Annexure 9

Indicative Specification at Centralized infrastructure

1. Data Base Server

Make & Model - (To be filled by the Supplier)		Complied / Not Complied
Form Factor	Rack	
OS Support	OS support: Microsoft® Windows Server 2003 / 2008, Enterprise Edition / Red Hat® Enterprise Linux 5 & 4 AP / SUSE® Linux Enterprise Server 9 / Solaris for x86	
Processor	Latest Generation x86-64 Bit Minimum Hexa-Core Processor with Minimum 1.86Ghz Clock Speed	
Number of Processors	Should be configured with 4 (Four) Processors with scalability upto 8 (Eight) Processors	
Cache	16 MB L3	
Memory	64 GB Scalable up to 1 TB	
Memory Type	DDR3 SDRAM	
Power Supplies	Power supplies: Hot pluggable/hot swappable redundant AC power supply	
Network Interface Ports	Minimum 4 * 10GbE NIC Ports The NIC Ports should support FCoE & iSCSI	
Internal HDD	Minimum 4 * 300GB Internal SAS SFF Hot Plug HDD scalable upto 8 HDD	
Hard Drive Bays	Should have provision for 8 hard drive bays.	
Others	• Raid controller capable of providing RAID 0, 1 and 5 configurations with minimum 512MB cache for RAID operations • 2 * 4 Gb/s FC-HBA Ports or more • At least 4 Ports available for USB, Serial, Network or more • Should have minimum 4 PCI/PCIe based slots or more • Should have internal 8x DVD-ROM drive. • Should have redundant Power supply (Hot Plug/Hot Swap) • Server Management Software • Should support web based remote management • UL, FCC Certifications	

2. Other Servers (Application, Web, Mail etc.)

Make & Model - (To be filled by the Supplier)	Complied / Not Complied
Form Factor : Blade	
Latest Chipset with two Quad-core processor of 2.2 GHz or better clock speed	
Should have initial 16 GB memory and scalable to 64 GB.	

Make & Model - (To be filled by the Supplier)	Complied / Not Complied
Should have provision for Min 2 Hard drive bays.	
Should have hot pluggable/Swapable 2x300GB SAS Hard drives	
Hard drives to be hot-pluggable and of small form factor.	
SAS Raid controller capable of providing RAID 0, and 1 configurations.	
Should have minimum 2 * 10Gbps NIC Ports	
Should have dual ported 4Gbps Fiber Channel HBA	
OS Support: Microsoft® Windows Server 2003 / 2008, Enterprise Edition / Red Hat® Enterprise Linux 5 & 4 AP / SUSE® Linux Enterprise Server 9 / Solaris for x86	
UL, FCC Certifications	
Blade Chassis Specification	
Single blade chassis should accommodate minimum 14 or higher hot pluggable server blades.	
Chassis should be 8U to 12U Rack-mountable	
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	
Blade enclosure should have provision to connect to display console /central console for local management like trouble shooting, configuration, system status / health display. Complete Hardware based Remote Administration from a standard web-browser with Event logging, detailed server status, Logs, Alert Forwarding, virtual control, remote graphical console, Remote Power Control / Shutdown, Virtual Media for Remote boot and configuration, Virtual Text and Graphical Control. The blade system should have the capability of managing all the blades in the same enclosure simultaneously.	
Chassis should be configured with dual Redundant Ethernet network module with minimum of four 10 Gbps Uplink ports	
Chassis should have minimum of 8 I/O bays	
Chassis should be configured with dual Redundant Hot-Swap 8GB Fibre Channel Modules with minimum of 6 x 8Gbps External uplink Ports and should provide no single point of failure.	
Chassis should have fully populated hot pluggable/swappable power supplier and fan.	
It should provide Secure Sockets Layer (SSL) 128 bit encryption and Secure Shell (SSH) Version 2 and support VPN for secure access over internet.	
Chassis should be configured with Redundant Management Modules which provide IPKVM functionality for the entire chassis	
Chassis should be configured with Internal/external CD-ROM/DVD-ROM Drive which can be shared among all the blade servers. The chassis should have minimum one USB 2.0 ports.	
Chassis should have LED/LCD panel to provide power-on, location, over-temperature, information and system error conditions	
Support heterogeneous environment: AMD, Xeon and RISC/EPIC CPU blades must be in same chassis with scope to run Win2003/2008 Server, Red Hat Linux / 64 Bit UNIX, Suse Linux / Solaris x86	

3. SAN

Make & Model - (To be filled by the Supplier)	Complied / Not Complied
The Proposed SAN Array should be configured with minimum 10 TB usable space after RAID5 on FC Disk of 450 GB 15k rpm for database and 20 TB usable after RAID5 using 1 TB SATA/FATA Disk for archival. The proposed SAN array should be 100% scalable in the same manner.	
The Proposed SAN Array must be rack mounted (Adequate OEM rack is being supplied)	
The Proposed SAN Array should be configured with Dual Active – Active Controllers for redundancy.	
The Proposed SAN Array should be configured with minimum 4 x 4Gbps FC front end ports and scalable to 8 or more port in the same controller pair and at least 8 X 4 Gbps back end ports for accessing the Disk.	
The Proposed SAN Array should be configured with at least 8 GB or more cache and upgradable to 16 GB cache across dual controllers by upgrading the controller pairs.	
The Proposed SAN Array should support RAID Levels: 0, 1, 5 & 6	
Support for Windows 2000/2003, HP-UX, IBM AIX, LINUX, Solaris OS	
Provision for Redundancy of Disk Drives, Controllers, Fans & Power Supplies	
In case of power failure, the SAN array must be provided with cache protection mechanism (Cache De-Stage to disk/Battery backed) to ensure no loss of data in case of power outage minimum of 96 hours.	
The storage array should be able to support intermix of Enterprise Flash, 15 K RPM FC disks, 10 K RPM FC disks and 7.2 K RPM SATA/FATA disks	
The SAN Array should be supplied with Snapshot or Point-in-time Copy functionality for snapshot and full copy of the production LUN's / volumes. The Software should be licensed for the entire supported capacity of the SAN Array / Frame from day one.	
The SAN Array should be supplied (with required software & hardware) with array based data replication in both synchronous & asynchronous modes. The replication capability should be bidirectional with ability to fail back to achieve RPO <= 60 Min and RTO <=6 hrs.	

4. Tape Library

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
Tape drives: Minimum 2 latest generation LTO 4 or higher tape drives	
Interface: Fiber Channel Interface	
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 back-up 50% of the entire production landscape in 8 hours window	

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
Should support latest generation LTO drives or latest technology based library with at least 2 latest generation LTO drives tape drives (>=4), rack mountable with redundant power supplies	
Cartridges should have physical capacity up to 800 GB native and 1600 GB compressed per cartridge	
At least 50 latest generation LTO drive Media Cartridges with 5 Cleaning Cartridges, Barcode labels shall also be provided	

5. SAN Switch

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
The SAN switch should have adequate populated ports to cater for the redundancy in connectivity from any other equipment.	
Switch should have non-blocking architecture	
All 24 ports should be concurrently active	
Throughput of each port in the SAN switch should be 4 Gbit/sec full duplex with no over-subscription.	
All the ports should operate at min 4Gbps in a nonblocking backplane	
Setting of the port speed to 4Gbps or 8Gbps from the lower speed should not impact the other ports in the same port blade.	
All the SAN Switch components should be hot swappable	
All the SAN Switch components should be field replaceable units	
The SAN switch should provide for redundant hot swappable cooling subsystems	
Power supply and fan assembly should have different FRU.	
The SAN Switch should support Virtual Fabrics feature	
The SAN Switch should enable partitioning of a physical SAN into logical fabrics	
The SAN Switch should enable isolation of logical fabrics by application	
The SAN Switch should provide advanced zoning capabilities	
The SAN Switch should allow health monitoring capabilities	
The SAN Switch should allow performance monitoring capabilities	
The SAN Switch should have support for web based management	
The SAN Switch should support CLI.	
The SAN Switch should have proactive fault detection to avoid any hot-spots in the fabric.	
The SAN Switch should have alerting capability to avoid any hot-spots in the fabric.	

6. KVM Switch 8 port & Console terminal with necessary cables

Make & Model Offered - (To be filled by the Supplier)		Complied / Not Complied
LEDs	Bank and Active Port Display	
Client/Host Connectors	Keyboard: 6-pin Mini-DIN Female PS/2/USB	
Mouse:	6-pin Mini-DIN Female PS/2/USB	
Monitor:	HDDB 15-pin Female VGA, SVGA, XGA, Multisync	
Daisy-Chain Connector:	Two 6-pin Mini-DIN + One 15-pin HDDB (Standard KVM Cable minimum 12 feet)	
Monitor Resolution Support:	Up to 1920 x 1440	
Display Data Channel:	DDC1, DDC2B, DDC2AB	
Keyboard State:	Saved and Restored	
On Screen Display:	Yes; Password Protected	
PC Control:	Keyboard, Hot Key, Push Button	
Switching Confirmation:	Buzzer	
Daisy-Chain Level:	8	
Max. PC Control:	64	
Bandwidth:	200MHz	
Form Factor:	Rack Mountable	
Power Requirements:	DC 12V, 1A	
Compliances:	CE, FCC Class B, VCCI	
Safety:	UL	

7. Server Load Balancer

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
Architecture	
Should have minimum 12 x 10/100/1000 BaseT Ports plus 4 x 1000Base-Lx Port.	
Should have dedicated 10/100/1000 BaseT port for out-of-band management.	
Should have minimum 8 GB RAM and upgrade-able	
Support minimum 2,000,000 Concurrent L4 TCP connections	
Should capable to handle 100,000 L4 connections per second	
Should provide minimum 2 Gbps Layer-7 throughput and can be scalable to 4-Gbps throughput.	
Should have non-blocking 24Gbps backplane	
Should provide minimum 5000 SSL TPS for SSL offloading scalable to 20,000 TPS for future requirement.	
Should provide minimum 1Gbps server-side hardware based http compression.	
Should provide minimum 100 Mbps SSL throughput.	
Should support Dynamic routing protocols like OSPF, RIP1, RIP2.	
Load Balancing Features	
Support for 2000 servers	

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
Support for minimum 512 Virtual IP	
Should support load balancing algorithms: Least amount of Bytes,	
Least number of users/session, Cyclic, weighted Cyclic, SNMP Parameters; like Server CPU utilization, memory utilization and combination of both.	
In case of Server / Application failure device should detect it in not more than 30 seconds	
In case of Server failure traffic should be diverted to another Server automatically	
Should support content based Load balancing features: HTTP Header based redirection, URL-Based Redirection, Browser Type Based Redirection, Preferential Treatment (Cookie-Based)	
Should Support session persistency Based on: IP, DNS, Cookie-based, URL Parameters, SSL Session ID-based etc.	
Should support Client NAT & Server NAT	
Should support TCP optimization and TCP Multiplexing	
Should support HTTP 1.1 protocol based caching	
Should support hardware based web compression	
Server Management Feature	
Should support Graceful shutdown of Servers	
Should support Graceful Activation of Servers	
Should able to redirect traffic based on Source IP, Destination IP & TCP PORT	
Redundancy	
Should Support standard VRRP (RFC - 2338)	
Should support transparent failover between 2 devices	
Support for Global Server Load Balancing Algorithms	
Should support DNS based redirection	
Should support HTTP redirection	
Should support RTSP Redirection	
Should support VIP advertisement via Dynamic Routing	
Health Monitoring	
Should provide individual health check for each Server & Application	
Should be able to do health check on protocols like HTTP, SMTP, POP etc	
Should able to check the health of Server OS, Application & contents as well	
Should provide AND & OR Grouping mechanism between health check for granular approach for detecting path failure in multi-tier application architecture like core banking solution	
Health Check configuration should be via simple GUI interface and easy to understand, it should not require any scripting or CLI configuration.	
Device Management & Reporting	
Should provide GUI interface for configuration & reporting	
Should provide HTTP / HTTPS interface management	
Should provide SSH / Telnet / CLI interface	
Should support SNMP V1, V2c, V3	

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
Should provide Detailed LIVE reporting for traffic on each farm	
Should provide detailed historic reporting for server traffic	

8. **Firewall + IPS**

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
Hardware Feature	
The Firewalls should be Hardware based, Reliable, purpose-built security appliance with at least 6 No.s of 10/100/1000 Base Tx interfaces & upgradeable to 8 Interfaces for future expansion with 2 USB ports & 1 console port	
Should be redundant supporting Active/Active or Active/Standby Firewall for High Availability & Scalability	
Firewall Throughput of minimum 20 Gbps	
IPSEC 3DES Throughput of Up to 4 Gbps	
Concurrent Sessions of at least 1,400,000	
IPSec VPN Peers of up to 2500	
Virtual Interfaces (VLANs) support for at least 2000 VLANs for forming Secure server Farms and DMZs	
Scalability through clustering and load balancing	
Software Features	
Application Security Services	
The Firewall should have Integrated specialized inspection engines for protocols like HTTP, FTP, DNS, SNMP, ICMP, NFS, H.323, SIP, RTSP and many more	
The Firewall should provide advanced inspection services to detect and optionally block instant messaging, peer-to-peer file sharing, and other applications tunneling through Web application ports	
Inspection of H.323, SIP based voice and multimedia streams	
To provide TCP stream reassembly and analysis services to help detect attacks that are spread across a series of packets	
Network Containment and Control Services	
Inbound and outbound access control lists (ACLs) for interfaces, time-based ACLs, and per-user or -group policies for improved control over network and application usage	
Powerful reporting and troubleshooting capabilities that help enable collection of detailed statistics on which ACL entries are triggered by network traffic attempting to traverse a security appliance	
Rich dynamic, static, and policy-based NAT and PAT services	
Secure Connectivity Services	
IPSec VPN services for up to hundreds of simultaneous remote devices	
Support for Internet Key Exchange (IKE) and IPSec VPN standards with hub-and-spoke or meshed VPN configurations	
High-Availability Services	
Support for Active/Active & Active/Standby failover.	

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
Support for bidirectional state sharing between Active/Active failover pair members for support of advanced network environments with asymmetric routing (PBR) topologies, allowing flows to enter through one Firewall appliance and exit through the other, if required	
Support for Synchronizing all security association state information and session key material between failover pair members	
Support to perform software maintenance release upgrades on the Firewall failover pairs without affecting network uptime or connections	
Intelligent Networking Services	
Support for multiple virtual interfaces on a single physical interface	
Comprehensive OSPF & BGP dynamic routing services	
Capability to forward DHCP requests from internal devices to an administrator-specified DHCP server, helping enable centralized distribution, tracking, and maintenance of IP addresses	
Support for NTP to provide convenient method for synchronizing the clock on the firewall appliance with other devices on a network	
Flexible Management Solutions	
Support for Built-in Management Software for simple, secure remote management of the security appliances through integrated, Web-based GUI	
Should provide a wide range of informative, real-time, and historical reports that give critical insight into usage trends, performance baselines, and security events	
Accessible through variety of methods, including console port, Telnet, and SSHv2	
Strong authentication of users through the Firewall appliance through a local user database or through integration with enterprise databases, either directly using RADIUS and TACACS+	

Gateway Level Antivirus

Make & Model Offered - (To be filled by the Supplier)	Compliance (Yes/No)
Gateway level Anti Virus should provide high-performance protection against viruses in SMTP, POP3, IMAP, HTTP and FTP traffic. It should block viruses and worms from penetrating into an organization's internal network through e-mail attachments, malicious Web pages, and files obtained through FTP.	
Virus gateway should provide real-time detection of viruses and malicious code at the gateway for SMTP, POP3, IMAP, HTTP, and FTP Internet traffic.	
The proposed solution should be licensed per unit and should support unlimited users	
Virus Gateway should have option to configure to respond to virus detection in several ways ie. Delete the file, quarantine the file, Alert email	
Frequent updates of virus pattern files should be available from the Web site, and option for scheduling for automatic download and installation should be available.	
In terms of SMTP AV scanning the solution should not act as mail relay or MTA by itself.	
Should have facility to block files based on file extensions over HTTP, FTP, SMTP,	

Make & Model Offered - (To be filled by the Supplier)	Compliance (Yes/No)
POP3 as well as IMAP	
Should have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc.	
If it is not integrated within firewall appliance then stand alone solution should not introduce delays	
Antivirus throughput of the appliance should be more than 900 Mbps minimum.	

Intrusion Prevention System (IPS)

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
IPS should be either integrated with firewall and should have 2 Gbps IPS throughput or an external device.	
Should not induce Latency into the Network, Latency should be less than 200 microseconds	
The appliance monitors upto 4 inline segment and has 8 10/100/1000 interfaces for the same.	
The appliance should have separate dedicated 10/100/1000 Mbps interface for management console. None of the monitoring ports should be used for this purpose.	
The IPS should be deployable in the following modes: Passive or IDS mode, Inline Protection Inline Simulation	
IPS vendor should have its own original threat intelligence analysis center and is not overly dependent on information available in the public domain.	
IPS should detect and block all known, high risk exploits along with their underlying vulnerability (not just one exploit of that vulnerability).	
IPS should employ full seven-layer protocol analysis of all internet protocols and data file format.	
IPS should operate effectively and protect against high risk, high impact malicious traffic via default out of box configuration, should be able to block more than 2000+ attacks by default.	
IPS should have option of automatic download of signatures through vendor's own signature database and not relying on any third party updates. IPS should perform stateful packet inspection	
IPS should detect and block malicious web traffic on any port.	
Does TCP stream reassembly?	
Does IP defragmentation.	
Does Protocol anamoly detection	
Does Bi- directional inspection	
Detects attacks within protocols independent of port used	
Does RFC Compliance	
Does Protocol tunnelling	
IPS should do attack recognition inside IPv6 encapsulated packets	
IPS should do active blocking of traffic based on pre-defined rules to thwart attacks	

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
before any damage is done.	
Accurately detects intrusion attempts and discerns between the various types and risk levels including unauthorized access attempts, pre-attack probes, suspicious activity, DoS, DDoS, vulnerability exploitation, brute force, hybrids, and zero-day attacks.	
Allows full policy configuration and IPS sensor control via encrypted communications with remote management system.	
Can enable/disable each individual signature.	
Each signature should allow granular tuning.	
Supports assigning of ports to custom applications.	
Filters traffic based on IP address or network range, protocol, and service in support of organizational security policy to allow/disallow specific types of activity between hosts.	
Should support Active/Passive and Active/Active for the appliance, the HA should be out of the box solution and should not requires any third party or additional software for the same.	
HA solution should support High Protection that is should maintain state such that there is no gap in protection during failure of one of the appliances.	
IPS should fail open in case of power, software or hardware failure when deployed in stand alone mode.	
IPS should notify console of unit interruption. The console should receive alert and/or provide additional notification to administrator should any component become non-operational or experience a communications problem.	
IPS should support granular management. Should allow policy to be assigned per device, port ,VLAN tag, IP address/range	
Management Console should be able to integrate and correlate with vulnerability assessment solution of the same brand/ third party.	
IPS should offer variety of built-in responses including console alerts, database logging, email notifications, SNMP traps, offending packet captures, and packet captures.	
IPS should offer Includes built-in reports. The console should be capable of producing graphical metrics and time-based comparison reporting.	
IPS vendor should have 24/7 security service update and should support real time signature update.	
Firewall, IPS, Antivirus and IPSec VPN solution should be ICSA certified	

9. Back-up Software

Make and Model Offered - (To be filled by the Supplier)	Complied / Not Complied
Backup Solution should be available on various Operating System platform like, UNIX (SUN Solaris, HP-UX and IBM AIX etc.), Linux, Netware, and Windows and etc. Should support clustered configurations of the backup application in a cluster. i.e. backup application should failover as a highly available resource in a cluster.	

Make and Model Offered - (To be filled by the Supplier)	Complied / Not Complied
The backup software should be capable of doing full, incremental, differential, and variable block based deduplicated backups. The software should also be capable of offering deduplicated tape outs.	
The backup software should be capable of performing self healing of backup indexes, this would include consistency checking on its indexes to verify if there is any corrupt data.	
The backup software should be able to encrypt the backed up data using 256-bit AES encryption.	
Software should have full command line support on above mention operating systems.	
Should have SAN support on above mention operating systems. Capable of doing LAN free backups for all platforms mentioned above.	
Should support "Hot-Online" backup for different type of Databases such as IBM DB2, Oracle, MS SQL, Sybase etc.	
Software should have an inbuilt feature for Tape to tape copy feature (cloning, within the tape library) to make multiple copies of the tapes without affecting the clients for sending tapes offsite as part of disaster recovery strategy.	
Should have the optional ability of staging the backup data on a disk and then de-stage to a tape based on the policy for faster backups.	
Should support NDMP backup to disk. Should support NDMP multiplexing of NDMP and no NDMP data to the same tape. The software should be capable of doing NDMP configuration through the GUI.	

10. Enterprise Management System (EMS)

Make and Model Offered - (To be filled by the Supplier)	Complied / Not Complied
Functional and technical requirements (DR servers & DR networks can be monitored from primary site)	
The Enterprise & Network Management System should be used to manage all enterprise resources with a solution that encompasses the heterogeneous networks, systems, applications, desktops and databases present in the system. It should have the capability to consolidate all the information to one console with a support for providing a Web interface. Proposed solution must be from same OEM for seamless integration as well as OEM products should be recognized by industry analysts like Gartner\Forrestor\IDC.	
The discovery services in the EMS should discover systems, network devices and the topology. This capability allows for a complete inventory of all visible IT resources. The inventory scanning process should be able to discover any custom IT resources, such as CSC interface application etc.	
Solution should be inclusive with hardware, OS, patches, etc. and should have compatibility to standard RDBMS	
Solution should provide for future scalability of the whole system without major architectural changes.	
Should provide fault and performance management for multi-vendor TCP/IP	

Make and Model Offered - (To be filled by the Supplier)	Complied / Not Complied
networks.	
User Interface	
EMS should provide a Graphical User Interface which is user-friendly to depict all the IT infrastructure and applications, making IT management much more intuitive.	
The EMS should offer a Web browser interface. The Web browser interface should enable management of IT resources via Internet or Intranet access or through Dial Up/remote access. EMS should be integrated with GIS solution.	
Event Management	
The EMS should offer a unique solution to the problem of managing exception events. It should correlate and filter events from different types of IT resources, and pinpoint the root cause of a problem.	
This event manager should also permit integrating custom applications with the EMS. It should be used to integrate not only management applications, but also general business applications to make them easier to manage. With event filtering and correlation, multi-level managers and agents, automatic corrective measure, the EMS should provide comprehensive event management capabilities. It should eliminate the clutter of spurious alarms and simplify the management of complex IT infrastructure.	
It should help to notify through cell phone andemail, of various/selective events occurring in the enterprise.	
Software Distribution	
The software distribution function should provide flexible and scalable delivery, installation, and configuration of software.	
The software distribution should support customizable distribution schedules, alternate methods, heterogeneous network protocols, diverse operating systems including UNIX, and both push and pull distribution modes.	
Compression should be supported while distributing the software across WAN.	
Furthermore, its integration with the event management functions of the EMS should provide complete tracking, logging, and automated correction of failures during the delivery and installation process. In addition, its integration with the security functions of the EMS should enable administrators to deliver software with peace of mind.	
It should be possible to store images of the servers and desktops and restore images from the image server. It should distribute the image to the desktops/Servers by using the booting from image floppies.	
Network & Server 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 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.	

Make and Model Offered - (To be filled by the Supplier)	Complied / Not Complied
The Network Management function should also provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment and the top-contributing hosts, 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 pagers, 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 security, system, and application event logs must be monitored.	
Reporting	
The Reporting and Analysis tool should provide a ready-to-use view into the wealth of data gathered by Management system and service management tools. It should consolidate data from all the relevant modules and transform it into easily accessible business-relevant information. This information, should be presented in a variety of graphical formats can be viewed interactively (slice, dice, drill down, drill through).	
The tool should allow customers to explore the real-time data in a variety of methods and patterns, and then produce reports to analyze the associated business and service affecting issues.	
The presentation of reports should be in an easy to analyze graphical form, enabling the administrator to put up easily summarized reports to the management for quick action (Customizable Reports). The software should be capable of supporting the needs to custom make some of the reports as per the needs of the organization.	
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.	
SLA Monitoring	
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;	

Make and Model Offered - (To be filled by the Supplier)	Complied / Not Complied
• Transaction handling capacity of application server in terms of number of concurrent connects; • Uptime of data center/ Servers; • Meantime for restoration of Data Center, Services etc. • Network Specific SLAs • System Specific SLAs • Application Specific SLAs • End-to-End Service Based SLAs	
EMS should compile the performance statistics from all the IT systems involved, including the EQMS and compute the average of the parameters over a month, and compare it with the SLA metrics laid down in this document;	
The EMS should compute the weighted average score of the SLA metrics and facilitate arriving at 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 to the mutual agreement of Purchaser & the Supplier, so as to ensure that it is in a trusted environment.	
Helpdesk Management	
The proposed ITIL-based Helpdesk Management System must provide the following features:	
The proposed helpdesk solution must provide flexibility of logging, viewing, updating and closing incident manually via web interface. The web interface console would also offer power-users tips.	
The proposed helpdesk solution must support at least 8 ITILv3 processes like request management, problem management, configuration management and change order management with out-of-the-box templates for various ITIL service support processes. Bidder should provide ITIL v3 certification letter on at least 8 processes.	
Each incident must be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.	
The proposed helpdesk solution must be able to provide flexibility of incident assignment based on the workload, category, location etc.	
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.	
The proposed helpdesk knowledge tools solution must provide grouping access on different security knowledge articles for different group of users.	
The proposed helpdesk solution must have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.	
The proposed helpdesk solution must support tracking of SLA (service level agreements) for call requests within the help desk through service types.	
The proposed helpdesk solution must be capable of assigning call requests to techal staff manually as well as automatically based on predefined rules, and should support notification and escalation over email, web etc.	
The proposed helpdesk solution must integrate tightly with the Knowledge tools and	

Make and Model Offered - (To be filled by the Supplier)	Complied / Not Complied
CMDB and should be accessible from the same login window.	
The proposed helpdesk solution must allow the IT team to see the CI relationships in pictorial format, with a specified number of relationships on single window.	
The proposed helpdesk solution must have a built-in workflow engine. The proposed helpdesk 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 with drag & drop feature for workflow creation and updates.	
The proposed helpdesk solution must have an integrated CMDB for better configuration management & change management process.	
It should support remote management for end-user & allow analysts to do the desktop sharing for any system located anywhere, just connected to internet.	
Remote desktop sharing in Service desk tool should be agent less & all activity should be automatically logged into the service desk ticket.	
It should allow IT team to create solution & make them available on the end – user login window for the most common requests	
Application Performance Management System	
The proposed solution must determine if the root cause of performance issues is inside the monitored application, in connected back-end systems or at the network layer from a single console view	
The proposed solution must proactively monitor 100%of real user transactions; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes	
The proposed solution must provide deeper end-to-end transaction visibility by monitoring at a transactional level and without deploying any software at end user desktop. The solution must provide a single view that shows entire end-to-end real user transaction and breaks down times spent within the application components, SQL statements, backend systems and external 3rd party systems.	
The proposed solution must be able to provide root-cause probability graphs for performance problems showing the most probable root-cause area within application infrastructure.	
The proposed solution must provide real-time monitoring of resource utilization.	
The proposed solution must identify any changes to application configuration files(.xml, properties etc), File system or application code and be able to correlate changes to application performance dynamically in production environments.	
The proposed solution must proactively identify any thread usage problems within applications and identify stalled or stuck threads. The proposed solution must also monitor web services across multiple processes	
The proposed solution should allow access to performance data both using a Graphical user interface (GUI) and web based access and provide ability to monitor performance of applications up to the method level of execution (Java/.Net method) 24x7 in production environments with negligible impact on monitored application.	
The proposed solution should measure the end users' experiences based on transactions without necessitating installation of client agents / probes on end-user desktops.	
The proposed system must be able to detect user impacting defects and anomalies	

Make and Model Offered - (To be filled by the Supplier)	Complied / Not Complied
and reports them in real-time. The proposed system must also be able to provide user usage analysis and show how user's success rate, average time and transaction count has changed over a specific period of time such as current week versus previous week.	
The proposed system must be able to pro-actively determine exactly which real users were impacted by transaction defects, their location and status.	
The proposed system must be able to provide the ability to detect and alert when users experience HTTP error codes such as 404 errors or errors coming from the web application.	
Identity Management	
• Identity administration and provisioning — authorize, control and manage creation, modification and deletion of user identities and access to increase security and reduce administrative costs. • Host-based access control — manage access to the organizations' IT assets such as systems, files, directories and databases, including centrally defining and distributing policies that control access. • Web access management — secure Web content, regulate access and provide access to Web resources to provide centralized identity and access management. • Single sign-on — provide secure and combined access to applications and databases supporting multiple forms of authentication including passwords, tokens and biometric authentication. • Monitoring and auditing — ensures that all events and activities associated with identities and resources are monitored and tracked across the enterprise to allow auditors to know who created what identity and when, what the identity accessed, and when the identity was terminated.	
Network Configuration Management	

• The proposed Fault Management Solution must support integration with proposed help desk or trouble ticketing system in the following ways:
  ○ Creates tickets when requested by Fault Management operators
  ○ Automatically creates tickets based on alarm type
  ○ Provides a link to directly launch a Service Desk view of a particular ticket created by alarm from within the Network Operation console.
• Helpdesk ticket number created for associated alarm should be visible inside Network Operation Console .It should be integrated in a way that Helpdesk incident can be launched once clicked on ticket number for associated alarm from with in Network Operation Console.
• The proposed network fault management system should attach an asset identifier when submitting a helpdesk ticket. In case the asset is not found in the helpdesk database, it should be automatically created prior to submitting the ticket.
• The proposed NMS should provide unified workflow .	