should support multi tenancy by segregating data, users, and workflows logically within the same platform.	M			
24.	Support flow path visualization from source to destination including intermediate hops.	M			
25.	The Solution should provide modular and should not be framework dependent so that required modules can be added in the future to meet growing/changing needs.	M			
26.	All AIOps functions including anomaly detection, trend forecasting, and correlation should extend beyond infrastructure elements to business service-level insights for proactive service management.	M			
27.	The system should offer a centralized monitoring console, displaying events across the environment with GUI-based colour indicators based on severity levels.	M			
28.	The Solution should provide ability to correlate events across the spectrum of infrastructure components and should support events from different OEM's.	M			
29.	The solution should have the ability to integrate with the LIC existing and upcoming system and application.	M			
	Network Management System				
30.	The deployed NM Solution should be an enterprise grade and support monitoring of 15000 network devices.	M			
31.	The Proposed Network Management system consoles must provide web-based topology map view from a single central console. The system should provide Auto Discovery & inventory of heterogeneous physical SNMP enabled network devices like switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level.	M			
32.	Network Management Solution should support Graphical User Interface (GUI).	M			
33.	The solution should allow for discovery to be run on a continuous basis, which tracks dynamic changes near real-time to keep the topology as up to date as possible. This discovery should run at a low overhead, incrementally discovering devices and interfaces.	M			
34.	The NMS should provide very powerful event correlation engine and thus must filter, correlate & process, the events that are created daily from network devices. It	M			

Technical Specification – 2 _Enterprise Network management system (NMS)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
	should find the root cause and provide relevant console messages.				
35.	Polling intervals should be configurable on a need basis through a GUI tool, to ensure that key systems are monitored as frequently as necessary.	M			
36.	The topology of the entire Network should be available in a single map along with a Network state poller with customizable polling intervals.	M			
37.	The Network performance operator console should provide operators with seamless transitions from fault data to performance reports and back. For example - select a node in NMS fault mgmt. system and cross launch it for historical and near real time data in performance Management.	M			
38.	Should have MIB browsing, MIB loading/ MIB expression collection features.	M			
39.	The proposed system must support multiple types of discovery like IP range discovery - including built-in support for IPv6, Import data - from pre-formatted files (IPs, ranges, strings or ports), Seed router based discovery - Using route tables and SNMP MIBs, Trap-Based Discovery - whenever new devices are added with capability to exclude specific devices based on IP addresses / IP Address range.	M			
40.	The system must deduce the root cause of the problem and in topology it should visually pinpoint single impacting device as well as other impacted devices through various colors.	M			
41.	Proposed Solution must provide Spotlight views for Router Redundancy, VLAN list. When clicked on a particular VLAN from VLAN List, participating devices only for that particular VLAN gets highlighted in the topology map.	NM			
42.	The proposed system should be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements like Capture and detect running & startup configuration, Upload configuration, Write startup configuration.	M			
43.	The proposed tool should display configuration changes differences in GUI showing modified, remove, masked lined from last captured network configurations for routers and switches. Also, this should be able to identify which user has made changes or modifications to device configurations.	M			
44.	Network Management Solution should depict changes when the link is Up and down	M			
45.	The System should be able to monitor Quality of Service (QoS) parameters configured to provide traffic classification and prioritization for reliable traffic transport. The solution should be able to discover, and model configured QoS classes, policies and behaviors.	M			
46.	The system should provide an outage summary that gives a high-level health indication for each device as well as the details and root cause of any outage.	M			
47.	Support for discovering and monitoring router redundancy groups using HSRP (Hot Standby Router Protocol) & VRRP (Virtual Router Redundancy Protocol).	M			

Technical Specification – 2 _Enterprise Network management system (NMS)					
#	**Category/Modules**	**Mandatory (M) / Non-Mandatory (NM)**	**Compliance (Yes / No)**	**Evidence**	**Remarks**
48.	Support for discovering and monitoring router redundancy groups using HSRP (Hot Standby Router Protocol) & VRRP (Virtual Router Redundancy Protocol) & recognizing situations that can result in multi-path conditions.	NM			
49.	Should be able to generate a graphical representation of the network. Identify which devices are inactive or out of compliance. Use filters to immediately view isolated specific network segments. Capture a snapshot of the current state of the network, including topology and virtual LAN (VLAN) information. Identify the hosts connected to specific switches or interfaces by MAC and IP address and host name.	M			
50.	Manage network compliance by comparing devices to defined, best- practice standards. The Defined best practice standards should be user defined.	M			
51.	In real time, detect configuration and asset information changes made across a multi-vendor device network, regardless of how each change is made and also support configuration deployment/rollback and configuration templates.	M			
52.	Manage dual-stack IPv4/IPv6 environments.	M			
53.	In real time, store a complete audit trail of configuration changes, made to network devices, including critical change information.	M			
54.	Configure granular, customizable user role based access control permissions on device views, device actions, and system actions.	M			
55.	Deploy and monitor IOS operating system images from a centralized network management system.	M			
56.	Proposed performance management should integrate with fault management to forward performance exception alarms by defining notified rules.	M			
57.	Should establish the status of network devices and interfaces with unified status calculation and visualization of network fault & performance data.	M			
58.	The proposed system shall identify over-and under-utilized links and assist in maximizing the utilization of current resources. The proposed system shall provide Performance of Network devices like CPU, memory & buffers etc., LAN and WAN interfaces & network segments and links.	M			
59.	Should enable efficient workflows using contextual navigation between reports and rich interactive report configuration capabilities.	M			
60.	The infrastructure fault management solution alerts should integrate with the inscope and existing Enterprise ITSM & ITOM solutions	M			
61.	The solutions should have very high-scale monitoring architecture on a platform that scales efficiently. Solutions should support Linux environment for scalability.	M			
62.	The solution should provide capability to monitor any device based on SNMP v1, v2c , v3 and more	M			
63.	The solution must be capable of monitoring the availability, health, and performance of all networking devices including but not limited to CPU, memory, temperature, interface bandwidth utilization. The solution should generate alerts on breach of threshold	M			

Technical Specification – 2 _Enterprise Network management system (NMS)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
	such as CPU utilization, memory utilization, drops, interfaces errors, reliability errors, temperature, Bandwidth utilization, etc.				
64.	The solution should have the ability to check on availability of ports, devices.	M			
65.	The system should be able to identify and alert in case any changes to NAC configuration is made.	M			
66.	The solution should automatically collect and store historical data so users can view and understand network performance trends.	M			
67.	The solution should provide the ability to “baseline” performance metrics and determine normal operating values and patterns based on time of day, week etc. The ability to threshold on these values should be available.	M			
68.	The solution should support auto-discovery of network devices	M			
69.	The solution should have the capability to provide end-to-end visibility for the network faults. E.g. : If the user unable to open an application, the solution should able to map entire network path from his endpoint to the application and pin-point the hop on which the problem is occurring (this is different from trace route)	NM	.		
70.	The solution should provide discovery of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices.	M			
71.	The solution must allow administrators to create own custom metrics and certify new devices for monitoring. It should also allow configuration of the device properties via an API.	M			
72.	The solution should provide bi-directional integration between the Fault & Performance management solution, the devices discovered in Fault Mgmt. product should be synchronized in Performance management solution.	M			
73.	The solution should provide functionality to create threshold profiles based on multiple rules for different metrics and should be able to apply these threshold profiles on group of devices.	M			
74.	Discovery profile should have option to prioritize naming order like hostname, sysName, IP address.	M			
75.	Should be able to generate reports based on business working hours and Non business Hours for the selected time frame.	M			
76.	The solution must provide the following Flow-based metrics for network flow analysis: • Rate • Utilization • Byte Count • Flow Count • IP hosts with automatic DNS resolution • IP conversation pairs with automatic DNS resolution • Router/interface with automatic SNMP name resolution • Protocol breakdown by host, link, ToS or conversation.	M			

Technical Specification – 2 _Enterprise Network management system (NMS)					
#	**Category/Modules**	**Mandatory (M) / Non-Mandatory (NM)**	**Compliance (Yes / No)**	**Evidence**	**Remarks**
	• Utilization by bit pattern matching of the TCP ToS field.				
77.	The solution must provide the following Flow-based metrics for network flow analysis: • Rate • Utilization • Byte Count • Flow Count • IP hosts with automatic DNS resolution • IP conversation pairs with automatic DNS resolution • Router/interface with automatic SNMP name resolution • Protocol breakdown by host, link, ToS or conversation. • Utilization by bit pattern matching of the TCP ToS field. • AS number BGP next hop address	NM			
78.	The solution must be capable of providing the following detailed analysis: • Top protocols by volume based on utilization of every link being monitored by every collection device • Top utilized links (inbound and outbound) based on utilization of every link being monitored by every collection device. • It must support geo-diverse deployment.	M			
79.	The solution must allow date range selection for the reporting period. The solution must also allow the defined custom reports to be saved indefinitely for future use. All reports should be generated and displayed directly by the solution from a common interface.	M			
80.	The solution must be able to restrict views for defined users to specific routers, interfaces, and reports.	M			
81.	Solution shall have provision for feed to NOC.	M			
82.	Must provide reports and logs for Audit Trails.	M			
83.	The solution should be able to push configuration centrally on all network devices. Multiple instances of pushing of configuration simultaneously should be provided.	M			
84.	The solution should, before pushing the configuration conduct a pre configuration check and alert in-case the configuration that going to be pushed will disrupt the network.	NM			
85.	Complete visibility across the entire network, including all devices, interfaces, and traffic flows, from a single console.	M			
86.	Ability to push and manage network device configurations remotely to ensure consistency and reduce configuration errors.	M			

Technical Specification – 2 _Enterprise Network management system (NMS)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
87.	Detailed information about IPs, MAC addresses, switch ports, and other critical network data for effective network management and troubleshooting.	M			
88.	Easy composible dashboards with pre-defined templates for Node Performance View, Interface Performance View, or Incident Performance View for quick visualization and troubleshooting. Should support UDT (User Defined Template) with widgets for comparing metrics By Type, By Field Group, By Relation, Top N, Bottom N.	M			
89.	NMS should provide integrated discovery, fault, and performance monitoring, configuration & compliance management together in one Solution.	M			
90.	Solution should adhere to Micro services and thus be built on modern container technologies (like Docker, Kubernetes) mode. The solution should either support built-in Kubernetes technology or Bring Your Own Kubernetes (BYOK, CNCF certified) platform provided by the bidder	NM			
91.	Web hook integration support for sending incident events (eg. From 3rd party source or System) as they occur instead of polling. Also support for update incident event attributes such as category, family or even custom attributes.	M			
92.	Ability to configure network tests from server to other IP device for troubleshooting common problems such as - site reachability, downloads taking lot of time or is interrupted, network latency to cloud VM	M			
93.	Configure and monitor network tests for network troubleshooting for all protocols such as, but not limited to - ICMP, UDP, UDPECHO, TCP, DNS, HTTP(s), ORACLE, DHCP.	M			
94.	Solution must be FIPS 140-2 compliant, which ensures that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data.	NM			
95.	Proposed NMS solution should be able to provide Visibility into all aspects of site-site SD-WAN such as, but not limited to, underlay connectivity using deep SD-WAN Overlay monitoring (Tunnel and Tunnel Endpoints) as well as underlay monitoring from a single console for incidents, status & performance reporting.	M			
96.	Proposed NMS solution must discover and monitor not only SDN underlay objects such as Leaf, Spine, and APIC along with APIC cluster; but also all overlay objects such as, but not limited to Tenant, Bridge Domain, End Point Group, VRF, and VXLAN, for synchronization & flexibility to generate variety of reports.	M			
97.	Proposed NMS solution must provide by default deep firewall monitoring by discovering and monitoring of site-to-site VPN tunnels. It also collects data for the firewall connection metrics and allows to set the threshold for the number of connections dropped and the number of active connections and get an alert when it violates the threshold.	M			
98.	Proposed NMS solution must support Network Telemetry collector-based monitoring of Network infra.	M			
99.	Solution should minimize maintenance and administrative tasks by sharing a single inventory database for tasks of monitoring of inventory, faults, performance, flow and configuration. Administrators and	M			

Technical Specification – 2 _Enterprise Network management system (NMS)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
	power users should not be required to populate multiple databases and keep them in sync.				
100.	Solution should manage network devices that can be discovered by IP address, link level address, or devices that run IP. System should take up the fault detection & health monitoring of various network elements from the device level to the protocol and interface levels.	M			
101.	Solution should provide network performance data & threshold-based alerts for real time performance monitoring, Service Level monitoring, reporting and historical trending.	M			
102.	At the lowest level, network communication should be done through TCP/IP, SNMP and API. System should process and obtain, automatically, meaningful information such as network discovery and layout of the Network and event handling.	M			
103.	Solution should be able to support mapping and modelling of the infrastructure grouped by network connectivity, physical location of equipment and user groups or departments.	M			
104.	Topology maps should display links utilization status and be able to define custom utilization bands through the UI.	M			
105.	Solution should provide information regarding capacity utilization and error statistics for WAN links.	M			
106.	Solution should allow to reduce the set of displayed devices in the topology views by flexible rules, based on the attribute contents stored with each device.	M			
107.	Solution should be able to support migration to SNMP v3 and/ or latest version to provide added security.	M			
108.	Solution should provide user-configurable discovery control to manage the frequency and scope network discovery, configured using a graphical user interface.	M			
109.	Solution should allow to take configuration snapshots directly from CLI and, SCP, TFTP and SFTP	M			
110.	Solution should allow to monitor devices for configuration changes and auto-backup configuration.	M			
111.	Solution should have customized Dashboards to provide auto-updated, visual representation of the networks status and performance based on the selected view or object, and report on multiple different metrics and, include facilities to fine tune dashboards that suite NOC and higher management use cases.	M			
112.	The system should be able to clearly identify configuration changes / policy violations / inventory changes across multi-Bidder network Solution.	M			
113.	Deep automation-oriented insights to capture and visualize the value of automations in network space. Provide analysis for tasks such as OS Upgrades, Provisioning, Remediation, Diagnostics, Audit Policy Check and Compliance Reporting.	NM			
114.	The proposed solution shall incorporate an advanced add-on module that delivers detailed, hop-by-hop visibility into network traffic paths.	M			
115.	Events should be presented in multiple visual formats like tables, tree structures, service views, and heat maps, allowing users to customize how they group and view data.	M			

Technical Specification – 2 _Enterprise Network management system (NMS)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
116.	The Solution should provide advanced filtering capabilities to eliminate unnecessary alarms and present relevant data cleanly within the web and GUI interfaces.	M			
117.	Supports auto-ticketing based on alerts from link failures (protocol or physical), performance anomalies (latency, jitter, packet loss), and threshold breaches. Integrates with SD-WAN controllers, WLAN controllers, wireless devices, and other network elements for real-time event detection and incident creation.	M			
118.	Auto-ticketing must be enabled for events such as interface/link down, high latency, jitter, or packet loss as reported by network monitoring Solutions or SD-WAN controllers.	M			
119.	The system should automatically generate incident tickets for interface up/down events, link flaps, high utilization, or tunnel health degradation from SD-WAN controllers.	M			
120.	Auto-ticketing must be triggered for link failures based on protocol or physical disconnection.	M			
121.	Raise incidents on pool member failure, high response latency, or VIP unreachability.				
122.	Push notifications and alerts for incidents with action buttons for escalation or assignment.	M			
123.	Trigger events and incidents from SNMP traps received from network devices.	M			
124.	Trigger alerts when CPU thresholds are exceeded for a sustained period.	M			
125.	Incidents must be auto-created for non-reachable IPs detected via ICMP probe failures.	M			
126.	Trigger incidents when memory breach crosses defined thresholds.	M			
127.	Include guided troubleshooting steps for incident handlers.	M			
128.	Generate alerts for duplicate MAC detection or spoofed MAC addresses.	M			
129.	Correlate forensic data with incidents for breach analysis and RCA.	M			
130.	The solution should provide alert, in case of failure of overlay from a location. It should also provide alert if an alternative overlay is being used to reach its destination.	NM			
131.	Interface down or flapping status should auto-trigger incident tickets with relevant metadata.	M			
132.	System should automatically generate incident tickets for interface up/down events, link flaps, and tunnel degradation.	M			
133.	Auto-ticketing must be enabled for SD-WAN events such as tunnel instability and path failover.	NM			
134.	Incidents must be auto-generated for ACI fabric faults and degraded components.	M			
135.	The proposed Fault Management Solution must support integration with proposed help desk or trouble ticketing system such that integration should Associates alarms with Service Desk tickets in the following ways: a) Manually creates tickets when requested by Fault Management GUI operators.	M			

Technical Specification – 2 _Enterprise Network management system (NMS)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
	b) Automatically creates tickets based on alarm type. c) Provides a link to directly launch a Service Desk view of a particular ticket created by alarm from within the Network Operation console. d) Maintains the consistency of the following information that is shared between alarm and its associated Service Desk ticket including status of alarms and associated tickets and current assignee assigned to tickets.				
136.	Alerts from SD-WAN controllers must be correlated and de-duplicated before triggering events or tickets.	NM			
137.	The Solution should provide ability to provide an event console for the entire environment for event monitoring. Events should be colour coded on the GUI based on severity.	M			
138.	Raise alerts on memory usage breach or abnormal consumption spikes.	M			
139.	The system should support ingestion of raw flow data in formats such as IPFIX, NetFlow v9/v10, JFlow, NetStream, etc from a wide range of devices including routers, switches, firewalls, load balancers, NGFWs, and capable endpoints.	M			
140.	It should support in-depth bandwidth utilization analysis by providing interface-specific reports showing user, source and destination IP, application types (HTTP, HTTPS, SFTP, TCP/UDP), and overhead data, with drill-down capabilities to identify end-host usage patterns.	M			
141.	The system should generate detailed traffic flow reports showing top users, applications, protocols, location, AS numbers, top routers, and interfaces consuming the most bandwidth, along with context-aware insights for each dimension.	NM			
142.	Flow-based traffic analysis should enable congestion and trend insights by key dimensions such as source/destination IP, protocol type, source/destination port, and routing interface.	M			
143.	The Solution should allow customizable flow sampling intervals ranging from 1 minutes to 1 hour, and correlate NetFlow data with interface utilization to enhance capacity planning accuracy.	M			
144.	It should allow mapping of application names to specific IP and port combinations, ensuring easier identification in all reports and dashboards.	NM			
145.	Must monitor utilization trends across WAN links, firewall throughput, load balancer capacity, and SD-WAN.	M			
146.	The system should analyze historical link usage, tunnel bandwidth, and interface statistics to forecast potential bottlenecks.	M			
147.	It must identify traffic spikes at load balancers or firewalls that may affect service performance and recommend resource allocation based on trends.	M			
148.	Must provide historical usage trends and forecast saturation of WAN and LAN links.	M			
149.	Traffic flows should be analyzed using NetFlow/IPFIX to identify top users, apps, and peak times.	M			

Technical Specification – 2 _Enterprise Network management system (NMS)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
150.	Trend CPU utilization and forecast resource exhaustion across critical devices.	M			
151.	Historical memory utilization should be stored for forecasting and resource planning.	NM			
152.	Show top IP-to-IP usage to detect congestion or misuse.	M			
153.	The Solution should automatically collect and store historical data so users can view and understand network performance trends.	NM			
154.	The Solution should provide the ability to “baseline” performance metrics and determine normal operating values and patterns based on time of day, week etc. The ability to threshold on these values should be available.	NM			
155.	Supports real-time alarm collection from all network elements including routers, switches, firewalls, SDWAN controllers, WLAN controllers, load balancers, UPS, and wireless access points. System allows exclusion of non-compliant devices from monitoring policies. Enables proactive detection through SNMP polling, telemetry ingestion, and event correlation across hybrid infrastructure.	NM			
156.	Provides interactive network topology visualization where nodes and links represent routers, switches, links, and media. Users can click on each node or link to access device IP, hostname, interface status, errors, VLAN, port speed, interface usage (Tx/Rx power), and ticket status. Supports overlay mapping of SD-WAN tunnels, depiction of primary/secondary links, and out-of-the-box dashboards for isolated sites. Enables correlation of performance metrics, alarms, and incidents for real-time operational awareness.	NM			
157.	The Solution should support intelligent alarm aggregation based on topology, device relationships, historical patterns, and CMDB correlations, reducing noise and enhancing incident clarity.	M			
158.	The system should be capable of managing high volumes of alerts from large networks within a single console and support multi-tenancy to cater to multiple organizational views securely.	M			
159.	Must visualize SD-WAN overlays and underlay paths, show link health and interface status	NM			
160.	The Solution must collect SNMP traps, and API-based telemetry from firewalls, routers, SDN platforms, and load balancers.	M			
161.	Real-time dashboards should reflect up/down status, packet loss, latency, and tunnel availability across both underlay and overlay networks.	M			
162.	Raise alerts for abnormal traffic spikes or blocked flows between specific IPs.	M			
163.	Correlate fault and performance data to assist in root cause identification.	M			
164.	Log MAC-level topology including L2 adjacency for network visualization.	M			
165.	Track MAC address information such as flaps, conflicts, and dynamic changes across switches.	NM			
166.	Monitor NAC enforcement logs and posture validation results.	NM			

Technical Specification – 2 _Enterprise Network management system (NMS)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
167.	Capture and log network flows.	M			
168.	Auto-ticketing should be enabled for events such as interface/link down, high latency, jitter, or packet loss as reported by network monitoring Solutions or SD-WAN controllers.	M			
169.	Must support SNMP-based interface polling for bandwidth, errors, discards, and packet loss.	M			
170.	Should provide visibility into link health and faults impacting the underlay layer.	M			
171.	Monitor ACI fabric metrics including fault domains, leaf-spine connectivity, and endpoint group status.	M			
172.	Support virtualization / HCI monitoring for virtual switch, logical routers, and flow statistics.	M			
173.	Must enable real-time data ingestion and outbound event publishing via API integration.	M			
174.	Solution must support SNMP v2/v3 polling, traps, and MIB browsing for network device metrics.	M			
175.	Support ICMP ping monitoring for packet loss, delay, and node availability verification.	M			
176.	The platform must include root cause correlation and diagnostic views from event chains.	M			
177.	Must capture flow metadata and log packet-level headers for forensic analysis.	NM			
178.	Dynamic network topology, Network Discovery and Reporting	M			
179.	Should support Fault Analysis	M			
180.	Integrations with other performance Solutions procured as part of this RFP or procured separately (including existing Solutions).	M			
181.	The Solution shall provide the capability to ingest Software Defined Network (SDN) topology and configuration details through APIs and ensuring visibility into traffic patterns and efficient troubleshooting of performance issues.	M			
182.	The Solution shall provide the capability to discover and monitor ACI environments, including mapping of endpoint groups (EPGs) and bridge domains to application services, thereby enabling comprehensive visibility into application-centric network infrastructure.	M			
183.	Use SNMP for discovery and attribute collection of routers, switches, and interfaces.	M			
184.	Maintain flow relationships and associate with devices/interfaces.	M			
185.	Auto-discover MAC addresses linked to interfaces and assign to asset records.	M			
186.	Store MAC address as part of CI properties with historical changes.	M			
187.	Overlay tunnel and underlay link mappings from SD-WAN controllers should be integrated into the CMDB.	M			
188.	Underlay (physical) network components must be discovered and linked with overlay tunnels.	M			
189.	Overlay tunnels should be associated with underlay paths and applications in the CMDB.	M			

Technical Specification – 2 _Enterprise Network management system (NMS)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
190.	System must support ingestion of configuration and topology data from SDN controllers via API or SNMP.	M			
191.	The Solution shall provide auto-discovery and mapping of ACI endpoint groups and bridge domains, with the ability to associate them to applications and Configuration Item (CI) records within the CMDB. The mapping should update dynamically to reflect changes in the network and application infrastructure.	M			
192.	SNMP data must be used for auto-discovery of devices, interfaces, and topology relationships.	M			
193.	The proposed system must support multiple types of discovery like IP range discovery - including built-in support for IPv6, Import data - from pre-formatted files (IPs, ranges, strings or ports), Seed router based discovery - Using route tables and SNMP MIBs, Trap-Based Discovery - whenever new devices are added with capability to exclude specific devices based on IP addresses / IP Address range.	M			
194.	Should be able to generate a graphical representation of the network. Identify which devices are inactive or out of compliance. Use filters to immediately view isolated specific network segments.	M			
195.	The Solution must allow administrators to create own custom metrics and certify new devices for monitoring. It should also allow configuration of the device properties via an API.	M			
196.	The Solution should have readily available integration with SCCM deployed in the environment.	NM			
197.	The Solution should support zero-touch on-boarding of devices through discovery profiles, enabling automated identification and configuration at the time of registration.	NM			
198.	The system must support SDN controller-triggered configuration change tracking and allow RFC generation for firewall, router, or load balancer updates.	NM			
199.	Load balancer rule modifications, firewall ACL updates, and SD-WAN policy changes must be validated via linked change workflows.	M			
200.	The Solution shall capture and track all changes to firewall rules. The solution must integrate with standard ITIL-based change management workflows to ensure that all modifications are logged, monitored, and audited for compliance and security requirements.	M			
201.	Capture underlay link and overlay changes and reflect in CMDB automatically.	NM			
202.	SDN controller-triggered configuration changes must be tracked and audited with rollback capability.	M			
203.	API triggers must allow workflow automation for configuration updates in firewall, routers, or SD-WAN controllers.	M			
204.	Load balancer configuration updates must be tracked, versioned, and integrated with change workflows.	M			
205.	The proposed system should be able to administer configuration changes to network elements by providing solutions to automate the following administrative tasks of effecting configuration changes to network elements like Capture and detect running & start up configuration, Upload configuration, Write start up configuration.	NM			

Technical Specification – 2 _Enterprise Network management system (NMS)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
206.	The proposed Solution should display configuration changes differences in GUI showing modified, remove, masked lined from last captured network configurations for routers and switches. Also this should be able to identify which user has made changes or modifications to device configurations.	M			
207.	The Solution shall have reports based on all types of SNMP traps.	M			
	Reports & Dashboard				
208.	Solution should have a well-defined set of pre-configured reports.	M			
209.	Solution should allow changing/customization of fields and time interval for each report	M			
210.	Solution should allow exporting reports in the format of portable document format (PDF), comma-separated values (CSV) or .doc formats	M			
211.	The proposed Solution must provide multiple type of graphs and data table options including matrix reports	M			
212.	The proposed Solution must have option of report wizard with options like group by, order by, filters, custom reports etc.	M			
213.	Solution should allow scheduling reports to be sent to user mailboxes in multiple formats like portable document format (PDF), comma-separated values (CSV), spreadsheet etc.	M			
214.	The Solution should support configurable SLA reporting with one-click generation of SLA adherence summaries.	M			
215.	Traffic analysis should support both combined (aggregate view) and separate (per-node/domain) visibility.	M			
216.	The proposed Solution should include a structured dashboard interface consisting of features which facilitate Monitor, Analytics, Workflows, Reports, and Solutions, each offering intuitive navigation, role-based access control, and actionable insights tailored to different operational areas.	M			
217.	The Solution must offer real-time visibility into infrastructure performance and health. It should include overview panels such as Site Health, Tunnel Health, WAN Edge Health, and Application Health, as well as sub-dashboards for Devices, Applications, Tunnels, and Logs.	NM			
218.	The platform should provide Geo Map Dashboards that deliver a global and topological view of the network, with overlays for site and tunnel health, allowing geographic performance visualization.	NM			
219.	Heat Map Dashboards should be available to graphically represent site and enabling quick identification of degraded service areas.	M			
220.	The platform must also offer a suite of Troubleshooting Solutions, including: 1. Network Insights for diagnostics based on current network state. 2. QoS Insights to analyse Quality of Service metrics.	NM			

Technical Specification – 2 _Enterprise Network management system (NMS)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
	3. Flow Details for tracking traffic behaviour. 4. Routing Insights for evaluating routing protocol status.				
221.	The platform must also offer a suite of Troubleshooting Solutions, including: 1. Network Insights for diagnostics based on current network state. 2. QoS Insights to analyse Quality of Service metrics.	M			
222.	The Solution should support both predefined and ad-hoc report generation, with export capabilities in PDF, CSV, and Excel formats. Available reports should include: 1. Executive Summary Report summarizing application, tunnel, and site health with trends. 2. Link Availability Report with uptime and availability metrics across devices and regions. 3. Site Availability Report detailing uptime and reliability by site and geography. 4. Link Utilization Report showing RX/TX bitrates and usage percentages. 5. Link SLA Report covering metrics such as jitter, latency, and packet loss. 6. Application Usage Report highlighting top applications based on bandwidth consumption.	M			
223.	Dashboards must show overlay tunnel status, underlay path availability, traffic latency trends, and load balancer pool health.	M			
224.	Historical reports should cover interface uptime, SLA breach analysis, SDN health, and asset-level incident trends.	M			
225.	Dashboards must show interface health, bandwidth utilization, tunnel status (overlay/underlay) and load balancer performance in real-time.	M			
226.	Reports should include, uptime/downtime of links/interfaces, SD-WAN SLA breach statistics, API error/failure rates and traffic analytics from network devices.	NM			
227.	Generate link availability and utilization reports with drill-down by interface or location.	M			
228.	Dashboards must show interface throughput, error count, and utilization trends.	M			
229.	Show device/link/interface up/down trends over time with performance impact insights.	M			
230.	Display SD-WAN tunnel SLA, jitter, latency, and throughput metrics.	M			
231.	Generate overlay tunnel performance reports with latency and loss statistics.	M			
232.	Display SDN flow stats and controller performance metrics.	M			

Technical Specification – 2 _Enterprise Network management system (NMS)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
233.	APIs should allow custom dashboard data ingestion and export for external BI Solutions.	M			
234.	Dashboards should be mobile-optimized.	M			
235.	Include SNMP-collected metrics in uptime, performance, and error rate reports.	M			
236.	Include average/max CPU usage per device in performance dashboards.	M			
237.	ICMP success/failure rates, response times, and packet loss trends must be visualized.	M			
238.	Display device memory usage trends with peak usage statistics.	M			
239.	Provide reports on source-destination IP traffic volume, protocols used, and bandwidth.	M			
240.	Provide diagnostic summaries for each alert, showing probable root cause.	M			
241.	Generate reports on forensic events including source, destination, and protocol data.	M			
242.	Retain historical data for at least 1 year to support trend analysis and for reporting purpose. Traffic analysis/ bandwidth utilization report for network should be available at a granularity of 5 mins for 3 months and with a granularity of 10mins for the remaining period.	M			
243.	Provide visual topology mapping with real-time status of links, nodes, and interfaces.	M			
244.	Enable logical grouping of nodes/devices by region, function, or custom tags for overview visibility.	NM			
245.	Dashboard must offer a high-level Overview with drill-down into key performance indicators.	NM			
246.	A Node Group Overview should summarize health, status, and alerts for grouped IT assets.	NM			
247.	Link Availability Report should include uptime and availability metrics across devices/assets and regions.	NM			
248.	Interface Dashboard must show statistics like packets, errors, utilization, and drops.	NM			
249.	Dashboards must include indicators for device up/down, link status, and threshold metrics.	NM			
250.	Reports must distinguish underlay link status and performance separately from overlay.	M			
251.	Support API data export to BI Solutions and dashboard systems.	M			
252.	Reports must show per-domain and per-application traffic, bandwidth utilization, and historical spikes.	M			
253.	Include SNMP metrics in interface error, utilization, and performance reports.	M			
254.	CPU usage dashboard must display average, peak, and threshold breach timelines.	NM			
255.	Dashboards should show memory utilization over time per device with breach alerts.	M			
256.	Must generate reports showing IP pair traffic volume, protocols used, and top bandwidth consumers.	M			
257.	System should have ability to ingest data from various systems (eg. ACI, SDWAN, etc.) and stored for further analysis from inbuilt portal. Support auto aggregation	M			

Technical Specification – 2 _Enterprise Network management system (NMS)					
#	**Category/Modules**	**Mandatory (M) / Non-Mandatory (NM)**	**Compliance (Yes / No)**	**Evidence**	**Remarks**
	such as hourly, daily roll-up for metrics such as min, max, avg.				
258.	Dashboards must show affected services, devices, and auto-suggest RCA based on alert patterns.	NM			
259.	The NMS performance system must provide out-of-the-box and highly customizable reporting across the network domain. The tool should provide sufficient reports pertaining to asset inventory, alarms & availability reports as well as a detailed asset report.	M			
260.	The proposed system must have a report authoring tool built-in which shall enable complete customization flexibility of performance reports for network devices.	M			
261.	Customized dashboard for daily & historic network health, reports as per requirement of LIC for the entire setup.	M			
262.	All the dashboards shall have resolution sufficient for display on large screens at NOC centre or elsewhere.	M			
263.	The Solution must provide out-of-the-box and highly customizable reporting across the network domain. The Solution should provide sufficient reports pertaining to asset inventory, alarms & availability reports as well as a detailed asset report.	NM			