Revised Annexure F1: Technical Specifications for ITSM (inclusive of ITAM, ITOM with capacity management)

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	**Category/Modules**	**Mandatory (M) / Non-Mandatory (NM)**	**Compliance (Yes / No)**	**Evidence**	**Remarks**
	General Requirement, Ticketing & Self Service				
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. The Solution should have the ability to operate all functionality available in the incident, problem, change, assets, requests etc., as per the scope of this RFP via mobile devices.	M			
6.	The Solution should have End users multi-channel support by allowing user to create tickets via email, phone calls, and a web-based self-service portal. Automatically convert emails to tickets; manage and track all incidents with a defined process through the entire life cycle.	M			
7.	The proposed Solution provides an option for users to track their incidents status and chat/comment with technicians on particular incident	M			
8.	The system should be able to handle loss of connectivity failure of the Centralized ITSM Solution with the ability to support mirrored systems at offsite Disaster recovery facilities.	M			
9.	The Solution should support scalability to support larger and Geographically separated infrastructure to be managed centrally without having to replace current hardware/software and only via addition of relevant modules.	M			
10.	The Solution should provide Search capabilities in all ITSM processes.	NM			
11.	The proposed Solution must provide role-based access control for each process, module, feature available in the Solution	M			
12.	Solution should be able to provide real-time notification alerts via email/ SMS / API/ WhatSapp to notify respective users about any state or status change of a ticket	M			
13.	The Solution should be able to configure the graphical using drag and drop for all fields	M			
14.	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			
15.	The Solution should be able to enable rapid creation of new users and administration of existing users.	M			
16.	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	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	**Category/Modules**	**Mandatory (M) / Non-Mandatory (NM)**	**Compliance (Yes / No)**	**Evidence**	**Remarks**
17.	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			
18.	The Solution should have an interface with all the information about user, readily available when a user calls the helpdesk.	M			
19.	The solution should provide a snapshot of the day, displaying activities feed with upcoming, pending requests, approvals, unresolved issues, and alerts from systems you use in your daily work.	M			
20.	The support person can interact with the end users through chat in built and add those chat transcripts to the ticket.	M			
21.	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			
22.	The Solution should allow categorization and separation of tickets based on compliance and security needs.	M			
23.	The Solution should be compatible with a wide range of protocols and interfaces for third-party integration, including REST APIs, SOAP, PowerShell, SNMP, SQL, FTP, SFTP, SSH, and other standard methods.	M			
24.	Solution must offer robust orchestration capabilities to automate and coordinate routine administrative tasks—such as user provisioning, incident remediation, and software deployment—across integrated systems using event-driven workflows, APIs, and reusable templates	M			
25.	The Solution should operate on a unified architecture while allowing data and workflows to be partitioned based on business units, user roles, or cost centres for better governance.	M			
26.	The Solution should support API integrations to enable seamless data exchange with third-party Solutions like SIEM, IAM, ERP, monitoring platforms, etc.	M			
27.	Must allow secure REST API access with role-based control, supporting OAuth2, API keys, MFA and token-based authentication.	M			
28.	Solution should include pre-built connectors and API for faster integration and automation enablement.	M			
29.	The Solution should support multi tenancy by segregating data, users, and workflows logically within the same platform.	M			
30.	Support flow path visualization from source to destination including intermediate hops.	M			
31.	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			
32.	The Solution should provide ability to support 3rd party integration and have open API/interfaces for integration.	M			
33.	The Solution should provide ability to support multiple levels of administrative delegation. It should be able to define multiple levels of administrative domains so that each administrator is assigned certain resources for which they are responsible.	M			
34.	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			
35.	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			
36.	The solution should provide the ability of integrating events to automatically create trouble tickets in Service desk system for	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	**Category/Modules**	**Mandatory (M) / Non-Mandatory (NM)**	**Compliance (Yes / No)**	**Evidence**	**Remarks**
	in-time problem resolution for supported service desk tool				
37.	Ability to perform event correlation, sending alerts to administrators, real-time and historical analysis with trend and ad-hoc reporting.	M			
38.	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			
39.	The system should offer a centralized monitoring console, displaying events across the environment with GUI-based colour indicators based on severity levels.	M			
40.	The Solution should provide ability to correlate events across the spectrum of infrastructure components and should support events from different OEM's and vendors of the components including Network, hardware, multiple-platform servers, database, etc.	M			
41.	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 Solution	M			
42.	The solution should have reporting ability to perform event correlation, sending alerts to administrators, real-time and historical analysis with trend and ad-hoc reporting.	M			
43.	The solution should have the ability to integrate with the LIC existing and upcoming system and application.				
	Incident Management				
44.	The Solution should support multi-channel different methodology to raise incidents, for example through self-service web portal, email, phone-call to IT support team, mobile app, Web, 3rd Party application, Monitoring Solution- NMS and ITOM	M			
45.	The solution should allow users to create, edit & delete incidents through web interface. Each incident in the Solution must have a unique Id	M			
46.	The time and date automatically recorded mandatorily in the incident record created by the Solution	M			
47.	The solution should have option to identify & record the source of reporting of the incident (such as event/alarm trigger, email, person or group, phone etc.)	M			
48.	The incident records separated from request, problem and change request records and should be able to convert, relate incident to problem, change request	M			
49.	The proposed Solution allows incident records classification according to service category, impacted service, problem category, impact, urgency & priority	M			
50.	Incident records linked to the caller should provide previous incident history of caller while adding the incident	M			
51.	The proposed Solution must have option to route incident records to technicians, third party Vendors.	M			
52.	Incident records can be associated to problem records and/or change records in the Solution	M			
53.	Solution should provide an option for bulk operations like incident categorization, assignment, on hold, resume, resolve, close, merge etc.	M			
54.	The Solution should have predefined escalation matrix for each business service and there should also be an option to update the matrix for each Incident while working on the same	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
55.	The Solution should allow administrators/managers to configure notification rules across the incident lifecycle, with the ability to select specific users who should receive notifications (via email/SMS) at each stage. These configurations must be dynamic and modifiable by administrators/managers as required.	NM			
56.	Should provide option to track the end-to-end SLA, team wise SLA for each team assignment	M			
57.	The proposed Solution must be flexible to include additional information that is required to be logged against incidents.	M			
58.	Solution should allow user to search similar related incidents that have been previously logged in the system	NM			
59.	Solution should allow incident assignment to groups, subgroups, technicians both manually and automatically	M			
60.	Solution should allow user to attach documents to the incident to aid troubleshooting. e.g., error screenshot.	M			
61.	Solution should allow user to attach subsequent tasks to the main incident to take help from other team members or 3rd party Vendors	M			
62.	Each task in the Solution should have the following fields (title, priority, status, due date, owner, estimated duration, actual start date & time, actual end date & time & description, etc) along with option to user to add their own Comments with respect to each Task that is created in the Solution	M			
63.	System should support multiple incident models. It should be able to define different workflow for each department, each location, for each type of business service. It should also be able to define (state, status, priority matrix, custom fields, teams, escalation matrix, dynamic service level agreement (SLA) flow, services, requester/ customers, role-based access control on fields, (dynamic notification templates, associated service asset/CMDB(change management database) etc.)	M			
64.	The proposed Solution must support auto-assignment of incidents to team/group/sub-group/engineer based on pre-defined rules configured from the Solution GUI with intelligence to ensure incidents are assigned to technicians based on services, technician shift details, technician leaves, technician workload etc.	M			
65.	The proposed Solution must provide option to input closure category & Comments for each incident logged in the Solution	M			
66.	The proposed Solution must provide option for recording customer feedback from the Solution GUI	M			
67.	Solution should provide option to log the comments or notes (sequentially record diagnostic activities and work done) at each Level of support staff (i.e. L1 to L2 to more levels) and should be able to extract it in the report	M			
68.	Solution should have incident record access control option to control open, modify and close incident privileges based on pre-established conditions	M			
69.	The proposed Solution must have a comprehensive audit trail which records all incident updates throughout the incident lifecycle with timestamp	M			
70.	Ability to manage and link incident records to multiple SLAs and tiers of service based on IT departments.	NM			
71.	The ability for hierarchical notification about incidents that exceed or will soon exceed Priority/SLA parameters.	M			
72.	The Solution supports the ability to automate incident models and workflow based on record classification.	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
73.	Ability to integrate with event and alert monitoring Solutions, and allow for automatic creation, updating and closure of tickets from these Solutions.	M			
74.	Ability for users (Incident Owners) to create Incident records through the Self-Service portal.	M			
75.	Flexible search capabilities for incident matching and trending based on any key value.	M			
76.	Ability to notify incident owners when the associated problem is resolved.	M			
77.	Ability to store and maintain alerting distribution lists based on incident types.	M			
78.	Ability to link to the Configuration Management database or Configuration Management data; i.e., incident record is pre-populated with relevant information from the Configuration Management database related to the item that failed.	M			
79.	Capability for storing historical incident data and other Incident related information including an audit log with updates and resolutions.	M			
80.	Ability to input free text, screen captures, and file attachments for the recording of incident descriptions and resolution activities.	M			
81.	Ability to use knowledge and/or support scripts for incident diagnosis and resolution.	M			
82.	Ability to create an RFC or problem from an incident with an automatic population of fields	M			
83.	The ability to put incidents on hold so time does not count against SLA.	M			
84.	Ability to reopen/reactivate incident in resolved status.	M			
85.	Ability to generate reports on incident history and trends, by type of incident and by user and by live dashboard.	M			
86.	The Solution should display a live countdown for the remaining response time based on the incidents associated SLA or priority.	NM			
87.	The system must support automatic closure of incidents after a configurable number of business days following resolution status.	NM			
88.	The system should support dynamic incident routing by evaluating parameters like technician availability, location, time of day, and service tiers.	M			
89.	The Solution must enable creation, editing, resolution, closure, or cancellation of incidents while maintaining full lifecycle traceability.	M			
90.	The Solution shall be integrated with existing LIC - IT infrastructure for automatic ticket logging, assigning, updating, closing etc.	M			
91.	The proposed service desk Solution must also provide flexibility of logging, assigning, viewing, updating and closing incident manually via web interface, SMS etc.	M			
92.	The service desk Solution shall provide the capability to identify duplicate tickets and allow for creating parent-child relationships that clubs all duplicate/repetitive tickets to a parent ticket.	M			
93.	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 colours.	NM			
94.	Each incident must be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management Solutions	NM			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
	Problem Management				
95.	The proposed Solution must record problem, record date and time, problem source, contact detail, symptoms and status	M			
96.	Solution should allow problem records to be classified according to priority and category	M			
97.	Solution should allow a problem record to be escalated based on pre-established rules with option to manually overridden conditions	M			
98.	Solution should have functionality to group incidents that share common characteristics or attributes into a cluster.	M			
99.	Problem records should have the below facilities but not limited to: 1.they can be linked to configuration items 2.Linked to and routed to support partners or 3rd party Bidders by the resolver/technician/helpdesk team. 3. Have option to add multiple workarounds and Solutions 4. can be created from an incident record or linked with one or more incidents.	M			
100.	Problem records should be continuously monitored for tolerance breaches, and the solution must automatically notify relevant users with detailed breach information. Notifications should be timely, contextual, and include impacted service, breach type, and recommended actions.	NM			
101.	Solution should have option to generate a single-click Root-Cause-Analysis report after problem closure	M			
102.	The solution should allow problem resolution to be tracked in the Knowledge Base, Incident Requests, and the respective Problem Request. It should also support extraction of resolution details as part of the problem report.	NM			
103.	Solution should have option to review major problem records separately	M			
104.	Solution should provide option to analyse the problem record.	M			
105.	The Solution should have logs for approval of RCA, problem manager and engineer inputs.	M			
106.	Ability to prevent closure of a problem before all assignments have been resolved	M			
107.	Ability to automatically update status or close all related incidents to a problem upon updating of status or closure of the problem	M			
108.	Ability to integrate problem management with incident and change management, i.e. ability to associate problem records with change records and incident records.	M			
109.	Ability to automate opening of a problem record from an incident record based on business rules and SLAs	M			
110.	Ability to view impacted CIs from within a problem record, and to view upstream and downstream affected CIs and IT services through a visual depiction.	M			
111.	Ability to track the total amount of time the problem was worked on and how long it was open.	M			
112.	Ability to link problems/known error records to a CI, group of CIs or a service.	M			
113.	Ability for authorized users to create new problem records and enforce data rules and required fields.	M			
114.	Ability of differentiating between problems and known errors.	M			
115.	The ability to make problem and known error details available to Incident Management for use in matching, troubleshooting and resolution.	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	**Category/Modules**	**Mandatory (M) / Non-Mandatory (NM)**	**Compliance (Yes / No)**	**Evidence**	**Remarks**
116.	The ability to route and assign problem records to pre-defined support staff or groups.	M			
117.	The ability to present historical data on problems and known errors for use by support staff during the investigation process.	M			
118.	The ability to support free text, screen captures, and file attachments for the recording of problem descriptions and resolution activities.	M			
119.	The ability for the problem management team to communicate status and progress reports, as well as temporary Solutions and workarounds.	M			
120.	The ability to increase/decrease the severity or impact classification of a problem according to the number of associated incidents and/or the number of end users affected.	M			
121.	The ability to track multiple tasks and assignments with a problem.	NM			
122.	The ability to report on the number of proposed Solutions, most used Solutions, and least used Solutions in the knowledgebase.	M			
123.	Ability to develop templates for recurring problems.	NM			
124.	The proposed 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. 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.	M			
125.	The system must support seamless bi-directional integration to the proposed service desk Solution for trouble ticketing.	M			
126.	The system must allow problems to be linked with persistent issues,	M			
127.	Problems identified through frequent firewall policy denials, SDN flow drops, or load balancer pool health issues must be supported with diagnostics from integrated Solutions.	M			
128.	Repetitive failures should be grouped into problems and analysed using trend data from historical incidents and monitoring events.	M			
129.	Problems related to firewall policy misconfigurations or SD-WAN path instability must be identified based on recurring alerts and root cause linkages.	M			
130.	The Solution should be capable of Identifying & Highlighting IT Infrastructure defects & speed resolution time.	M			
	Change Management				
131.	Solution should allow users to create, edit & delete Change request through web interface. Each Change Request should have a unique and authorized user should be able to raise request for change (RFC)	M			
132.	The proposed Solution must allow change records categorization, classification according to change class (permanent, temporary, recurring), change type (normal, standard, expedited, latent, emergency), change category, service category, impacted service, impact, urgency, priority	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
133.	Change records can be linked to configuration items and multiple CIs should be able to add, edit, delete from change management database (CMDB) automatically.	M			
134.	On the run, team should be created within change, change advisory board (CAB), emergency change advisory board (ECAB), Global Cab, reviewers, approver's team should be able to create and assign them when it is required.	NM			
135.	Change task should be available and it should be categorized in plan, deploy, rollout, rollback, test category. Change manager can be able to create new category based on release requirement.	M			
136.	Each task should have the relevant fields like title, status, due date, owner, Start and End Date along with option to user to add comments.	M			
137.	For Each change all the stakeholders should be able to communicate through Chat/offline Chat or any other option.	M			
138.	Entire change history, approval history should be maintained in chronological order.	M			
139.	Change record should allow to create multiple change models as change template and further change record can be created using these templates	M			
140.	The solution should support creation of custom fields, role-based access control for both fixed and custom fields, dynamic notifications, and configurable workflow rules. This should allow workflows to be easily modified based on changing business requirements.	M			
141.	There should be an option to add change advisory board (CAB) agenda meetings for every change, each meeting should have an agenda to have a discussion on scheduled time for each change, minutes and action plan should be able to add with in CAB agenda meeting and it should be recorded for reference purpose along with date, user, discussion Point	M			
142.	Ability to provide configurable change process and categorization templates.	M			
143.	Ability to relate post implementation incidents and problems resulting from an implemented change.	M			
144.	Ability to create sub activities or task records for a specific change record, for separate assignment to an individual, group or vendors.	M			
145.	Ability to provide a change calendar with scheduled change viewing by group, and to customize the sorting and filtering of calendar views.	NM			
146.	Ability to easily identify the affected CIs whenever a change is made to a particular CI.	NM			
147.	Ability to provide visual depictions of upstream and downstream Cis that can be navigated in a configuration management database (CMDB).	M			
148.	Ability to select and create "preapproved changes" from a list of predefined templates with prepopulated content, such as categorization, text, etc.	M			
149.	Ability to open an RFC against an incident/problem/known error record, and automatic population of the RFC.	M			
150.	Automated notification of RFCs to appropriate person(s) when change is updated, status change, etc.	M			
151.	Ability to have multiple approvers and electronic routing of those approvals	M			
152.	Ability to set response thresholds for automated approval process	NM			
153.	Ability to provide real-time dashboards.	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
154.	Ability to integrate with Incident Management, Problem Management, Configuration Management, Release and Deployment Management, other modules as per the RFP.	M			
155.	Ability to create different process flows according to urgency.	M			
156.	Ability to clone/replicate change records.	NM			
157.	Ability to restrict desired deployment dates during RFC submission based on minimum lead times like month end, quarter end, year-end etc.	NM			
158.	The ability to enter free form text, screen captures, and file attachments as well as the use of codes for recording of change requests.	NM			
159.	The ability to monitor and track the lifecycle of a Change request.	M			
160.	Discovery capabilities for service dependencies highlighting potential impact if a service is added, modified or deleted.	M			
161.	Ability to provide notification and approval workflow to stakeholders and change advisory committee members for changes with critical business impact, collisions and compliancy issues.	M			
162.	Ability to support release and deployment management as part of the change process.	M			
163.	Ability to automatically create a change request for any changes to CIs.	M			
164.	Ability to promote one or more RFC(s) to a release, with corresponding notifications.	NM			
165.	Ability to provide change workflow feeds into release workflow.	NM			
166.	Predetermined fields shall be auto populated when a standard change from the library is entered. Manual entry for certain fields shall be permitted.	NM			
167.	Ability to customize Change Dashboard by person, group and customer.	M			
168.	Automatic warnings of any RFC's that exceed pre-specified time periods during any stage (OLA).	M			
169.	The ability to communicate information of changes and schedules that can be distributed to the key groups such as the Service Desk and user groups	NM			
170.	The Solution should offer pre-defined workflow templates aligned with ITIL best practices for emergency, normal, and preapproved changes.	M			
171.	Each change request should contain a set of mandatory data fields by default to ensure complete documentation of the change process.	M			
172.	The system must allow role-based permissions to approve, retract, or reschedule change requests at any stage of their lifecycle.	M			
173.	The Solution should permit RFC editing based on the user's role and the current status of the change request.	NM			
174.	The Solution must provide options to easily reschedule changes and identify any potential scheduling conflicts in real time.	NM			
175.	The system should support automatic approval routing, capturing responses, tracking approval history, resending approvals, and status changes based on approval outcomes.	M			
176.	The Solution should track and clearly display the progression of change requests through various authorization and implementation phases.	M			
177.	The system should automatically notify assigned individuals at the scheduled start time of their associated change activity.	NM			
178.	The self-service interface should allow end users to search and	NM			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
	utilize a knowledge base to resolve common issues without assistance.				
	CMDB & Configuration Management				
	The proposed Solution should include the following functionalities with single CMDB covering all the in- scope module as per the RFP.				
179.	Solution should allow to dynamically create multiple classes of configuration items for categorization and logical grouping.	M			
180.	Solution should allow to dynamically create custom input forms for each item type.	M			
181.	Each item type in the proposed Solution must have a unique name and unique identifier (like asset id).	M			
182.	Solution should display individual CI details for each item type like server, network equipment, operating system (OS), database, endpoints, documents etc.	M			
183.	The proposed Solution must store CI details including asset ID, asset lifecycle status, criticality, barcode no., serial no., tag no., asset original equipment manufacturer (OEM), asset Bidder, asset warranty/annual maintenance contract (AMC), installation date, invoice no., part no., cost and purchase date.	M			
184.	CIs stored in the solution should support linking with Customers, Incidents, Vendor, and Locations to enable traceability, impact analysis, and efficient service management. This ensures each CI is contextually connected to its users, issues, vendors, and physical or logical placement.	M			
185.	Solution should have option to create the relationship of each CI's with other Item types	NM			
186.	The proposed Solution must have option to attach documents for each CI like invoice soft copy, annual maintenance contract (AMC) soft copy etc.	M			
187.	CMDB should support tracking and managing configuration items involved in release, build, and deployment activities to ensure version control, impact analysis, and deployment traceability.	M			
188.	Ability to automatically flag for update CMDB	M			
189.	Ability to integrate the CMDB to support the Configuration Items prior to or following an approved release.	M			
190.	The Solution must have the ability to encompass the applications and establish the relationship with different types of underlying infrastructure assets. Ability to add or delete Configuration Item (CI) Types and their corresponding fields.	M			
191.	The proposed Solution must have option to capture and store the entire history of each CI in chronological order with timestamps	NM			
192.	Ability to enforce data validation rules on field values on registration of any new CI.	M			
193.	Ability to edit and delete any existing CI field values by authorized users.	M			
194.	Ability to provide predefined CI relationship templates.	M			
195.	Integrates with Incident, Problem and Change Management allowing for the linking of incident, problem and change records to CI records and to make CI information readily available to assist in the classification and prioritization of incidents.	M			
196.	Ability to integrate with Knowledge Management allowing for the linking of knowledge to CI records.	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
197.	Ability to create automated alerts to various people or systems when a CI is found to be in an unauthorized state.	M			
198.	Ability to define the dependency relationship between CIs in both directions using custom terminology if desired. (i.e. hosted on, hosts)	M			
199.	Ability to provide a graphical representation of the dependencies between CIs.	M			
200.	Ability to provide different levels of access to configuration information based on roles.	M			
201.	Ability to maintain an audit trail of changes made to a CI attribute over time.	NM			
202.	Ability to search for a CI by any CI field.	M			
203.	Ability to perform ad hoc/general queries	NM			
204.	Ability to track Asset status and lifecycle management such as procurement, stored, configured, deployed, active and retired stages to support release impact analysis, planning, rollout and deployment activities	M			
205.	Ability to record a wide variety of contracts and licensing agreements by attaching them to records.	M			
206.	Ability to perform software license management including automated notification of license expiration and noncompliance and reporting, tracking and auditing.	M			
207.	The CMDB must support integration with Capacity, Availability, event Management along with other in scope modules to display current status and metrics for each CI.	M			
208.	The Solution should be capable of auto-discovering Configuration Items and automatically mapping dependencies between them to support impact analysis.	M			
209.	The Solution should allow configuring automatic workflow actions triggered by specific CI field values or changes.	M			
210.	Supports API-based discovery and configuration ingestion from routers, switches, firewalls, load balancers, and endpoint devices. Includes GitHub and Ansible integration for version-controlled configuration management. Devices are auto-modelled based on function (router, firewall, etc.) using out-of-the-box templates. Topology includes real-time relationships and configuration details.	M			
211.	The Solution shall support configuration compliance by enabling comparison of device configurations against predefined golden image standards defined by ITSM or security teams. The Solution shall provide automated compliance checks, test specifications, deviation detection, and detailed reports to ensure adherence to organizational and regulatory requirements. It is Asset Management solution's capability.	M			
212.	System must support ingestion of configuration and topology data from SDN controllers, firewalls, load balancers, routers, and various switches using API or SNMP from multiple vendors/ OEM's.	M			
213.	Devices should classify (router, firewall, load balancer, server, database), and linked with associated interfaces, virtual servers, and policies.	M			
214.	Incidents should correlate to specific devices, interfaces, tunnels, and load balancers using CMDB data for rapid resolution.	M			
215.	Support visual mapping of overlay tunnels and underlay paths with ability to track failover history and link health.	NM			
216.	The CMDB must support automated discovery of IT asset in the LIC IT infrastructure.	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
217.	Must discover and store metadata of each interface including speed, duplex, and MTU.	M			
218.	It should provide detail asset information on hardware and software inventory through seamless integration with asset management Solutions and other system/application.	M			
	Capacity Management				
219.	The Solution should be able to monitor and calculate the end-to-end IT Service Capacity as perceived by the customer of the Service	M			
220.	Solution should have the capability or integrate with infrastructure virtualization platforms (VMware, Hyper-V), management frameworks (SNMP, REST APIs) and monitoring Solutions so users can understand and analyse resource capacity, as well as performance characteristics and parameters (e.g., power, storage, server, router, network, etc.)?	M			
221.	The Solution should provide customizable alerts and notifications for storage-related issues like low disk space, high I/O latency, hardware failures, etc. It should support multiple notification channels like email, SMS, and integration with popular platforms like WhatSapp	M			
222.	The Solution should provide real-time monitoring of storage performance metrics such as IOPS (Input/output Operations Per Second), latency, throughput, queue depth, and bandwidth utilization. Historical data analysis and visualization are also beneficial.	M			
223.	The Solution should have features to analyse storage capacity usage trends and predict future storage requirements. It should help identifying potential bottlenecks and proactively plan for storage expansion or optimization.	M			
224.	The monitoring Solution should provide comprehensive visibility into the health and status of your storage infrastructure. It should monitor factors like disk health, RAID array status, temperature, SMART attributes, and other relevant hardware metrics.	M			
225.	The Solution should provide customizable reports and analytics capabilities. It should allow user to generate performance summaries, capacity forecasts, and other storage-related insights for auditing, compliance, and decision-making purposes.	M			
226.	The Solution should handle the current storage environment size and has the ability to scale with the future growth. It should support monitoring of multiple storage devices and provide centralized management.	M			
227.	The Solution should facilitate the monitoring of CI performance and usage levels against customer defined thresholds	M			
228.	The Solution should facilitate the collection of data to measure capacity and performance levels of IT components beyond the defined thresholds from various domains/platforms used as part of an IT system including servers (physical and virtual), databases, middleware, web servers, network devices (Switches, router, LANs etc.) and application. The Solution should support the monitoring of established capacity thresholds and can initiate alerts if thresholds are exceeded.	M			
229.	Solution should have a dashboard with all relevant detail about the performance and capacity of a specific service or SLA (service demand level; end-to-end service performance indicators; supporting resource utilisation; related performance problems, incidents, alerts etc.)	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
230.	The Solution must identify over- and under-utilized links and support optimization of resource usage through performance trend analysis, capacity planning, and bottleneck identification.	M			
231.	It should allow base lining of performance metrics using historical patterns (e.g., time of day/week) and define thresholds with alerts for deviation from normal operating behavior.	M			
232.	The Solution should allow monitoring and trend visualization through custom reports filtered by business and non-business hours, with the ability to select date ranges and save report templates.	M			
233.	The Solution must support detailed reporting on top utilized links, protocols by volume, and traffic distribution across geo-diverse deployments, enabling proactive network planning.	M			
234.	It should support aggregated utilization views and generate typical usage profiles at interface, node, or group levels, enabling clustering and business-service-aligned capacity insights.	M			
235.	The system should support custom threshold profiles for different device groups and allow generations of exception-based reports for proactive alerting.	NM			
236.	Users should be able to define custom metrics, extend monitoring support for new devices via API, and configure device-specific properties for enhanced resource tracking.	M			
237.	It should offer univariate forecasting for bandwidth and capacity usage using machine learning models (Gen AI or any Advanced AI model) to proactively plan for resource expansion and optimize ISP SLA terms.	NM			
	Service Desk and Service Request Fulfilment Management				
238.	The ability to define a catalog of service request types reflects what services are offered to internal or external customers.	M			
239.	Ability to quickly gain efficiencies in the delivery and support of IT services through a self-service Solution on top of ITSM solution.	M			
240.	Provide a centralized catalog of requests (service-level targets, and approval rules) to automate and monitor standard requests.	M			
241.	Enable self-help through knowledge access to reduce the number of calls to the service desk.	M			
242.	The Solution should facilitate the creation of Service Request Records which have unique identifier and number for each Service Request Record	M			
243.	The Solution should provide a pre-defined list of services and descriptions which can be requested by the users.	M			
244.	The Solution should automate capture the date and time of the request registration and all updates throughout the lifecycle of the Service Request Record.	M			
245.	Solution should have self-service interface for end users to submit and track service request, spanning both IT services and non-IT services.	M			
246.	The Solution automates request routing for appropriate authorizations and approvals.	M			
247.	The Solution should have fields to identify Impact, Urgency and Priority based on user-defined factors which can be assigned to Service Request Records	M			
248.	The Solution should have the ability to notify and functionally escalate (assign) a Service request to an individual or support group based on pre-defined parameters, thresholds or manual override condition	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
249.	The Solution should have a self-service interface, making it easy for users to find services and order from a standard 'menu' of pre-defined service option	M			
250.	Solution should provide for Service Requests Workflows and Fulfilment definitions for commonly used IT/non-IT services with approvals, auto assignment, SLA and escalations.	NM			
251.	The Solution should facilitate the ability to create simple to complex request workflows through sequential and parallel tasking	M			
252.	The Solution should facilitate the monitoring and tracking of service request activities from opening through fulfilment to closure	NM			
253.	The Solution should be able to measure ongoing demands for specific services and requests for those services	NM			
254.	The Solution should facilitate gathering customer feedback and / or rating of IT service provisioning.	M			
255.	The Solution should apply rules controlling the re-opening a service request. Time-Based Rule: A service request can be reopened only if it was resolved within the last XX days. Eg: Network Deployment Package" that includes consulting hours, hardware setup, and post-installation support.	NM			
256.	The self-service interface should support knowledge base available to end users' self-resolution.	M			
257.	The self-service interface should be accessible through native mobile in the form of app which users can download through URL or enterprise app store.	M			
258.	Auto-ticketing enabled for link or device issues such as non-reachability, high latency, jitter, or threshold breach. Tickets are correlated with impacted devices and interfaces. SD-WAN tunnel status and service impact visualization included in ticket metadata for improved resolution context.	M			
259.	Users should be able to request network-related services such as "VPN tunnel creation," "Firewall rule modification," or "Load Balancer configuration" via predefined templates.	M			
260.	The requests should trigger automated workflows and approval chains integrated with API-enabled external systems.	M			
261.	The Solution should have a process driven workflow which will incorporate routing of request, setup of service desk, SLA management, electronic request approvals by actionable e-mail, SMS alerts etc.	M			
262.	Request Fulfilment ability to generate workflows in a natural manner through interactive, graphical User interface with drag and drop capabilities.	M			
263.	Request Fulfilment approvers should be able to setup delegates	M			
264.	Proposed ITSM Solution have ability of developing workflow and routing to change the priority of an incident/event.	M			
265.	Ability to create an RFC or problem from an incident with an automatic population of fields.	M			
266.	The service desk should be integrated with topology awareness enabling agents to see the impacted link/interface/tunnel directly from the ticket view.	M			
267.	The solution should ensure that tickets related to a specific Zone, Division, or Branch are accessible only to users and devices within the corresponding domain, maintaining strict access control and segregation.	NM			
268.	Solution should have a chat console for relevant stakeholders to login and jointly address issues.	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
269.	Configure granular, customizable user roles to control permissions on device views, device actions, and system actions.	NM			
270.	The proposed service desk Solution must be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and should support notification and escalation over email, web etc.	M			
271.	The proposed service desk Solution must have a built-in workflow engine. The proposed service desk Solution must support Non-linear workflows with decision-based branching and the ability to perform parallel processing. It should also have a graphical workflow designer for workflow creation and updates.	M			
272.	The solution should automate service desk workflows by capturing and tracking request data, enabling faster resolution such as auto-assigning incidents based on category and urgency.	NM			
273.	The Solution should have the ability to log request on behalf on other users and allow users to track the request as if the requestor has initiated the request	M			
	Knowledge Management				
274.	Solution must have a powerful knowledge management functionality.	M			
275.	Solution must provide role based, team based & user-based access control on Knowledge Base Articles/FAQ/Information/ /Solutions etc.	M			
276.	In FAQ/Solutions type of knowledge, system should allow to add multiple questions/multiple Solutions with single knowledge article	M			
277.	Application should have option to suggest or advice users about knowledge articles during Incident, call, processes are being entered to ensure incidents are logged mostly when resolution details aren't available in Knowledge Base.	NM			
278.	Able to add /view knowledge articles with full-text search and keyword search across all fields.	NM			
279.	Able automatically capture knowledge from incidents, problems, changes and other processes.	M			
280.	Solution should have option to save new resolutions created by technicians as Knowledge Base articles to ensure Knowledge Base can suggest Solutions to users.	M			
281.	Solution should allow to attach files with knowledge articles.	M			
282.	Should be able to highlight the duplicate knowledge base article automatically.	M			
283.	Solution should provide feature to find out knowledge Gaps. E.g. Flagging missing or outdated knowledge articles when similar incidents are logged frequently.	M			
284.	Solutions should provide option to search from external sites.	NM			
285.	Ability to provide knowledge management capabilities by floating the most relevant hits to the top, in order of closest match to search.	M			
286.	Ability to launch fast knowledge searches using the categorization (or partial categorization) selections as key value search parameters	M			
287.	Ability to create a knowledge article via a fill-in-the-blank form	NM			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
288.	Ability to automatically populate a knowledge article into an incident	NM			
289.	Ability to support role-based knowledge items (i.e., a technical role can access either technical-facing or customer-facing articles)	NM			
290.	Ability to manage full life cycle of knowledge articles through administration capabilities (e.g., submission, editing, review, approval, publishing, usage monitoring, etc.)	M			
291.	Ability to have a rich-text editor (RTE) that supports links within documents, document-to-document links and attaching images to documents.	M			
292.	Ability to provide automated administration (ease of adding, editing and maintaining the data, and ability for end-user submission to require review/approval prior to posting)	M			
293.	Ability to have a defined workflow process for reviewing and approving pending knowledge articles that can be displayed graphically.	M			
294.	The solution shall provide the capability to designate certain fields in knowledge article templates as mandatory.	M			
295.	Ability to allow user feedback to rate/score content for usefulness related to the inquiry	M			
296.	Ability to provide a web-based knowledge base that assists in finding, organizing, and publishing knowledge articles that aid in self-service & faster turn-around time.	M			
297.	Solution should be able to communicate with multiple sources service desk discussion forums, internet for knowledge search.	M			
298.	The knowledge component of the service desk should allow grouping and access control for knowledge articles based on user roles or security levels.	NM			
299.	The platform must allow IT teams to publish commonly used Solutions directly to the end-user interface for self-resolution of frequent issues.	NM			
300.	The system should help users and agents search for relevant resolutions across a unified knowledge index, pulling from incidents, problems, known errors, and Solutions in a single search.	NM			
301.	Knowledge article should be linked to repeated issues with standard resolution steps	NM			
302.	Knowledge articles must be created for recurring SD-WAN tunnel issues, firewall troubleshooting, and performance anomalies observed on key interfaces.	NM			
303.	Auto-suggest knowledgebase articles based on error codes and logs for faster resolution.	M			
304.	Store past breach patterns and forensic summaries as knowledge base references.	M			
305.	The proposed service desk knowledge Solutions must provide grouping access to different security knowledge articles for different group of users.	NM			
306.	Enable end users to solve simple and repetitive incidents on their own by accessing relevant Solutions in the knowledge.	M			
	Service Level Management				
307.	Solution should support comprehensive SLA management platform that cuts across Infrastructure Management and Service Management	M			
308.	The Solution should have the capability to record and manage service level targets in terms of automated business rules, alerts, escalations and notifications	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
309.	SLA record have field or fields to record service information. For example: scope, service criticality, contacts, service level targets, agreement date.	M			
310.	The Solution should have the capability to schedule the review cycle and renewal of SLAs, OLAs and Supplier / Underpinning Contracts	M			
311.	The Solution should facilitate the production of real time performance dashboards related to service and process metrics	M			
312.	The solution should support creating Service Improvement Plans (SIPs) linked to the Continual Service Improvement (CSI) register—such as initiating a SIP when SLA breaches are detected for high-priority incidents over a defined period.	M			
313.	The Solution should facilitate the production of Key Performance Indicator (KPI) reports as out-of-the-box or ad hoc reporting	NM			
314.	The Solution should be able to track, store, and access client/customer contracts	M			
315.	Solution should have a consolidated, automated graphical report for SLA compliance with ability to drill down to reason for non-compliance.	M			
316.	Ability to manage service levels for delivery and support of business services	M			
317.	It should enable creation, measurement and reporting of three categories of SLA service targets - time-based response/ resolution of tickets, availability relating to uptime of systems/services, or performance monitoring catering to system metrics like end-user transaction	M			
318.	Ability to link SLAs to business units or departments, so that impact can be assessed if a service is performing below agreed upon levels.	M			
319.	Ability to create dashboards or scorecards that communicate to Service owners in case of any issues and/or failures.	M			
320.	Ability to provide a dashboard view to appropriate SLAs in order to measure request fulfilment against targets.	M			
321.	The product should facilitate linking of services & customers to associate multiple agreements with a customer contract as well as link multiple customers to a particular service.	NM			
322.	The Service Level Management module should integrate with incident and problem management and other modules/solutions to automate escalation and notification activities based on response and resolution targets.	M			
323.	The solution should support with event management and monitoring Solutions to enable triggering of service support related actions based on established thresholds	M			
324.	Ability to publish different support levels for the same service	M			
325.	Ability to incorporate a search engine to facilitate locating service information and ability to provide severity definitions for SLA's.	M			
326.	Ability to handle priority definitions and action times different for each customer	M			
327.	Ability to automate service availability and performance thresholds monitoring against defined SLA's	M			
328.	Ability to support multiple SLA structures such as master agreements with extensions or addendums for specific business units.	M			
329.	Ability to build workflows that allow for the building, agreeing on, approval of and maintenance of SLA/OLAs.	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
330.	The proposed IT Service Management solution must support integration with project management systems to enable seamless synchronization of service requests, incidents, and project tasks.	NM			
331.	Ability to store business process schedules in a central calendar to facilitate the management of Service Level Agreements.	M			
332.	Ability to create and publish Service Components that may include both Professional Services and Technical Services. Eg: Network Deployment Package" that includes consulting hours, hardware setup, and post-installation support.	NM			
333.	Ability to associate individuals with contracts and services (SLM) Service level management.	M			
334.	SLA's violation on monitored end user response time must open a service desk incident out of the box.	NM			
335.	SLAs should be applicable to network link uptime, SD-WAN tunnel availability, firewall service response, and load balancer Virtual IP (VIP) availability.	M			
336.	SLA breaches must trigger real-time escalations and provide dashboards.	M			
337.	SLAs must define metrics such as link uptime, tunnel availability (overlay/underlay), firewall response latency, and mobile app notification delivery times—for example, triggering alerts if tunnel availability drops below 98% over a 24-hour period.	M			
338.	Breach of SLA on Server, storage, application IT asset, network interface health (e.g., repeated down states or congestion) should be tracked and escalated automatically.	M			
339.	Track SLA compliance based on up/down status of critical IT assets and services.	M			
340.	Managing Service Levels for devices and network lines with necessary customization from time to time depending on LIC's agreements with Bidders. Bidder shall be responsible for the customization.	M			
341.	The assignment and escalations shall be customized as per the matrix shared by LIC with the selected bidder.	M			
342.	The solution must ensure that assignments and escalations directed to one bidder remain confidential and inaccessible to other bidders—for example, when a service request is escalated to Bidder A, Bidder B should not be able to view or act on that request.	M			
343.	Each escalation policy must allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console.	M			
344.	The proposed service desk Solution shall support tracking of multi-Bidder SLA (service level agreements) for call requests within the help desk through service types.	NM			
345.	Each escalation policy must allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no or minimum programming.	M			
346.	The proposed service desk Solution must support tracking of SLA (service level agreements) for call requests within the help desk through service types.	NM			
347.	The Solution should be able to provide insights in the service level associated with each ticket	M			
348.	The Solution should be capable of sending automated feedback surveys to end users after request resolution, enabling measurement of user satisfaction.	NM			
349.	The solution must support defining SLAs and escalation rules across support teams, allow configuration of group-based	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
	OLAs, while noting that multi-party service delivery is currently not feasible.				
	Asset Management (Hardware Asset Management and Software Asset Management)				
350.	Ability to maintain organization wide IT, hardware, software and network assets inventory. The Solution should cover endpoints as well as servers.	M			
351.	Asset/inventory management Solution must manage assets from purchase to salvage i.e. from the beginning to the end of an asset's life cycle.	M			
352.	The Solution should maintain an up-to date inventory of distributed hardware and software assets in LIC's IT infrastructure. As the LIC have wide branch network with Zonal offices acting as Local admins, the Solution should be capable to offer local admin roles to zone, IT staff with all capabilities based on role assigned to them.	M			
353.	Asset/inventory management Solution should be such that it can be used to create and store asset numbers and corresponding information, such as parent, location, Bidder and maintenance costs for each asset.	M			
354.	Asset/inventory management Solution should have bundled reporting software so that there are no third-party Solutions required to customize reports.	M			
355.	It should provide a powerful reporting engine administrator to schedule large batch reports automatically e-mailed to multiple recipients, created in multiple formats such as PDF, DHTML revisions of past report output can be archived	M			
356.	The Solution shall support corporate, VPN and internet connected users. There should not be the need to purchase additional software/hardware to support users not connected to the corporate network.	M			
357.	Solution should provide an out-of-box agent deployment Solution for installing agents and it should be able to take feeds from Active Directory, Domains and manually. It should also support the following agent deployment methods – Active Directory Group, Policies, login scripts, email, software distribution Solutions, manually installing the agent.	NM			
358.	The Solution must have built-in support for encrypted communications between components without requiring additional software/hardware.	M			
359.	The Solution should support local distribution preferred servers and peer downloading	NM			
360.	The agents able to dynamically connect to the next nearest Distribution Point if the Distribution Point assigned to the agent is not available.	NM			
361.	The Solution should prevent users with admin rights to uninstall the agent	M			
362.	The Solution should be able to hide the agent from the Desktops "Add/Remove Program" list from the central console.	NM			
363.	The Solution should allow console users to create custom queries on hardware asset information to be retrieved by the agents.	M			
364.	The Solution should have ability to track standalone executable-based applications on each computer i.e., Applications that do not need to be installed but just needs to execute a standalone program	M			
365.	The Software analysis by system on covered systems should include the following information (but not limited to) :	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
	1) Publisher name 2) Software title name 3) Software title version 4) Total computers Count 5) Total runs Count 6) Total time 7) Average runs 8) Last used Time with the ability to drill down for more detailed views.				
366.	Solution must include a "Software ID Catalogue" that identifies all commonly used applications / thousands of Standard publishers/ software Bidders & their Solutions.	NM			
367.	Solution must include a "Software ID catalogue" that allows for the entry of custom developed software titles& custom classification of standard applications based on user references.	NM			
368.	The Solution should provide history capability till each asset level for hardware/software changes for troubleshooting/ auditing purposes	M			
369.	The Solution should provide Scheduler to determine when the inventory scans can be scheduled for specific group of devices at pre-defined intervals.	M			
370.	The Solution should have capability to discover all unmanaged devices like desktops, servers, laptops, printers, switches and routers. Even if devices are behind firewall.	M			
371.	The system should allow scheduled or on-demand rediscovery with inclusion/exclusion criteria based on IP, hostnames, or device types, and reconcile asset data with ITSM/ITAM Solutions periodically.	M			
372.	The Solution should have ability to track changes in inventory and ability to collect registry information	NM			
373.	The Solution should have full inventory scan for newly discovered devices for all hardware and software. All subsequent scans should be delta scan only	M			
374.	Discovered assets should include detailed metadata such as device name, serial number, hardware/software version, system name, and description for CMDB updates.	M			
375.	It should be capable of inventorying heterogeneous physical network devices, capturing details like make, model, type, software version, and categorized by device function (e.g., router, firewall, and switch).	M			
376.	The Solution should allow scanning of specific device/group of devices on demand	NM			
377.	The Solution should have the ability to identify and maintain records of virtual hosts	M			
378.	The dashboard should visually depict device and link statuses (up/down), performance thresholds, and provide real-time metrics using color-coded indicators for better clarity.	M			
379.	The system should be able to do Inventory governance, including software (authorized and unauthorized) and hardware components.	M			
380.	Interactive topology maps should allow users to click on nodes or links to view device/interface details, errors, performance, and active tickets, aiding in fast troubleshooting.	M			
381.	The System should be able to report last logged in user for any particular asset	NM			
382.	The Solution should manage device name changes in endpoints without losing history. It should also maintain ownership record of each device.	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
383.	The Solution should track assets from the time its purchased to when it is retired	M			
384.	The Solution should be able to consume CSV files so that data in CSV files can be tied with managed devices. It will help in inventorying stand-alone/old/unused devices	M			
385.	The Solution should be able to share data with other systems/Solutions and integrate with SIEM, IT GRC etc. via APIs	M			
386.	The Solution should support backup and configuration management over SSH, TELNET, FTP, SFTP, NETCONF, and APIs, with capabilities for automated IOS upgrades and configuration pushes.	M			
387.	The System should be able to recognize software that is in the following: · Hidden files · Hidden directories	M			
388.	The System should be able to recognize software whose file name has been changed by the user by reading the original header information.	NM			
389.	The Solution should have ability to create customized inventory scans based on business unit like branch, zone etc. or for only specific asset class at pre-defined time periods.	M			
390.	For Hardware Inventory Management the System should allow admin to configure which serial number is retrieved (motherboard chassis, array, controllers, or hard drive chassis).	M			
391.	The System should be able to do automatic identification of the following software attributes (many more required) • Product name • Product version • Manufacturer • Language • File name • Directory file time • Executable type • Internal name • Known as • File description • File extension • File path • File date/time File size	M			
392.	The Solution should maintain full audit trails of configuration changes, compare real-time device configurations with baselines, and support automated backups triggered by change detection.	M			
393.	The System should be able to do Software/Application usage reporting with ability to identify products with minimum usage	M			
394.	The System should be able to Identify software installations which occur outside approved channels	NM			
395.	It should allow rollback to previous configurations with side-by-side comparison, identify non-compliant configurations proactively, and send alert notifications with failure reasons.	NM			
396.	The system should support dynamic grouping of devices by location, model, or type and allow configuration versioning with color-coded difference views.	M			
397.	The System should be able to store data in a centralized-open Relational Database Management Systems (RDBMS)	M			
398.	The System should be able to capture the history of the client's • Hardware changes	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
	• Software changes				
399.	Admins should be able to configure backup retry attempts for failed devices within the same day and schedule configuration restorations from trusted snapshots.	NM			
400.	All hardware asset information shall be recorded in the management server and some of the basic information shall include but not limited to: I. CPU speed and type II. Hard disk space III. Computer name IV. Computer model V. IP address VI. Operating System Attached peripherals	M			
401.	The system should log detailed user actions including session start, configuration changes, and authorization levels for audit and traceability.	M			
402.	The Solution should be able to maintain Asset Classification values with CIA details for each Asset covered under Asset Management Solution.	M			
403.	The Solution should be capable to support each local admin to maintain cost & depreciation sheets with respect to each asset / at aggregate level as per LIC's custom policy within Asset Management Solution itself.	M			
404.	The Solution should have ability to model power policies before being deployed to estimate savings	NM			
405.	The Solution should support bare metal provisioning where-in existing servers can be re-imaged	NM			
406.	The Solution should have Self Service Portal for allowing end-user to manage their own devices. This will reduce Helpdesk calls for password reset and other simple tasks.	NM			
407.	The Solution should support ability to manage and enforce policies settings such as the following: Password Enabled; Password Length; Require Alphanumeric Password; Inactivity Timeout; Wrong Attempts Before Wipe The Solution should also support tracking of warranty/AMC information of covered endpoints and raise expiration alerts	NM			
408.	Solution must have the ability to import contract information like PO, AMC Contract etc. from an external source like Excel / CSV file & link with specific Assets.	M			
409.	The Solution should be capable of generating license compliance reports for both Windows and non-windows OS platforms.	M			
410.	The Solution should be capable to give each local admin the cost structure of IT operations under categories like hardware / software / AMC / Network links etc. as output from reporting Solution.	M			
411.	The Solution should support customized dashboards showing calendar-based counts of configuration backup successes/failures globally and regionally, with drill-down for failure causes.	NM			
412.	The Solution must support application/process blacklisting or whitelisting on end user computing devices	M			
413.	The Solution must be able to perform compliance checks as Cyber Security to ensure compliance as per IRDAI guidelines	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
414.	Must track physical and logical assets such as routers, switches, firewalls, SDN components, load balancers, and map them to their interface details and traffic metrics.	M			
415.	Logical assets such as overlay tunnels, firewall rule sets, and API endpoints should be documented with change/version history.	M			
416.	Store MAC ID metadata along with device inventory.	M			
417.	Associate MAC with hardware assets for traceability and compliance.	M			
418.	Tag devices with NAC status, authentication method, and user info.	M			
419.	MAC discovery should populate asset inventory with connected device relationships.	M			
420.	Inventory Management such as asset report, organized by Vendor name and device.	NM			
	Release and Deployment Management				
421.	Ability to manage all aspects of the end-to-end release process	M			
422.	Ability to capture implementation risk and integration issues related to any release	M			
423.	Ability to log a Release so that changes can be identified and related to the release.	M			
424.	Ensures coordination of build and test environments teams and release teams	M			
425.	Provides management reports on release progress	M			
426.	Ability to capture the release date and time, and who will be implementing.	M			
427.	Ability to attach and store documentation with the release record.	M			
428.	Ability to link resources/approvers to releases.	M			
429.	Ability to display impact of release on configuration items like servers, applications etc.	M			
430.	Ability to assign tasks to individuals to be accomplished within a specified time frame.	NM			
431.	Ability to notify the assignee of the task and due date and the associated Release.	M			
432.	Ability to change status of release and linked changes.	M			
433.	Ability to change status of release approvals.	M			
434.	Ability to automatically send approval requests to the appropriate approvers	M			
435.	Ability to alert release manager when approvals are past due.	NM			
436.	Ability to be automatically notified when the status of a change associated with a release changes status	NM			
437.	Ability to automatically approve releases when all approvals are returned approved and communicate with appropriate parties regarding the approval	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
438.	Ability to store approver comments with the approval, and store approval history for a release.	NM			
439.	Ability to integrate with Change Management of release records to Change records	M			
440.	Ability to validate required information from the CMDB for release build and deployment activities.	M			
441.	Ability to authorize and schedule release deployments in conjunction with Change management processes	M			
442.	Ability to ensure that release deployments are subject to scheduling and approval requirements managed by the change management process.	M			
443.	Ability to automatically flag an update in CMDB with Configuration Items prior to or following an approved release	M			
444.	Ability to support varying Release models such as large-scale or phased deployments.	M			
445.	Ability to integrate with the CMDB to support the association of release records to CI records.	M			
446.	Ability to configure an acceptable date range for approval for each release.	NM			
447.	Ability to manually kick off approval process or override approval workflow.	NM			
448.	Ability to create a real-time dashboard that allows the release manager or any other approved user to quickly ascertain details on release management in one location.	NM			
449.	Ability to search all releases by any release data attribute captured by the Solution.	NM			
450.	Ability to integrate with Problem Management allowing for the linking of Problem and Known error records to Release records.	NM			
451.	Ability to define Release Windows (show conflicts that impact when Releases can be scheduled).	NM			
452.	Ability to create and publish a Master Release Schedule.	M			
453.	Ability to associate the Master Release Schedule with the Service Level Agreement information.	M			
454.	Ability to have full visibility into which changes are associated with which releases.	M			
455.	Ability to support the establishment and governance of release readiness criteria.	NM			
456.	Ability to build, bundle and schedule different types of release packages for deployment.	M			
457.	Ability to identify and control a release package.	NM			
458.	Ability to version release components and packages.	M			
459.	Ability to support the logical association between changes and releases.	M			
460.	The solution should allow administrators to manually initiate the approval process or override the existing approval workflow when necessary.	NM			
461.	The solution must provide the ability to create a real-time, role-based dashboard that enables Release Managers and other authorized users to view consolidated release management details including release status, approvals, and deployment progress within a single interface.	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
462.	Release deployments should validate post-implementation status of interfaces, tunnels, and critical service paths.	M			
463.	The system must track planned releases affecting firewall configurations, SDN controller policies, and link updates.	M			
464.	All related interface or tunnel disruptions during releases must be documented with pre- and post-deployment performance metrics.	M			
465.	Deployment Features & IOS bulk firmware upload	M			
	Availability Management				
466.	The Solution should support the aggregation of availability data from multiple systems for service availability reporting	M			
467.	The Solution should be able to monitor and calculate the end-to-end IT Service Availability as perceived by the customer of the Service	M			
468.	The Solution should be able to perform historical analysis and reporting on availability data	M			
469.	The Solution should generate historical performance trend reports, including best and worst-performing devices or links, to help assess current versus past service behaviour.	M			
470.	The Solution should be able to integrate with event, discovery and provisioning Solutions to monitor various levels of the IT environment	M			
471.	Ability to capture the application/service level details and the interconnectivity/dependency between various systems	M			
472.	The Solution should support the monitoring of established thresholds and can initiate alerts (i.e.: Paging, email, digital bulletin board, etc.) if availability thresholds are exceeded	M			
473.	The system should also generate utilization trend reports for device-level metrics like CPU usage, memory, temperature, and error/discard counts to track performance over time.	M			
474.	The Solution should support the ability to track the number of end-user productivity hours lost (Lost User Hours) for each Availability event	M			
475.	It should include support for comparison reports between service domains or regions, highlighting key variations in uptime, response, or throughput.	M			
476.	The solution should provide functions for tracking the schedule and status of Availability and Continuity exercises, including planned maintenance, failover testing, disaster recovery drills, and high-availability validations.	M			
477.	Customizable alerting rules and thresholds for different metrics, Real-time notifications via email, SMS, or other communication channels. Escalation policies to ensure alerts reach the appropriate personnel. Integration with incident management systems (e.g., ticketing systems).	NM			
478.	Role-based access control should restrict users to view only their authorized asset or network performance data within the platform.	NM			
479.	The system must support continuous discovery with incremental updates to reflect real-time changes and maintain an accurate topology with low overhead.	M			
480.	Fault and performance correlation should be visual, allowing operators to drill down from fault alerts to performance metrics and vice versa, aiding quick RCA.	M			
481.	The Solution must include an event correlation engine that filters and de-duplicates alerts, helps identify root causes, and prevents console flooding.	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
482.	The console should provide color-coded visual cues for primary and backup links, device outages, VLAN participation, and redundancy status using protocols like HSRP and VRRP.	M			
483.	The system should offer status aggregation for fault and performance data, enabling unified status representation of devices and interfaces.	M			
484.	Should allow cross-module integration between fault, performance, and service desk systems, including synchronized discovery and alert routing.	M			
485.	Must support high-scale monitoring architecture optimized for Linux environments, ensuring scalability across large, distributed networks.	M			
486.	Reports and dashboards must offer interactive navigation, contextual drill-down, and spotlight views (e.g., VLAN highlighting, redundancy views).	M			
487.	Solutions must monitor memory usage on network devices and servers and raise alerts when thresholds are breached.	M			
488.	Performance & Availability of heterogeneous networking, server devices	m			
489.	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			
490.	The Solution must be capable of monitoring the availability, health, and performance of core networking devices including but not limited to CPU, memory, temperature, interface bandwidth utilization.	M			
491.	The Solution should have the ability to check on availability of IT assets.	M			
	Service Catalogue Management				
492.	Should maintain a detailed service catalogue that includes descriptions and service level agreements (SLAs) for each service.	M			
493.	The tool enables the creation and management of an IT service catalogue and stores service-relevant data in the tool, including the associated service descriptions. It should allow the creation of categories and multiple sub-categories (for each category) in a hierarchical order for services offered to the end users.	M			
494.	The tool allows the flexible design of service catalogues to meet individual requirements (e.g., create a service catalogue from a template or a wizard); the tool should have the option to define the workflow for each service made in the Service Catalogues for each process (Incident, Problem, Change, Request)	M			
495.	Solution should define service customers / consumers, possible to define teams responsible for each service.	M			
496.	Solution should create an individually adapted/customized structure of a service catalogue, support individual catalogue views for different target groups	M			
497.	Allow access rights to be assigned depending on the categorization of services based on their role.	M			
498.	Should be able to define the Request template for each catalogue item, which will automatically create a dynamic input form for the user, Predefined content while raising a request, Automatic Assignment Rule, Automatic Task Creation, and Automatic Rules for Task Creation to fulfil the request, Sequential Task Creation and execution.	M			
499.	The solution must support creation of service Catalogue entries that clearly indicate the impact on service availability and provide expected provisioning timelines. These timelines must	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
	be configurable to align with approved change windows and SLA targets.				
	Event Management				
500.	The Monitoring Solution should provide End to End monitoring of complete IT Infrastructure within the Single Module/Product without the need to install multiple products. A single Solution should be able to monitor all of the below without the need to install or configure additional modules / products: • Server Monitoring • Database Monitoring • Kubernetes / Container Monitoring • Virtualization Platform Monitoring • Storage Monitoring • Big Data Monitoring • Cloud Monitoring • Capacity Planning • Log Analytics	M			
501.	The monitoring Solution should support multiple data collection methods including SNMP v3 polling, telemetry streaming, CLI-based monitoring, syslog event parsing, and SNMP trap reception to ensure comprehensive visibility.	M			
502.	The proposed monitoring platform must have a publish/subscribe message-bus architecture – thereby allowing the Solution to provide scalable and resilient monitoring across the infrastructure domain	M			
503.	Proposed Solution must have some inbuilt mechanism to collects management server data from the database. The data includes performance management Solution environment information such as internal details, inventory details, and other data that is helpful for troubleshooting the management server. Proposed component should be automatically installed with the performance management Solution.	M			
504.	The platform must allow configuration of polling intervals on a per-device basis, enabling optimized performance and tailored monitoring granularity.	M			
505.	The proposed Solution must support a multi- tier deployment architecture with distributed management servers for scalability and high availability purposes.	M			
506.	The proposed monitoring Solution should provide secure and encrypted data transfer between data collectors through SSL.	NM			
507.	The proposed Solution should be capable to provide hybrid monitoring architecture through support of both agent-based monitoring and agentless monitoring approach.	M			
508.	The system should enrich raw alarms/events with contextual data such as service, customer, and site information to enhance operational insight.	M			
509.	The proposed monitoring Solution should possess the inherent capability to leverage API's and SDKs to enable integration and monitoring.	M			
510.	The proposed monitoring Solution should have capability to configure actions-based rules for set of pre-defined alarms/alerts enabling automation of set tasks e.g., initiating a script.	NM			
511.	The Solution should support AI / GPT-powered analysis features for anomaly detection and predictive insight generation in infrastructure monitoring environments.	NM			
512.	The system should support remote event correlation capabilities, specifically for network metrics such as packet loss	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	Category/Modules	Mandatory (M) / Non-Mandatory (NM)	Compliance (Yes / No)	Evidence	Remarks
	and jitter, to facilitate end-to-end troubleshooting.				
513.	The monitoring Solution must support profile-based configuration hardening, enabling enforcement of predefined secure baselines per device profile.	NM			
514.	The Solution should support auto-ticketing for events such as device unreachability, link down (both protocol and physical), threshold breaches, and performance issues like latency, jitter, and packet loss. Integration with ITSM systems for ticket management must also be supported.	NM			
515.	The proposed Solution should support distributed/remote monitoring by installing additional management servers / Hubs / collectors at remote locations without any additional licensing overhead or charges for them and should possess capability to store data during any connectivity outage for pre-defined time interval.	NM			
516.	Event correlation engine should map raw events to impacted services using CMDB, suppressing duplicates and enhancing signal clarity.	M			
517.	Single platform to monitor and report on the Infrastructure components/services	M			
518.	The platform must be capable of filtering symptom-level alarms and deducing root causes automatically using event correlation and dependency rules.	NM			
519.	The Monitoring Platform should be able to install on all the standard Operation Systems and hardware platforms including Windows and Linux platforms	M			
520.	The Monitoring Platform must support the all the standard RDBMS databases like PostgreSQL, MS-SQL, MySQL and Oracle and other legacy system.	M			
521.	The proposed monitoring Solution should provide the ability to create custom dashboards with ability to aggregate metrics from all monitored devices and should provide drill down functionality to other defined dashboards within the Solution.	M			
522.	The proposed monitoring Solution should provide functionality to sync with online library for latest updates and support for new functionalities	NM			
523.	Raise alerts for abnormal traffic spikes or blocked flows between specific IPs.	M			
524.	Correlate fault and performance data to assist in root cause identification.	M			
	Reports & Dashboard				
525.	Solution should have a well-defined set of pre-configured reports for the Service Management modules	M			
526.	Solution should allow changing/customization of fields and time interval for each report	M			
527.	Solution should allow exporting reports in the format of portable document format (PDF), comma-separated values (CSV) or .doc formats	M			
528.	The proposed Solution must provide multiple type of graphs and data table options including matrix reports	M			
529.	The proposed Solution must have option of report wizard to add structured query language (SQL) type report with options like group by, order by, filters etc.	M			
530.	The proposed Solution must have option to restrict user access to reports	M			

Technical Specification 1_ Enterprise ITSM (inclusive of ITAM, ITOM with capacity management)					
#	**Category/Modules**	**Mandatory (M) / Non-Mandatory (NM)**	**Compliance (Yes / No)**	**Evidence**	**Remarks**
531.	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			
532.	Solution should provide predefined dashboards for all major process incident, problem, change, release, SLA, request, survey etc.	M			
533.	Should be able to provide the dynamic filters	M			
534.	Should be able to do colour coding, multiple graph type, filters, preview option	M			
535.	The Solution should provide the ability to integrate SDLC indicators within the ITOM/monitoring Management Dashboard, enabling holistic visibility into development and operational metrics.	M			
536.	The Solution should support a single consolidated dashboard for Operations Management, providing visualizations of all IT infrastructure environments with performance summaries and alerts.	M			
537.	The dashboards must support bandwidth bifurcation views for per-domain and per-application consumption over configurable durations (e.g., 6-month sampling, per-minute resolution).	M			

Authorized Signatory of the bidder
Name:
Designation:
Date:
Place:
Seal of the company