7. Enterprise management system

Sr no	Minimum Requirement Specifications
1	Enterprise Management System should provide for end to end performance,availability, fault and event and impact management for all enterprise resources that encompasses the heterogeneous networks, systems, applications, databases and client infrastructure present in the enterprise.
2	The solution provider should be in the Magic Quadrant of Gartner
3	The Service Management solution to be used for incident and problem management, Inventory & Asset management, Knowledge Management, Service Request Management, Self Service, Service level management & Helpdesk management should be built on the same application platform and leverage the same common Configuration Management Database (CMDB) with a unified architecture. The same platform should be used across all modules.
4	The service automation solution should provide an unified solution supporting provisioning, configuration management and compliance assurance across servers, networks and applications.
5	Solution should provide for future scalability of the whole system without major architectural changes.
6	Solution should be distributed and scalable and open to third party integration.
7	The solution should be able to monitor all the IT assets for the organization across all the location spread across the state including servers, storage, network & client level IT assets like laptops, desktops ,printers, routers, switches etc.
8	The solution should provide both Agent based and Agentless Monitoring in a single architecture which will provide the organization with the flexibility to choose the level of management required and deploys the right-sized solution to meet those requirements
9	The agent and agentless monitor should be able to collect & manage event/fault, performance and capacity data and should not require separate collectors.
10	The solution should reduce manual customization efforts and should speed-up problem identification and resolution of the IT performance anomalies with intelligent events.
11	The solution should accelerate problem isolation through accurate analysis of probable cause through end-to-end correlation.
12	The solution should have the capability to identify probable root cause using a variety of filtering and statistical correlation methods to determine their relevance to the issue being researched.
13	The solution should possess capabilities that deliver self-learning capabilities to virtually eliminate the effort of manual threshold, rule, and script maintenance.

DRAFT

14	The solution should be able to generate dynamic performance baselines and continuously update and refine these normal operational bands by automatically adapting to the changes in enterprise infrastructure.
15	The solution should have the capability to perform automated dynamic threshold management.
16	The solution should have predictive analytics and intelligence in-built into it so as to detect any anomaly before it could potentially hit the threshold thereby giving enough lead time to users to resolve the issues before the threshold is breached.
17	The solution should carry out automated probable cause analysis by picking up feeds from every infrastructure component being monitored and automating the correlation of these alarms/events to point out the probable cause of an infrastructure error.
18	Solution should carry out probable cause analysis thereby helping operators to identify the root cause without having to write complex rules for correlation.
19	Should be configurable to suppress events for key systems/devices that are down for routine maintenance or planned outage.
20	Should be able to monitor on user-defined thresholds for warning/ critical states and have mechanism for escalating these events to event console of enterprise management system and raise various kinds of alerts like email, SMS etc.
21	The solution should provide the mechanism for creation of knowledge base and provision the same to the end users with the ability to search for known errors from the knowledgebase
22	Solution should be able to score the events and display the highest impacting events in descending order or any other order as customized by the administrator.
23	The Solution should offer the ability to monitor any custom/homegrown applications for whom the monitoring areas have been defined
24	The solution should be extensible enough to support capacity planning and optimization with data collected through the deployed performance management agent or from agentless data collectors.
25	Should be able to monitor/ manage large heterogeneous systems environment continuously.
26	Should be able to monitor & manage distributed & heterogeneous systems (both 32 bit & 64 Bit) - Windows, UNIX & LINUX, including various market leading virtual platforms like Vmware, Microsoft HyperV etc.
27	Database Monitoring: The solution should be able to monitor all the market leading database solution providers including but not limited to MS SQL, Oracle, MySQL, Postgress etc.
28	The Database monitoring should seamlessly integrate with the same EMS Dashboard/Portal and provide integration with the central event console

DRAFT

29	The tool should provide the organization the ability to easily collect and analyze specific information of applications & databases
30	Servers: Should be able to monitor the server instances, database and instance status, initialization parameters, CPU usage, parallel processing, and SQL tracing
31	Should be able to monitor performance statistics reported as timings and throughput values for such operations as reads, writes, and recursive calls
32	Should be able to monitor statistics reports as averages and percentages for such items as data caches hits, queue waits, disk sorts, and rollbacks
33	Sessions: Should be able to monitor types and numbers of sessions, session status, session details, and SQL text
34	System Global Area: Should be able to monitor usage and free space for the SGA and the library, dictionary, and data caches
35	The Network Management must monitor performance across heterogeneous networks having multiple categories of devices like routers, switches etc. across the organization including the data center, DR site, near DR site & remote offices.
36	It should proactively analyze problems to improve network performance.
37	The Network Management function should create a graphical display of all discovered resources.
38	The Network Management function should have extensive reporting facility, providing the ability to format and present data in a graphical and tabular display
39	Discovery solution should do a complete discovery of IT environment across distributed, virtual and heterogeneous environment and provide a clear and visual mapping of IT infrastructure to business services.
40	Should support discovery of Physical, virtual, network, application, storage and remote infrastructure spread across multiple
41	Solution should support complete agent-less discovery requiring no software to be installed on devices to be discovered.
42	Should automatically map IT infrastructure to business services
43	Should support continuous updates of configuration & dependency data to CMDB
44	The discovery data should contain all the details of the discovery process including where it came from and what was the method to retrieve that
45	Should support troubleshooting and diagnostics for any discovery scan failures
46	Business owners should be able to graphically view the health of the various IT assets & the services
47	Business owners should have a clear view of the extent of impact to their business and if need be the reason behind the impact for any incident planned or unplanned

DRAFT

48	The IT organization should be able to view their incident tickets by business service and impact of the same
49	Solution should have the ability to display the events in a table, service, infrastructure, tree views in multiple levels of view. It should provide each user the ability to select or view the events as per their convenience
50	Should monitor various operating system parameters such as processors, memory, files, processes, file systems etc. where applicable using agent /agentless on the servers to be monitored.
51	Provide performance threshold configuration for all the agents to be done from a central GUI based console that provide a common look and feel across various platforms in the enterprise. These agents could then dynamically reconfigure the performance monitors to use these threshold profiles they receive.
52	The Solution displays the complete process flow for Incident, problem, Change and release Management
53	The solution should have Service Management Process Model in built based on ITIL v3 best practices.
54	At each stage in the cycle of the incident, the system should prompt users on the status and the missing information that is required to complete the flow. The solution should have capability to fill out missing info as much as possible automatically. In case any process step is missed, the system should intelligently identify the missing step and prompts users to complete that step before they move to the next step
55	Solution should provide the helpdesk engineer an ability to see the list of assets used by the end user. This list should be displayed within the incident ticket (incident, change, problem etc.).
56	Should provide relationship viewer to the helpdesk engineer from within the incident ticket for quick incident resolution. The relationship viewer should display the dependencies and impact relationships to other assets and users.
57	Solution should automatically provide solutions from the knowledge base to the helpdesk engineer
58	The helpdesk engineer should be able to view detailed configuration of a selected asset (for example: CPU, RAM, Disk Space, IP address, software installed, software used etc.) for problem resolution.
59	The solution should allow administrators to customize the according to the need and the organizational policies.
60	Workflow must be able to raise notification via email, SMS, alert to EMS dashboard etc. and the have provision to interface with other communication modes.

DRAFT

61	The solution should provide remote control of the asset by Helpdesk Analyst for problem diagnosis
62	Flexibility of logging incidents via various means - web interface, client interface, phone, auto integration with EMS tools
63	Help Desk solution should allow detailed multiple levels/tiers of categorization on the type of incident being logged.
64	Help Desk solution should provide classification to differentiate the criticality of the security incident via the priority levels, severity levels and impact levels.
65	The solution should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location or group individually as well as collectively.
66	It should be possible for the helpdesk engineer to view the Health of a selected asset from within the ticket raised or through the asset monitoring tools.
67	The health view should be consistent across platform (Windows/Linux/Unix) if viewed from within the ticket or through the asset monitoring tools
68	Should support automatic assignment of ticket to the right skilled resource based on business priority. For example for a database crash the issue need not be assigned to an L3 DBA unless the business service is completely down. The solution should allow the administrator to define the skilled resource matrix for correct allocation.
69	Asset causing the business failure and business service that has failed should be automatically related to the ticket.
70	Should be able to consolidated view/reports across locations along with localized views/reports.
71	It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues. Should support full text search capabilities.
72	The proposed solution shall provide comprehensive hardware and software discovery and store the configuration details in a single location.
73	The proposed solution shall allow automated delivery of Software, Patches and OS patches from Central location.
74	The proposed solution shall store inventory and configuration information with date stamps.
75	The Configuration Management Database should support multiple datasets with reconciliation facilities so as to get data from various discovery tools and also through manual import process.
76	The system should not be an end of life / end of service product.
77	Updates and upgrades for minimum three years should be factored

DRAFT