Annexure 08: Technical Specification for Data Centre IT Infrastructure

i. Application Switches

Feature	Specification
General Features	• Rack Mountable: Mountable in standard 42U rack • The switch should have minimum 24 ports, 10/ 100/1000 Base auto-sensing with 4 Nos. SFP slots populated with 2 Nos. of SFP • At least one console port for CLI based configuration
Performance	• 32 Gbps switching fabric • 38 Mpps forwarding rate • Link Aggregation Control Protocol (LACP) to aggregate 4x1Gbps i.e. 4Gbps uplink to the Core LAN Switch
Management	• SSH v2,SNMP v1/v2c/v3, IGMP, RMON I, VLANs, GUI, Web based interface • Compatibility with network management with auto discovery & management. • Manageability on per port basis • Per-port broadcast, multicast, uni-cast storm control to prevent faulty end stations from degrading overall systems performance
Quality of Service (QoS)	• The switches should support the aggregate QoS model by enabling classification, policing/metering & marking functions on a per-port basis at ingress and queuing/scheduling function at egress • The switches should support QoS classification of incoming packets for QoS flows based on Layer 2, Layer 3, and Layer 4 fields.
Security	• 802.1x support • RADIUS support • MAC address based port level filtering support • Time based ACL's
Support	• IEEE 802.3ad support required • The switches should support identification of traffic based on Layer 3 ToS field – DSCP values • Support for rate limiting with granularity of traffic flows.

Feature	Specification
	• TFTP & NTP support
Standards	• Compliant to Standards such as IEEE 802.1x, 802.1w, 802.1s, 802.3x, 802.1D, 802.1p, 802.1Q, 802.3ad, 802.3u, 802.3ab, 802.3z

ii. Specifications for Servers running CAS (State) Solution (Internet, Intranet, Application, Database Mail)

Feature	Specifications
Processor	Minimum 2 x Quad core @ 2.1 GHz or above with 8 MB shared L2 / L3 cache, 1066 MHz / 2000 MT/s FSB expandable to 4 physical processor
Form Factor	Blade can be half / full height with I/O connectivity to backplane
Chipset	Latest Server Chipset
Memory	Min 64 GB FBD DDR2 / DDR 3 RAM scalable to 128 GB with min 2 No's free slots for future expandable capability. Advanced ECC memory support, memory mirroring
HBA with required Cables	The Blade should have redundant 4 Gbps Fiber Channel HBA with required cables
HDD	2 X 146 GB 15 K RPM SAS HDD or more hot swappable system disk per server with 64 MB with mirroring using integrated RAID 0,1 on internal disks. It should be possible to hot swap the drives without shutting down the server
LAN Ports	2 X (1000BASE-T) Tx Gigabit LAN ports with TCP / IP offload engine support / dedicated chipset for network I/O on blade server
Graphics	VGA / Graphics Port / Controller
Server Management	Dedicated Management Chip providing comprehensive remote management capabilities along with a dedicated management port for accessing the chip.

Chassis Specifications:

Feature	Specifications

Feature	Specifications
Processor	Single blade chassis should accommodate minimum 6 (Quad-Processor) / 8 (Dual Processor) or higher hot pluggable blades. Same chassis should support dual CPU and Quad CPU blades
Form Factor	6 U to 12 U Rack-mountable with 25% scalability inside the blade chassis.
Switches	Layer 3 managed switches fitted into the enclosure to connect to 2 ports per blade server and at-least 2 uplink ports per switch. Fiber Channel Switches with minimum 4 Gbps ports fitted into Enclosure to cater to 2 FC Ports per Blade.
Network Connectivity	Dual network connectivity for each blade server for redundancy should be provided. Backplane should be completely passive device. If it is active, dual backplane should be provided for redundancy
Cooling Units	Hot Swappable and redundant Cooling Unit
Visual Management Feature	LED / LCD Alert indicators / Visual Management feature on Blade servers / Chassis for Hard disk drives, processors, blowers, memory etc.
System Management Software	Systems Management and deployment tools to aid in Blade Server configuration and OS deployment. Blade enclosure should have provision to connect to display console / central console for local management like trouble shooting, configuration, system status/health display. Should support proactive identification of out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software / firmware components. Should be able to perform comprehensive system data collection and enable users to quickly produce detailed inventory reports for managed devices. Should support the reports to be saved in HTML, CSV or XML format
Server Remote Management	Remote management capabilities through internet browser with event logging, detailed server status, logs, alert forwarding, virtual control, remote graphical console, remote power control / shutdown, Virtual Floppy and CD for remote boot and configuration, Virtual Text and graphical control, automatic IP configuration via DHCP / DNS/ WINS, with 128 bit SSL Encryption Security. The blade system should have the capability of managing all the blades in the enclosure simultaneously. Should provide Role-based security which allows effective delegation of management responsibilities by giving systems administrator's granular control over which users can perform management operations on devices. Ability to measure power historically for servers or group of servers for optimum power usage

Feature	Specifications
Power	Hot Swap redundant power supplies to be provided. Power supplies should have N+N. All Power Supplies modules should be populated in the chassis.
Optical / Diskette	DVD ROM can be internal or external, which can be shared by all the blades allowing remote installation of S/W and OS
KVM Console	Single console for all blades in the enclosure with built-in KVM switch or Virtual KVM feature over IP
USB Ports	Minimum 2 external USB connections functionality
Security	Should provide Secure Sockets Layer (SSL) 128 bit encryption and Secure Shell (SSH) Version 2 and support VPN for secure access over internet
Operating System	64 bit Microsoft® Windows Server 2008 Enterprise Edition / Red Hat® Enterprise Linux 5 & 4 AS or latest / SUSE® Linux Enterprise Server 9 / Unix / Solaris / Netware / VMware etc. with OEM support, updates, patches for the entire contract period
Multi-platform Support	Should accommodate x64 / RISC / EPIC Processor based Blade Servers for future applications.
Virtualization Support	Server should have capability for minimum 4 Partitions to run Independent OS instance on each partition

iii. SAN

Feature	Specifications
SAN Controller	Dual Active-Active Controller
Cache	• 8 GB Total Mirrored Cache for Disk IO Operations scalable to minimum 16 GB across dual controller
Host Interface	4 host ports per controller, Fibre Channel (FC),4 Gbps per port
Drive Interface	4 drive ports—Fibre Channel (FC) Switched or FC Arbitrated Loop (FC-AL) standard per controller, 4 Gbps per port
RAID	RAID Levels supported: 0, 1, 5, 6.
Power Supply	Fans and Power supplies: Dual redundant, hot-swappable
SAN Support	Box should be compatible of SAN environment
Configuration	• The storage array shall be configured with at least 8 GB cache scalable to minimum 16 GB mirrored across two storage controllers for disk I/O operations.

Feature	Specifications
	• Storage subsystem shall support 300GB 15K RPM disks and 400GB or higher 10K RPM Fibre channel drives & 1TB SATA or higher SATA/equivalent drives in the same device array • Presently, the storage sub system shall be configured with 400 GB or higher of Performance drives and 1 TB or higher on SATA / equivalent. • The storage system should support Flash drives to maximize performance with minimum foot print and power consumption. • The storage system should keep write keep caches persistent during fault conditions to prevent data loss • The storage system should provide upgrade path to larger or future array controller and software technology while maintaining the existing investment. • All the necessary software to configure and manage the storage space, RAID configuration, logical drives allocation, virtualization, snapshots (including snap clones and snap mirrors) for entire capacity etc. • Redundant power supplies, batteries and cooling fans and data path and storage controller. • Load balancing should be controlled by system management software tools. • The multi-path software should not only support the supplied storage and operating systems but should also support heterogeneous storage and operating systems from different OEMs • The storage array should have complete cache protection mechanism either by de-staging data to disk or providing complete cache data protection with battery backup for upto 72 hours or more. • The storage system should be pre-configured with at least 10 TB of raw Storage Capacity (excluding the storage capacity required for storing the storage array operating system) implemented out of which 4 TB shall be configured using Fiber Channel Hard disks @ 400 GB 15 K RPM drives and 6 TB raw capacity shall be configured using 1 TB or higher SATA / equivalent drives. The Storage should have at least 16 Gbps port bandwidth per controller for the connectivity to servers and at least 16 Gbps port bandwidth (aggregated) for disk

Feature	Specifications
	connectivity per controller • The storage array should have the capability to do array based remote replication using FCIP or IP technology • The storage array should support Synchronous and Asynchronous replication across heterogeneous storage arrays from different OEMs • The storage array should support Operating System Platforms & Clustering including: Windows Server 2008 (Enterprise Edition), Sun Solaris, HP-UX, IBM-AIX, Linux. • Storage should support non-disruptive online firmware upgrade for both Controllers and disk drives • The storage array should support hardware based data replication at the array controller level across all models of the offered family • The storage should provide automatic rerouting of I/O traffic from the host in case of primary path failure • Should provision for LUN masking, fibre zoning and SAN security • Should support storage virtualization, i.e. automatic logical drive expansion and shrinking based on policy, creation of different RAID types with in disk group etc. • Should support hot-swappable physical drive raid array expansion with the addition of extra hard disks • The storage system should be scalable from 10 TB to 30 TB of raw capacity using 40% on Fiber Channel drives and 60% on SATA / equivalent drives using the same configuration • Should be able to allocate logical spaces to multiple operating systems in the same storage facility • Should be able to support clustered and individual servers at the same time • Should be to take "snapshots" of the stored data to another logical drive for backup purposes • Should be configured with "snapshots and clone" for 50% of the entire capacity of the storage array • IA should also offer storage performance monitoring and management software. • The IA should provide the functionality of proactive monitoring of

Feature	Specifications
	Disk drive and Storage system for all possible hard or soft disk failure

iv. SAN Switches

Feature	Specifications
Port	• Minimum 16 Active ports (each with minimum port speed 4 GB) within same switch upgradeable to 24 ports with minimum 2 Nos. of additional 10 Gbps FC ports • All cable of length of 10 meter each and accessories for connecting Servers /Devices to SAN • Should have capability of ISL trunking of minimum 8 ports.
Maintenance	• Should support multiple OS. • Non disruptive subsystem maintenance.
Power Supply	Should have dual Fans and Hot plug power supplies switching and service modules.
Management Features	• Should have web based management software for administration and configuration. • Non disruptive microcode / firmware upgrades and hot code activation. • Should support Applications for device management and full fabric management. The management software shall be able to perform following: ○ Fabric View ○ Summary View ○ Physical View ○ Discovery and Topology Mapping ○ Network Diagnostics ○ Monitoring and Alerts
Diagnostics	• Switch shall support in built diagnostics, power on self-test, command level diagnostics, online and offline diagnostics. • Should support the following diagnostics: ○ Online Diagnostics ○ Internal Loopbacks

Feature	Specifications
	○ SPAN ○ FC Debug ○ Syslog ○ Online system health ○ Power on self test (POST) diagnostics
Security	• Should support hardware ACL based Port security, Port Zoning and LUN Zoning • Should support Secure Shell (SSH) encryption to provide additional security for Telnet sessions to the switch. • Should support multilevel security on console access prevent unauthorized users from altering the switch configuration • Should support Fibre Channel trace route and Fibre Channel Ping for ease of troubleshooting and fault isolation

v. Tape Library

Feature	Specifications
Tape Drives	6 x LTO 4 FC drives scalable to minimum 15
Interface	Fiber Channel Interface
Backup	• Should have sufficient speed backup to Tape Library in High Availability for backing up data from the SAN without any user intervention. • Should be able to backup 50% of the entire production landscape in 8 hours window.
Tape Drives	• Should support LTO-4 or latest technology based library with at least 6 LTO-4 tape drives (>=6), rack mountable with redundant power supplies.
Cartridges	• Cartridges should have physical capacity up to 1600 GB per cartridge compressed; 800 GB native. • Atleast 25 LTO 4 Media Cartridges with 2 Cleaning Cartridges, Barcode labels shall also be provided

vi. Internal Firewalls

Feature	Specifications
Physical Attributes	• Should be mountable on 19" Rack • Modular Chassis • Internal Redundant power supply
Interfaces	• 4 x GE, upgradeable to 8 x GE • Console Port 1 number
Memory	• Minimum RAM 1024 MB, Upgradeable to 2048 MB RAM • Flash 256 MB Upgradeable to Flash 512 MB • Cleartext throughput: minimum 4 Gbps • Concurrent connections: up to 1,000,000 • Simultaneous VPN tunnels: 2000
Routing Protocols	• Static Routes • RIPv1, RIPv2 • OSPF
Protocols	• TCP/IP, PPTP • RTP • IPSec, GRE, DES/3DES/AES • PPPoE, EAP-TLS, RTP • FTP, HTTP, HTTPS • SNMP, SMTP • DHCP, DNS • Support for IPv6
Other support	• 802.1Q, NAT, PAT, IP Multicast support, Remote Access VPN, Time based Access control lists, URL Filtering, support VLAN, Layer 2 Firewall, Virtual Firewall, Radius/ TACACS
QoS	• QoS features like traffic prioritization, differentiated services, committed access rate. Should support for QoS features for defining the QoS policies. • Management: Console, Telnet, SSHv2, Browser based configuration, SNMPv1, SNMPv2

vii. Server Load Balancer

Feature	Specifications
Ports	10/100/1000Mbps Ethernet Ports – minimum 2 ports upgradeable to 4 ports
Memory	1 GB upgradeable to 2 GB
Performance	• Minimum of 2 Gbps throughput upgradeable upto 4 Gbps • Minimum of 1 Gbps SSL throughput • Minimum of 4000 SSL connections scalable to 7500 SSL connections
Server Load Balancing Mechanism	• Cyclic, Hash, Least numbers of users • Weighted Cyclic, Least Amount of Traffic • NT Algorithm / Private Algorithm / Customizable Algorithm / Response Time
Redundancy Features	• Supports Active-Active and Active-Standby Redundancy • Segmentation / Virtualization support along with resource allocation per segment / dedicated access control for each segment
Server Load Balancing Features	• Server and Client process coexist • UDP Stateless • Service Failover • Backup/Overflow • Direct Server Return • Client NAT • Port Multiplexing-Virtual Ports to Real Ports Mapping • DNS Load Balancing
Load Balancing Applications	• Application/ Web Server, MMS, RTSP, Streaming Media • DNS, FTP- ACTIVE & PASSIVE, REXEC, RSH, • LDAP, RADIUS
Content Intelligent SLB	
HTTP Header Super Farm	
URL-Based SLB	SLB should support below Management options:

Feature	Specifications
	• Secure Web Based Management • SSH • TELNET • SNMP v1, 2, 3 Based GUI • Command Line
Browser Type Farm	• HTTP Redirection, • HTTP • DNS Redirection, RTSP Redirection • DNS Fallback Redirection, HTTP Layer 7 Redirection

viii. 8 Port KVM Switch

Feature	Specification
Form Factor	It should be rack-mountable.
Ports	• It should have a minimum of 8 ports scalable up to 24 ports. • It should support local user port for rack access. • It should support both USB and PS/2 connections.
Functionality	• It should be capable of storing username and profiles. • It should support high resolution up to 1600 x 1200 • It should be capable to auto scan servers • It should work on CAT 6 / CAT 7 cables.
Rack Mountable LCD Monitor with In-built Keyboard & Mouse	• 1 U Rack Mount • Display size: 15 inches diagonal • Contrast Ratio: 700:1 • Display colors: 16 million • Resolution: SXGA 1280 x 1024 • Brightness: 300 nit • Compatible to both PS/2 and USB based inputs

ix. IP based KVM switch

Feature	Specification
Ports	• It should have a minimum of 16 ports scalable & upgradeable. • It should support 2 remote users and 1 user at the rack
Functionality	• It should take control of servers at BIOS Level • It should facilitate both in-band & out-of band access • It should be able to integrate with power strips, so as to be able to reset power of remote device at port level. • Remote access of both Servers and serial devices such as routers (through same or different appliances).
Integration with secure management device	• Gigabit Ethernet ports • Virtual Media Support of multiple media including 'ISO image' files • Dual (redundant) Power supply • Dual Ethernet with Failover • PC selection – On screen Display menu hot key
Rack Mountable LCD Monitor with In-built Keyboard & Mouse	• 19 inch Rack mountable design • KVM access over IP • Browser based Management available at both remote and local (Supported Browsers = Internet Explorer for MS-Windows, Firefox for MS-Windows and Linux) • Support for resolution of 1600*1200 or above • Single window access to all equipment. • Equipment access logs and event history and send email alerts based on logs details as triggers • Logging should be centralizable in one Syslog server • Absolute Mouse Synchronization
IP KVM Control Center	• The management appliance should provide unified, secure access to KVM, serial and power ports of Data Centre devices via a Web browser. • It should provide policy and security management of users and devices connected to KVM.

Feature	Specification
	• It should be able to assign specific node access to a specific user. • It should allow the administrators to access, manage and view all equipment, manage users and access permissions from a single remote device. • It should support Virtual Media Deny, View and Control access policies. • Should be able to create unlimited user and minimum 10 concurrent users should be allowed. • It should log user activity (login/logout, connect/disconnect) and configuration changes at both Appliance and managed devices, and status changes of the connected appliances. All of the above can be forwarded to a network management system or enterprise notification system via SNMP or Syslog. • Flexible session time-outs • "Strong" user name and password authentication • Network Interfaces allows: TCP/IP, HTTP/HTTPS, SSL, DNS, LDAP/LDAPS • Auto-discovery with device-availability status, and alarms • An array of flexible logging and reporting options with audit trails for diagnostics and troubleshooting • View and manage active user sessions and active ports in real time • OS Support: Windows 2000 Server/2003 Server/XP, Windows Vista, RHEL AS 4.0 and Fedora Core 4

x. Host Based Intrusion Prevention System (HIPS)

Feature	Specification
Functionality	• HIPS should perform log analysis, integrity checking, root kit detection, time-based alerting and active response. It should help to detect attacks, software misuse, policy violations and other forms of inappropriate activities. • Must have “Zero-day” protection against DoS / DDoS and

Feature	Specification
	worm attacks based on traffic behavior. Also it should mitigate Zero day http floods and brute force attack & vulnerability scanning attempts based on traffic behavior analysis
Supporting Platforms	• MS Windows • Solaris (SPARC) • SUSE Linux Server • Red Hat Enterprise Linux / HP-UX / AIX
Minimum Features of Host-based intrusion Prevention:	• Time to Time Signature updates • Monitoring and prevention from Intrusion attack • Verifies success or failure of an server • Monitors specific system • Detects attacks that network-based systems miss • Well-suited for encrypted and switched environments • Near-real-time detection and response

xi. Antivirus software

Features
• Should restrict e-mail bound Virus attacks in real time without compromising performance of the system • Should be capable of providing multiple layers of defense • Should have installation support on gateway / mailing server • Should be capable of detecting and cleaning virus infected attachments as well • Should support scanning for ZIP, RAR compressed files, and TAR archive files • Should support online upgrade, where by most product upgrades and patches can be performed without bringing messaging server off-line. • Should use multiple scan engines during the scanning process • Should support in-memory scanning so as to minimize Disk IO • Should support Multi-threaded scanning • Should support scanning of a single mailbox or a one off scan. • Should support scanning by file type for attachments

Features

• Should support scanning of nested compressed files
• Should be capable of specifying the logic with which scan engines are applied; such as the most recently updated scan engine should scan all emails etc
• Should support heuristic scanning to allow rule-based detection of unknown viruses
• Updates to the scan engines should be automated and should not require manual intervention
• All binaries from the vendor that are downloaded and distributed should be signed and the signature verified during runtime for enhanced security
• Updates should not cause queuing or rejection of email
• Updates should be capable of being rolled back in case required
• Should support content filtering based on sender or domain filtering
• Should provide content filtering for message body and subject line, blocking messages that contain keywords for inappropriate content
• File filtering should be supported by the proposed solution; file filtering should be based on true file type.
• Common solution for anti-spyware and anti-virus infections; and anti-virus and anti-spyware solution should have a common web based management console.
• Should support various types of reporting formats such as CSV, HTML and text files
• Should be capable of being managed by a central management station
• Should support client lockdown feature for preventing desktop users from changing real-time settings
• Should support insertion of disclaimers to message bodies
• Product shall be provided with all the required licenses, software as applicable to meet all the above mentioned specification and hence the proposed solution.
• The bidder has to account for the following client antivirus software :
  o for all servers being installed
  o for all other computing devices such as desktops, laptops etc.
• The bidder would ensure client antivirus subscription valid for the period of project, therefore, no. of client antivirus software/solution, there subscription should work for the project period without any expiration of services.

xii. Backup Software

Features
• Backup Solution should be available on various OS platforms such as Windows and UNIX platforms and be capable of supporting SAN based backup / restore from various platforms including UNIX, Linux, and Windows etc. • Centralized, web-based administration with a single view of all back up servers within the enterprise. Single console should be able to manage de-duplicated and traditional backups. • Should allow creating tape clone facility after the backup process. • Should have in-built frequency and calendar based scheduling system. • Should support the capability to write multiple data streams to a single tape device or multiple tape devices in parallel from multiple clients to leverage the throughput of the Drives using Multiplexing technology. • Should support de-multiplexing of data cartridge to another set of cartridge for selective set of data for faster restores operation to client/servers • Should be capable of taking back up of SAN environment as well as LAN based backup. • Should offer 5 Nos. licenses for SAN based backup and 8 Nos. licenses LAN based backup. • Should support advanced Disk staging. • Should have in-built media management and supports cross platform Device & Media sharing in SAN environment. Should provide centralized scratched pool thus ensuring backups never fail for media. • Should be able to rebuild the Backup Database/Catalog from tapes in the event of catalog loss/corruption. • Should ensure data recovery on any archived tape. • Should offer online backup for all the Operating Systems i.e. UNIX, Windows & Linux etc • Should have online backup solution for different type of Databases such as Oracle, MS SQL, Sybase / DB2 etc. on various OS. • Should provide granularity of single file restore. • Should be designed in a manner so that every client/server in a SAN can share the robotic tape library. • Should be able to copy data across firewall. • Should be capable of reorganizing the data onto tapes within the library by migrating data from one set of tapes into another, so that the space available is utilized to the maximum. The software should be capable of setting this utilization threshold for tapes • Should be able to support versioning and should be applicable to individual backed up object's

Features
• Should have the ability to retroactively update changes to data management policies that will then be applied to the data that is already being backed up or archived

xiii. Archival Software

Features
• The software shall support defined policies that are based on a variety of standard file attributes such as age of file / last access time. • The software shall set high and low watermark levels for purging data from high performance storage based upon a percentage of disk space in use. • The software shall keep active data on host arrays while inactive or compliance data is automatically moved to disk or tape. • The software shall support truncated stub files to point to migrated data, enabling seamless file access regardless of location of the data. • Shall enable back-ups at disk speed, while dramatically decreasing recovery times. • Shall offer a single logical view of both active and inactive data regardless of where it is physically located. • Shall eliminate repeated backups of the same archived data. • OS support: Microsoft® Windows Server 2008, Enterprise Edition / Red Hat® Enterprise Linux 5 & 4 AS or latest / SUSE® Linux Enterprise Server 9 / Unix / Solaris / HP Unix / IBM AIX • Archival servers shall be offered in cluster, Min 2 Node cluster shall be offered based on Industry Standard Servers with 2 x Dual Core Intel CPU , Min 8 GB of RAM , 2 x DC HBA's (4 Gbps) , 4 x NIC Ports on each node.

xiv. Enterprise Management System

Features
Basic Requirement : • Solution should provide for future scalability of the whole system without major architectural changes. • Should be SNMP compliant. • Filtering of events should be possible, with advance sort option based on components, type of message, time etc. • Should support Web / Administration Interface. • Should provide compatibility to standard RDBMS. • Solution should be open, distributed, and scalable and open to third party integration. • Should provide fault and performance management for multi-vendor TCP/IP networks.
Security : • Should be able to provide secured windows based consoles / secured web based consoles for accessibility to EMS. • Should have web browser interface with user name and Password Authentication. • Administrator/ Manager should have privilege to create/modify/delete user.
Polling Cycle: • Support discriminated polling • Should be able to update device configuration changes such as re-indexing of ports
Fault Management • Should be able to get fault information in real time and present the same in alarm window with description, affected component, time stamp etc. • Should be able to get fault information from heterogeneous devices routers, switches, servers etc. • Event related to servers should go to a common enterprise event console where a set of automated tasks can be defined based on the policy. • Should have ability to correlate events across the entire infrastructure components of DC/DR. • Should support automatic event correlation in order to reduce events occurring in DC/DR. • Should support advanced filtering to eliminate extraneous data / alarms in Web browser and GUI. • Should be configurable to suppress events for key systems/devices that are down for routine maintenance or planned outage. • Should be able to monitor on user-defined thresholds for warning/ critical states and escalate events to event console of enterprise management system. • Should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. • Should have self-certification capabilities so that it can easily add support for new traps and automatically generate alarms. • Should provide sufficient reports pertaining to asset and change management, alarms and availability of critical network resources as well as network response times for critical links.

- The tool shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network and system components. The current performance state of the entire network and system infrastructure shall be visible in an integrated console.
- Should provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them. It should be possible to drill-down into the performance view to execute context specific reports.
- Should provide the following reports for troubleshooting, diagnosis, analysis and resolution purposes: Trend Reports, At-A-Glance Reports, & capacity prediction reports.
- Should be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits.

Discovery:

- Should provide accurate discovery of layer 3 and heterogeneous layer 2 switched networks for Ethernet, LAN, and Servers etc.
- Manual discovery can be done for identified network segment, single, or multiple devices.

Presentation:

- Should be able to discover links with proper colour status propagation for complete network visualization.
- Should support dynamic object collections and auto discovery. The topology of the entire Network should be available in a single map.
- Should give user option to create his /or her map based on certain group of devices or region.

Agents

- Should monitor various operating system parameters such as processors, memory, files, processes, file systems etc. where applicable using agents on the servers to be monitored.
- 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 them to use these threshold profiles they receive.

System Monitoring

- Should be able to monitor/manage large heterogeneous systems environment continuously. Should monitor / manage following (based on Stack):
  - Event log monitoring.
  - Virtual and physical memory statistics
  - Paging and swap statistics
  - Operating system
  - Memory
  - Logical disk
  - Physical disk
  - Process
  - Processor
  - Paging file
  - IP statistics

- ICMP statistics
- Network interface traffic
- Cache
- Active Directory / LDAP Services

- Should monitor following with statistics :
  - CPU Utilization, CPU Load Averages
  - System virtual memory (includes swapping and paging)
  - Disk Usage
  - No. of Nodes in each file system
  - Network interface traffic
  - Critical System log integration

Infrastructure Services

- IIS / Tomcat / Apache / Web server statistics
- HTTP service
- HTTPS services
- FTP server statistics
- POP/ SMTP Services
- ICMP services
- Database Services – Monitor various critical relational database management system (RDBMS) parameters such as database tables / table spaces, logs etc.

Application Performance Management

- End to end Management of applications (J2EE/.NET based)
- Determination of the root cause of performance issues whether inside the
- Java / .Net application in connected back-end systems or at the network layer.
- Automatic discovery and monitoring of the web application environment
- Ability to monitor applications with a dashboard.
- Ability to expose performance of individual SQL statements within problem transactions.
- Monitoring of third-party applications without any source code change requirements.
- Proactive monitoring of all end user transactions; detecting failed transactions; gathering evidence necessary for problem diagnose.
- Storage of historical data is for problem diagnosis, trend analysis etc.
- Monitoring of application performance based on transaction type.
- Ability to identify the potential cause of memory leaks.

Reporting

- Should able to generate reports on predefined / customized hours.
- Should be able to present the reports through web and also generate “pdf” / CSV / reports of the same.
- Should provide user flexibility to create his /or her custom reports on the basis of time duration, group of elements, custom elements etc.
- Should provide information regarding interface utilization and error statistics for physical and logical links.
- Should create historical performance and trend analysis for capacity planning.
- Should be capable to send the reports through e-mail to pre-defined user with pre-defined interval.
- Should have capability to exclude the planned-downtimes or downtime outside SLA.

- Should be able to generate all sorts of SLA Reports.
- Should be able to generate web-based reports, historical data for the systems and network devices and Near Real Time reports on the local management console.
- Should be able to generate the reports for Server, Application.
- Provide Historical Data Analysis: The software should be able to provide a time snapshot of the required information as well as the period analysis of the same in order to help in projecting the demand for bandwidth in the future.

Availability Reports:

- Availability and Uptime – Daily, Weekly, Monthly and Yearly Basis
- Trend Report
- Custom report
- MTBF and MTTR reports

Performance Reports:

- Device Performance – CPU and Memory utilized
- Interface errors
- Server and Infrastructure service statistics
- Trend report based on Historical Information
- Custom report
- SLA Reporting
- Computation of SLA for entire DC/DR Infrastructure
- Automated Daily, Weekly, Monthly, Quarterly and Yearly SLA reports.

Data Collection

- For reporting, required RDBMS to be provided with all licenses.
- Should have sufficient Storage capacity should to support all reporting data

Integration:

- Should be able to receive and process SNMP traps from infrastructure components such as router, switch, servers etc.
- Should be able integrate with Helpdesk system for incidents.
- Should be able to send e-mail or Mobile –SMS to pre-defined users for predefined faults.
- Should trigger automated actions based on incoming events / traps. These actions can be automated scripts/batch files.

Network Management :

- The Network Management function must monitor performance across heterogeneous networks from one end of the enterprise to the other.
- It should proactively analyze problems to improve network performance.
- The Network Management function should create a graphical display of all discovered resources.
- The Network Management function should have extensive reporting facility, providing the ability to format and present data in a graphical and tabular display.
- The Network Management function should collect and analyze the data. Once collected, it should automatically store data gathered by the NMS system in a database. This enterprise-wide data should be easily accessed from a central location and used to help with capacity planning, reporting, and analysis.

- The Network Management function should also provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment, WAN links and routers.
- Alerts should be shown on the Event Management map when thresholds are exceeded and should subsequently be able to inform Network Operations Center (NOC) and notify concerned authority using different methods such as emails, etc.
- It should be able to automatically generate a notification in the event of a link failure to ensure proper handling of link related issues.
- The Systems and Distributed Monitoring (Operating Systems) of EMS should be able to monitor:
  - Processors: Each processor in the system should be monitored for CPU utilization. Current utilization should be compared against user-specified warning and critical thresholds.
  - File Systems: Each file system should be monitored for the amount of file system space used, which is compared to user-defined warning and critical thresholds.
  - Log Files: Logs should be monitored to detect faults in the operating system, the communication subsystem and in applications. The function should also analyze the files residing on the host for specified string patterns.
  - System Processes: The System Management function should provide real-time collection of data from all system processes. This should identify whether or not an important process has stopped unexpectedly. Critical processes should be automatically restarted using the System Management function.
  - Memory: The System Management function should monitor memory utilization and available swap space.
  - Event Log: User-defined events in the

SLA Monitoring :

The SLA Monitoring component of EMS will have to possess the following capabilities:

- EMS should integrate with the application software component of portal software that measures performance of system against the following SLA parameters:
  - Response times of Portal;
  - Uptime of IT Infrastructure;
  - Meantime for restoration of services etc.
- EMS should compile the performance statistics from all the IT systems involved and compute the average of the parameters over a quarter, and compare it with the SLA metrics laid down in the RFP.
- The EMS should compute the weighted average score of the SLA metrics and arrive at the quarterly service charges payable to the Agency after applying the system of penalties and rewards.
- The SLA monitoring component of the EMS should be under the control of the authority that is nominated the client so as to ensure that it is in a trusted environment.
- The SLA monitoring component of the EMS should be subject to random third party audit to vouchsafe its accuracy, reliability, and integrity.

ITIL based Helpdesk

- Helpdesk system would automatically generate the incident tickets and log the call. Such calls are forwarded to the desired system support personnel deputed by the Implementation Agency. These personnel would look into the problem, diagnose and

isolate such faults and resolve the issues timely. The helpdesk system would be having necessary workflow for transparent, smoother and cordial DC/DR support framework.

- The Helpdesk system should provide flexibility of logging incident manually via windows GUI and web interface.
- The web interface console of the incident tracking system would allow viewing, updating, and closing of incident tickets.
- The trouble-ticket should be generated for each complaint and given to asset owner immediately as well as part of email.
- Helpdesk system should allow detailed multiple levels/tiers of categorization on the type of security incident being logged.
- It should provide classification to differentiate the criticality of the security incident via the priority levels, severity levels and impact levels.
- It 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.
- It should maintain the SLA for each item/service. The system should be able to generate report on the SLA violation or regular SLA compliance levels.
- It should be possible to sort requests based on how close are the requests to violate their defined SLA's.
- It should support multiple time zones and work shifts for SLA & automatic ticket assignment.
- It should allow the helpdesk administrator to define escalation policy, with multiple levels & notification, through easy to use window GUI / console.
- System should provide a knowledge base to store history of useful incident resolution.
- It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
- The web-based knowledge tool would allow users to access his / her knowledge article for quick references.
- It should provide functionality to add / remove a knowledge base solution based on prior approval from the concerned authorities.
- Provide seamless integration to generate events/incident automatically from NMS / EMS.
- Each incident could be able to associate multiple activity logs entries manually or automatically events / incidents from other security tools or EMS / NMS.
- Allow categorization on the type of incident being logged.
- Provide audit logs and reports to track the updating of each incident ticket.
- Proposed incident tracking system would be ITIL compliant.
- It should be possible to do any customizations or policy updates in flash with zero or very minimal coding or down time.
- It should integrate with Enterprise Management System event management and support automatic problem registration, based on predefined policies.
- It should be able to log and escalate user interactions and requests.
- It should support tracking of SLA (service level agreements) for call requests within the help desk through service types.
- It should 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.
- It should provide status of registered calls to end-users over email and through web.
- The solution should provide web based administration so that the same can be performed

from anywhere.
- It should have a customized Management Dashboard for senior executives with live reports from helpdesk database.

Client Management System

The proposed desktop management system should provide single integrated agent for asset management, remote software deployment and remote desktop control.

Asset Management System:

- The proposed Asset Management solution must provide inventory of hardware and software applications on end-user desktops including information on processor, memory, operating system, mouse, key board of desktops etc. through agents installed on them.
- The proposed Asset Management solution must have reporting capabilities; provide predefined reports and the possibility to create customized reports on data in the inventory database. Report results could be displayed as lists or graphs.
- The proposed Asset Management solution must have the capability to export the reports to CSV, HTML and XML format.
- The proposed Asset Management solution must provide the facility for user defined templates to collect custom information from desktops.
- The proposed Asset Management solution must provide facility to recognize custom applications on desktops.
- The proposed Asset Management solution must support administrators to register a new application to the detectable application list using certain identification criteria's (Like executable, Date/time stamp etc.). The new application must be detected automatically from next time the inventory is scanned.
- The proposed Asset Management solution must provide facility for queries and automated policies to be set up and permit scheduling of collecting engines to pick up the data at defined intervals.
- The proposed Asset Management solution must be able to collect WBEM information.
- The proposed Asset Management solution must integrate with the helpdesk solution and allow ticket creation automatically on an event defined in asset management solution. It should also allow manual ticket creation also.
- The proposed Asset Management solution must support Software metering to audit and control software usage where launching of an application can be prevented based on centrally configured number of licenses for an application.

Remote Software Deployment System:

- It should provide delivery, installation, and un-installation of software (ex. Patches of Anti-virus solution etc.) installed on end-user desktops by software delivery remotely through agents installed on them. It must allow pre- and post-installation steps to be specified if required & support rollback in the event of failure in installing software to end-user desktops.
- The tool should have the capability to install applications based on interdependencies i.e. to be installed in a particular order.
- It should support deployment of MSI based packages using drag and drop method.
- It should perform actual distribution of software remotely, not mere file transfer and manual installation at other end. Automated installation should be possible.

- It should include a Software packager for creating software packages to be delivered to end-user desktops which uses a snap-shot technology.
- It should support both push and pull software distribution modes. A catalog/advertisement option of the existing software delivery packages must be provided for end-user to download and install software of his / her choice.
- Users must be allowed to cancel jobs if they are launched at an inconvenient time. Cancelled jobs must be allowed to be reactivated. Forcing packages onto the computer must also be possible.

Remote Desktop Control Management System:

- The proposed solution should allow remote control of end-user desktop for facilitating resolution of desktop issues without the need to go to the end-user desktop, through agents installed on them.
- It should provide the capability of taking Remote control of Linux systems also using Views sitting on Windows platform.
- It should provide Windows integrated authentication as well as application based authentication option to choose from for the agent installed.
- It should allow host enabled recording which allows the end user to initiate a recording session.
- It should have the ability to convert the recorded sessions in AVI/WMA format so it can be replayed using commonly available Windows media player.
- Centralized User Management should allow administrators to centrally manage remote control users' and their access rights. Administrators must be able to define preferences and capabilities different users or user groups have, as well as defining which targets they can control.
- It should support Seamless integration with management applications such as helpdesk, asset management and Software delivery.
- It should support remote Reboot & Chat functions between nodes.
- It should provide facility for encrypting the authentication traffic and support AES 256.

xv. Cabling CAT6, Fiber MM/ SM Technical Specs

CAT-6 U/UTP Cable

- 4 Pair Cable, 23 AWG Copper with integral cross -member pair separator for uniform characteristic impedance.
- Standardization: ISO/IEC 11801 2nd Ed.; IEC 61156-5 2nd Ed.; EN 50173-1; EN 50288-6-1; EIA/TIA 568B.2.1
- Cable overall diameter 6.3 mm.
- Cable jacket material : PVC
- Should have tensile strength of 100N.
- The cable should have 100ohm impedance and data transmission frequencies up to 250MHz.
- It should be certified by independent test labs like 3P/Delta to meet Cat -6 Standards.

- The cable should be supplied in 500m reel.

Mechanical Test	
Ultimate Breaking Strength	>400 N (90 lbf)
Minimum Bend Radius	≥35mm without load, ≥55mm with load
Electrical Test	
DC Resistance	≤14.5Ω/100 m
DC Resistance Unbalance	≤2%
Mutual Capacitance	4.4pF/100m max.
Capacitance Unbalance	≤150pF/100m max.
Propagation Velocity	67%

Connection Module/Information Outlet

- RJ45 connection module of Category 6, for the establishing of transmission channels of class E with up to 4 plugged connections, complies with Category 6 requirements of the standards ISO/IEC 11801:2002, EN 50173-1: May 2007, DIN EN 50173-1: Dec. 2007 as well as ANSI/TIA/EIA 568-B.2-1, de-embedded tested in acc. with IEC 60603-7-4, interoperable and backwards compatible with Cat.5e and Cat.5.
- Suitable for 10GBase-T applications in acc. with IEEE 802.3an up to 500 MHz and 55 m.
- Parallel pair termination without crossover in acc. with EIA/TIA 568-A/B, gold-plated bronze contacts for >1000 mating cycles, IDC contacts with single-wire strain relief and >20 insertion cycles, contact resistance <50 m Ohm, dielectric strength >1000 Veff..
- Maximum reliability through special contact design without internal transfer points.
- Should have integral dust cover and integrated bend-limiting strain -relief unit for cable entry.
- Should have IDC to hold conductor without using any tool for termination of cable.
- Outlets should be of single metal piece design without any PCB to support the IDC / Contacts.
- Should be reusable and tool less in design in terms of termination of solid wire installation cable AWG22-24 as well as stranded cables AWG 22/7 – 26/7
- Should be made of halogen free material and should be certified by third party like 3P or Delta or GHMT.

Patch Panel 24 port- Straight

- Patch panel with integrated cable tie shelf, 19" fastening kit, labeling field, accepting the snap-in type color coding clips in 8 colors.
- Material: sub-rack made of sheet steel (DC01A) 1.5 mm, color blue achromatized, screen made of plastic (ABS), halogen-free, color medium gray (NCS 2502-B)

- Complies with Category 6 requirements of the standards ISO/IEC 11801:2002, EN 50173-1: May 2007, DIN-EN 50173-1: Dec. 2007 as well as ANSI/TIA/EIA 568-B.2-1, de-embedded tested in acc. with IEC 60603-7-4, interoperable and backwards compatible with Cat.5e and Cat.5.
- Suitable for 10GBase-T applications in acc. with IEEE 802.3an up to 500 MHz and 55 m in case of unshielded.
- Each port should be individually terminated i.e. each Port should be individually replaceable & provide consistent port-to-port performance.
- Each port should have an integral dust cover and integrated bend-limiting strain relief unit for cable entry.
- Patch panels shall be modular in design and capable of supporting Cat 6 UTP/FTP and S/FTP modules on same port. The same panel should have the capability of terminating multimode and single mode fibers alongside the copper terminations.

Patch Cord UTP

- **Standardization:** Compliant with Cat.6, Class E (250 MHz) requirements: ISO/IEC 11801 2nd Edition Compliant with Cat.6 component standards IEC 60603-7-4 and 60603-7-5
- Patch Cords should have PVC jacket with conductor diameter copper strand AWG26.
- Patch cords to use IDC contact technology for all the conductor terminations for better performance and not piercing type contact technology.
- Cat 6 patch cord plug to have metal screening & round cable holder and strain relief boot to avoid bending.
- Plug to have two physically separated levels and all 8 wires need to be separated by dielectrically.
- Should support optional locking mechanism for security purpose wherein the patch cords can be locked on servers and all RJ45 ports and required Mechanical key to open patch Cord.
- All the conductors should be IDC based termination at the RJ-45 plugs without directly crimping the plug on cable.

xvi. Server Racks

Feature	Required specification
Feature	• Depth: 1000 mm • Width: 19” equipment mounting, extra width is recommended for managing voluminous cables • 19” 42U racks should be mounted on the floor with castor wheels with brakes (set of 4 per rack) • Metal: Aluminum extruded profile • Side panel: Detachable side panels (set of 2 per Rack)

Feature	Required specification
	• Floor Standing Server Rack - 42U with Heavy Duty Extruded Aluminum Frame for rigidity. Top cover with FHU provision. Top & Bottom cover with cable entry gland plates. Heavy Duty Top and Bottom frame of MS. Two pairs of 19" mounting angles with 'U' marking. Depth support channels - 3 pairs with an overall weight carrying Capacity of 500 Kgs. • Keyboard Tray with BB Slides (Rotary Type) (1 no. per Rack). • Stationery Shelf 627 mm Network (2 sets per Rack). • All racks must be lockable on all sides with unique key for each rack. • Racks should be compatible with floor-throw as well as top-throw data centre cooling systems. • The racks should conform to EIA-310 Standard for Cabinets, Racks, Panels and Associated Equipment and accommodate industry standard 19” rack mount equipment.
Front/Rear Door	• The racks must have steel (solid / grill / mesh) front / rear doors and side panels. Racks should NOT have glass doors / panels. • Front and Back doors should be perforated with at least 63% or higher perforations. • Both the front and rear doors should be designed with quick release hinges allowing for quick and easy detachment without the use of tools.
Mounting	• All racks should have mounting hardware 2 Packs, Blanking Panel (1) varying from 4 U to 5 U size. • All racks should be OEM racks with Adjustable mounting depth, Multi-operator component compatibility, Numbered U positions, Powder coat paint finish and Protective grounding provisions.
Fan	• Fan trays: Fan 90CFM 230V AC, 4" dia (4 Nos. per Rack) • Fan Housing Unit 4 Fan Position (Top Mounted) (1 no. per Rack) - Monitored - Thermostat based - The Fans should switch on based on the Temperature within the rack. The temperature setting should be factory settable. This unit should also include - humidity & temperature sensor
Cable Manager	• Racks should have Rear Cable Management channels, Roof and base cable access. • Wire managers: Two vertical and four horizontal.
Power Supply	Power Distribution Unit - Vertically Mounted, 32AMPs with 25 Power Outputs. (20 Power outs of IEC 320 C13 Sockets & 5 Power outs of 5/15

Feature	Required specification
	Amp Sockets), Electronically controlled circuits for Surge & Spike protection, LED readout for the total current being drawn from the channel, 32AMPS MCB, 5 KVA isolated input to Ground & Output to Ground (1 No per Rack)

xvii. Network Rack

Feature	Required specification
Feature	• Should be available in 2-Post Configurations • Option of 84" or 96" height • Should be available with an option of Rail Widths: 3", 6", 12" (2-Post) • EIA-310-E Compliant • UL Listed, Certification - Information Technology and Communications equipment • Load Capacity: 1000 lb (2 and 4-Post Al) • EIA Standard Hole Pattern: 12-24 Threads @ 5/8" (127mm), 1/2" (25.4mm) centers • Material: Al: 6061-T6 Aluminum Extrusion (3" Rail), Al: 6061-T6 0.125" Thick, (6" and 12" Rail), Steel: 14 Gauge (0.075 Thick), CRS • Finish: Durable black epoxy powder-coat • Ergonomically designed and aesthetically pleasing, Lightweight, but sturdy
Front/Rear Door	• Should have dual hinge latching door & can be opened right or left. • Easy one point removal and installation process for door • Handle should be recessed to eliminate snag potential for clothes and arms
Cable Manager	• Cable fingers spaced at 1RMU increments for exact alignment with EIA standard • Cable fingers support up to 48 cables per RMU • Should be available in 6", 8", 10" & 12" vertical trough widths both single sided or double sided • In case of Horizontal cable management the cover should hinges up or down and locks into position with cylindrical finger ends for easy snap on installation • Horizontal cable management troughs should be available in 1, 2 & 3 RMU • Open back on 2U and 3U horizontal troughs for easy pass through

Feature	Required specification
	of cables Should have C Channel bracket allowing for easy access to the cable trough • Provision for Tool-less installation of Cable Spool