वर्गीय आवश्यकताओं के लिए मानक

टीईसी ४८१००:२०२x

(सं: टीईसी ४८१००-२०२५ को अधिक्रमित करता है)

STANDARD FOR GENERIC REQUIREMENTS

TEC 48100:202x

(Supersedes No. TEC 48100:2025)

नेटवर्क मैनेजमेंट सिसटम्स

Network Management Systems (NMS)

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र

खुर्शीदलालभवन, जनपथ, नई दिल्ली–११०००१, भारत

TELECOMMUNICATION ENGINEERING CENTRE

KHURSHID LAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA

www.tec.gov.in

Release xx: Month, 202x

FOREWORD

Telecommunication Engineering Centre (TEC) is the technical arm of Department of Telecommunications (DOT), Government of India. Its activities include:

- Framing of TEC Standards for Generic Requirements for a Product/Equipment, Standards for Interface Requirements for a Product/Equipment, Standards for Service Requirements & Standard document of TEC for Telecom Products and Services
- Formulation of Essential Requirements (ERs) under Mandatory Testing and Certification of Telecom Equipment (MTCTE)
- Field evaluation of Telecom Products and Systems
- Designation of Conformity Assessment Bodies (CABs)/Testing facilities
- Testing & Certification of Telecom products
- Adoption of Standards
- Support to DoT on technical/technology issues

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

This GR specifies the Generic Requirements (GR) for Network Management System. The NMS provides Fault, Configuration, Accounting, and Performance, Security (FCAPS) of the Network and Service Management layers and other functionalities for the management of a Telecommunication network. The NMS integrates with the eMS for the management of the Network Elements (NE)

Contents

HISTORY SHEET

Sl. No.	GR No.	Particulars	Remarks
1.	Generic Requirement No. TEC/GR/IT/NMS-001/01/NOV 2015	Network Management System (NMS).	Ist Issue
2.	Standard for Generic Requirements No TEC 48100:2025 released in April 2025	Network Management Systems (NMS)	2nd issue

REFERENCES

S. No.	Document No.	Title/Document Name
1.	GB921	Enhanced Telecom Operations Map (eTOM), The Business Process Framework
2.	GB921D	Enhanced Telecom Operations Map (eTOM), The Business Process Framework Addendum D
3.	GB921DX	Enhanced Telecom Operations Map (eTOM), The Business Process Framework Addendum DX
4.	M.3000	ITU-T document Telecommunication Management Network
5.	M.3010	ITU-T document, Principles for a telecommunications management network
6.	M.3400	ITU-T document TMN management functions
7.	M.20	Maintenance philosophy for telecommunication networks
8.	M.3050	ITU-T document, Enhanced Telecom Operations Map (eTOM), Supplement 3: eTOM to M.3400 mapping
9.	X.800	Security architecture for Open Systems Interconnection for CCITT applications
10.	X.509	Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks
11.	TMF 814	Multi Technology Network Management IDL Solution Set

CHAPTER-1

1.0 INTRODUCTION

1.1 Telecommunication networks consist of multi-vendor and multi-technology equipments. In this environment there is a need to manage diverse equipment's from a central location to enable effective utilization of equipment and human resources. This leads to a need for deployment of a NMS at a central location which is capable of Operation, Administration and Management (OAM) of the diverse network elements.

1.2 Element Management Systems (eMS) acts as an interface to the network elements of a particular vendor and technology for performing functions of Fault, Configuration, Accounting, Performance Management and Security Management termed as FCAPS functions specific to the Network Elements (Resources).

1.3 The Generic Requirements for Management of equipment's belonging to a single technology (e.g. Router) from an OEM will be part of the eMS of the Generic requirements of the respective product.

1.4 NMS systems perform all the FCAPS functions in a multi-vendor environment and having a complete view of the network comprising of equipment of different functional layers.

1.5 This document is for an NMS system which is technology neutral i.e., NMS will interface with eMS systems of multiple vendors serving NEs of multiple technologies.

1.6 The structure of the NMS described in this document is based on the ITU-T standards as well as the TMN forum eTOM model. The document describes various functions in a layered architecture, both horizontally as shown in Figure-2 and vertically as per clause 2.1.6. This document includes Network Management Layer and Service Management Layer functions. There are optional functions of Service Management Functions and Business Management Functions (Customer Oriented Functions) also which may be decided by the

purchaser while procurement. Moreover the Security requirements of this document also include Security Information Event Management Functions requirement of which also may be decided by the purchaser while tendering.

1.7 An architecture diagram of network management using eMS and NMS system is given in Figure-1 below.

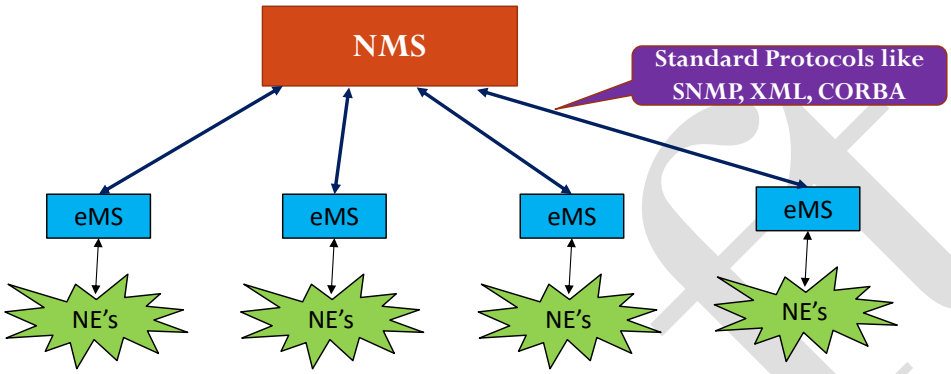

Figure-1: eMS and NMS architecture in a TSP network

2.0 DESCRIPTION

ITU-T and Telecom Management Forum develops standards for the Telecom Management Systems. The Telecom Management Forum has released the eTOM (Enhanced Telecom Operations Map) Standards (GB921). The ITU-T has standardized TMN Model vide recommendation M3010 and TMN Functions vide M3400. There is a convergence between these two standards as ITU-T has standardized the eTOM to M3400 Mapping vide recommendation M3050.

2.1 ITU TMN Model

The architecture of TMN model is defined in ITU-T Rec M.3010 and shown in Figure-2. TMN Model has been layered horizontally into five layers.

i. Business Management Layer (BML)
ii. Service Management Layer (SML)
iii. Network Management Layer (NML)
iv. Element Management Layer (EML)
v. Network Element Layer (NEL)

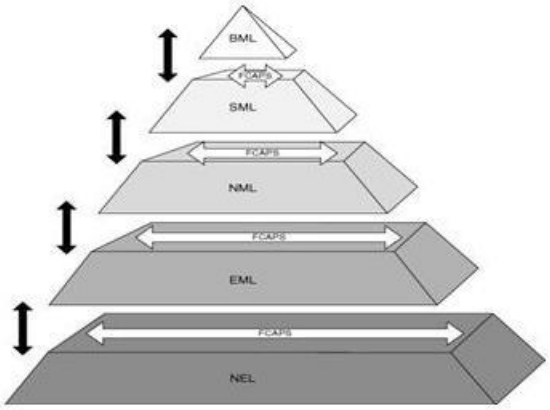

Figure-2: TMN Layered Architecture
(Ref. Figure-5 of M-3010 and Figure-1 of ITU-T M-3050)

2.1.1 Network Element Layer

It contains the actual Hardware or Network devices that are responsible for providing the various services. This layer includes the Switches, Routers, Transmission Systems etc. This layer communicates with EML for different operations like provisioning, activation, testing, etc. Network Elements provide all information/ functions required by the Element Management Layer.

2.1.2 Element Management Layer

This layer is responsible for managing the set of homogeneous network elements i.e. from a single OEM and having same technology. EML function provides data, receive commands and fetch the responses to the NML. EML helps in providing the FCAPS management functionality to the network elements on the basis of orders received from NML. All proprietary implementations shall end at EML itself. EML provides all information/ functions required by NMS over open interfaces as per standards.

2.1.3 Network Management Layer

All the network elements in the network are managed and controlled through Element Managers. The Network Management Layer shall provide the interface between the Service Management Layer and Element Management Layer. The Network Management layer is responsible for all the FCAPS functionalities.

2.1.4 **Service Management Layer (SML)**

This layer manages the service offered to the customers e.g. meeting the customer service levels, service quality, cost and time-to-market objectives etc. SML is the customer interface of the networks of any telecommunication service provider. It keeps all the customer records and other related information like SLA, services inventory, etc. Order Management, Orchestration, Middleware, Service Provisioning Management, User account management, QoS management, Inventory management, monitoring of service performance etc., are functions of the SML.

2.1.5 **Business Management Layer (BML)**

BML is responsible for high level planning, budgeting, goal setting, business decisions, business level agreements (BLAs), partner management, etc. This layer manages the overall business i.e. achieving the return on investments, market share, employee satisfaction, community and government goals etc. Customer Management, Fault Reporting, Customer Billing, Business Reporting Tools falls in this layer.

2.1.6 **FCAPS Functions**

The Management Functions are vertically divided across Fault Management, Configuration Management, Accounting Management, Performance Management and Security Management, known by the acronym FCAPS. The functions coming under the various verticals is given in the table below:

Fault Management	Quality Assurance, Alarm surveillance, Fault localization, Fault Correction, Testing, Trouble administration
Configuration Management	Network Planning and Engineering, Installation, Service Planning and Negotiation, Provisioning, Status and control
Accounting	Usage Measurement, Tariffing/pricing, Collections and Finance, Enterprise Control

Performance Management	Performance Monitoring, Performance Management Control, Performance Analysis
Security Management	Prevention, Detection, Containment and Recovery, Security Administration

2.2 TMF forum eTOM Model

The Business Process Framework (eTOM) standards released by Telecom Management Forum (TMF) defines a library of business processes in a hierarchical process decomposition. At the overall enterprise level (Level 0) it captures process descriptions, inputs and outputs. At each subsequent level (Level 1, 2 and sometimes even 3 or 4) other key elements of the process are documented. The processes described under the eTOM model are about the overall management system which may include many management systems like eMS, NMS, OSS/BSS systems etc. The processes required in the NMS perspective are further specified in section 2.5 of this document.

2.2.1 eTOM Level-0, Level-1

2.2.1.1 Level 0 and Level 1 process areas from the Business Process Framework are shown in the Figure-3. At the overall conceptual level, the Business Process Framework is viewed as having the following three major (Level 0) process areas given in Figure-3:

a) Strategy, Infrastructure & Product covering planning and life-cycle management

b) Operations covering the core of operational management

c) Enterprise Management covering corporate or business support management

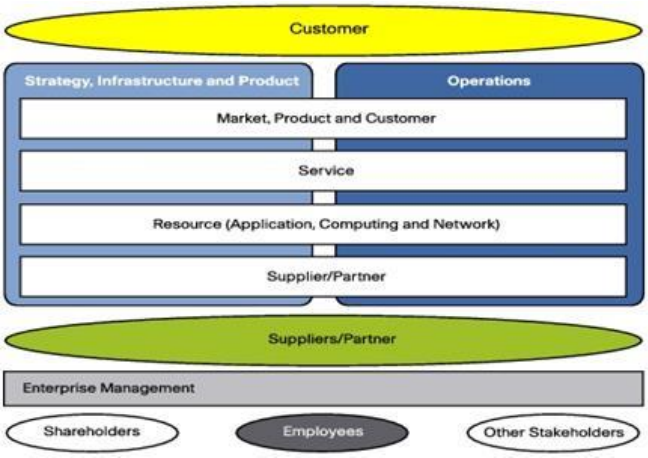

Figure-3: eTOM Level-0 Process

(Ref: Figure 1.1 of GB921 Enhanced Telecom Operations Map (eTOM) the Business Process Framework by Telecom Management Forum)

2.2.1.2 The Business Process Framework contains seven end-to-end vertical Level 1 process groupings in the areas of Strategy, Infrastructure and Product and Operations. These vertical groupings of processes focus on end-to-end activities and each grouping includes processes involving customers, supporting services, resources and suppliers/partners. These vertical groupings can be thought of as a lifecycle when seen from left to right in Figure-4.

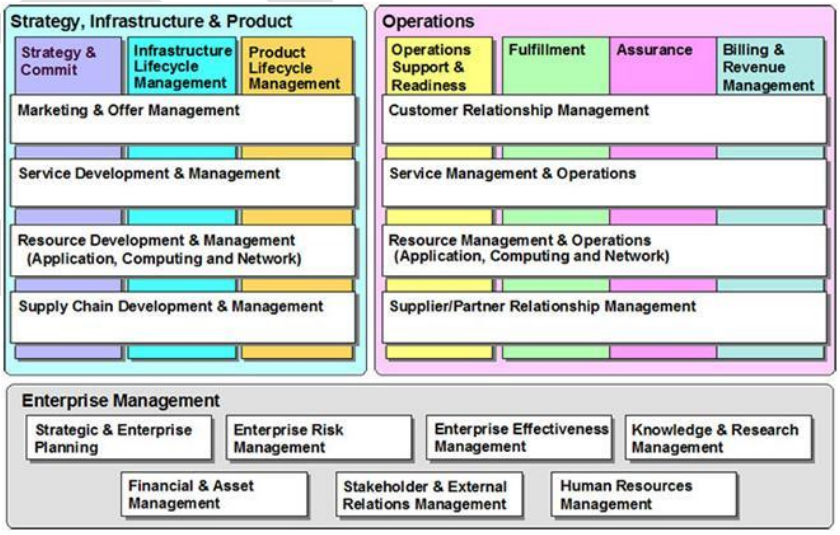

Figure-4: eTOM Level-1 Business Process Framework

(Ref: Figure 1.2 of GB921 Enhanced Telecom Operations Map (eTOM) the Business Process Framework by Telecom Management Forum)

2.2.1.3 The Strategy, Infrastructure & Product process area in Figure- 4 contains the “back-office” processes. They enable, support and direct the work done during Operations

2.2.1.4 The focal point of the Business Process Framework is in the area of Fulfillment, Assurance and Billing. These vertical groupings contain the core processes related to customer operations.

2.2.1.5 The fourth vertical grouping in the operations area is Operations Support & Readiness (OSR). Its processes focus on the support and automation of customer operations

2.2.1.6 The horizontal groupings represent major programs or functions that cut horizontally across an enterprise's internal business activities. For example, customer relationship management includes business processes in marketing, ordering, billing, after-service support and follow-on sales. Where a vertical process grouping and a horizontal process grouping intersect across the map, further process detail can be applied in either that horizontal or vertical context, according to the user's needs.

2.2.2 **eTOM Level-2 end to end process breakdown**

2.2.2.1 Within the Business Process Framework, processes are decomposed to the lowest possible level. The operations vertical is the focus area coming under management systems and its Level-2 breakup is shown in Figure-5.

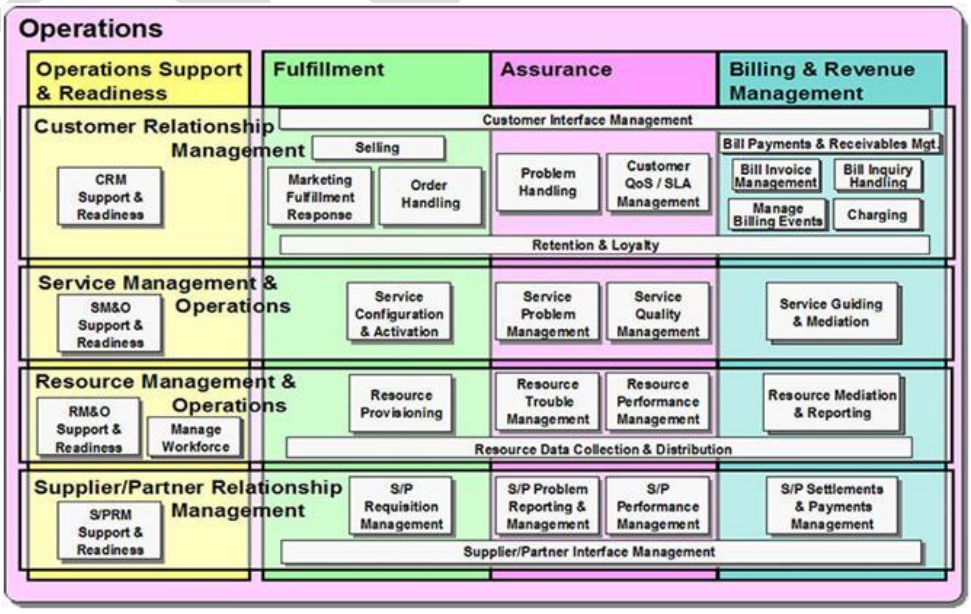

Figure-5: Level 2 Breakdown of Operations Business Process
(Ref: Figure A.1 of GB921 Enhanced Telecom Operations Map (eTOM) the Business Process Framework by Telecom Management Forum)

2.2.2.2 Operations includes processes that support customers, network operations, and management. This also consists of sales management and supplier/partner relationships management

2.2.2.3 Fulfillment is responsible for delivering products and services to the customer. This includes order handling, service configuration and activation, and resource provisioning

2.2.2.4 Assurance consists of proactive and reactive maintenance activities, service monitoring (SLA or QoS), resource status and performance monitoring, and troubleshooting. This includes continuous resource status and performance monitoring to proactively detect possible failures, and the collection of performance data and analysis to identify and resolve potential or real problems

2.2.2.5 Billing collects usage data records (accounting), various rating functions, and billing operations. This includes production of timely and accurate bills, providing pre-bill use information and billing to customers, processing their payments, and performing payment collections. A detailed description of each layer can be found in the TMF's eTOM document (GB921).

2.2.2.6 Resource Management & Operations (RM&O) is responsible for application, computing, and network resources. It includes Resource Trouble Management, which performs fault monitoring and management functions, such as processing device notifications, root cause analysis, and fault reporting. Resource Performance Management monitors, analyzes, and reports performance data from the devices. A common RM&O function between assurance and billing is Resource Data Collection and Processing. It gathers and distributes management data between devices and service instances.

2.2.2.7 Service Management & Operations (SM&O) consists of Service Problem Management and Service Quality Management in the assurance section. These are responsible for monitoring, analyzing, and controlling operational services, as well as detecting, analyzing, and localizing service problems

2.2.2.8 In the billing area, Service and Specific Instance Rating correlates service events and converts them into a specific format.

2.3 eTOM-M3400 Mapping

The synergy between the standards of ITU-T and the TMF has been brought by ITU-T through its recommendation M.3050 where a mapping has been recommended between the ITU-T Functional Areas as per M.3400 and the eTOM Level-2 processes.

2.4 Generalised Model

The Operations area is as per the eTOM model given in Figure-5 and the FCAPS functionality are as per the M.3400. Based on these standards, a generalised model for the various building Blocks of Telecom Management System is given in Figure-6. The various functions in the M.3400 Model are performed by the eMS, NMS and OSS/BSS Systems in a Telecom Network. However, eTOM model goes into additional functionalities in Strategies, Infrastructure & Product and Enterprise Management segments which are performed by Enterprise Resource Planning [ERP] systems. The role of ERP systems is not dealt with in this document.

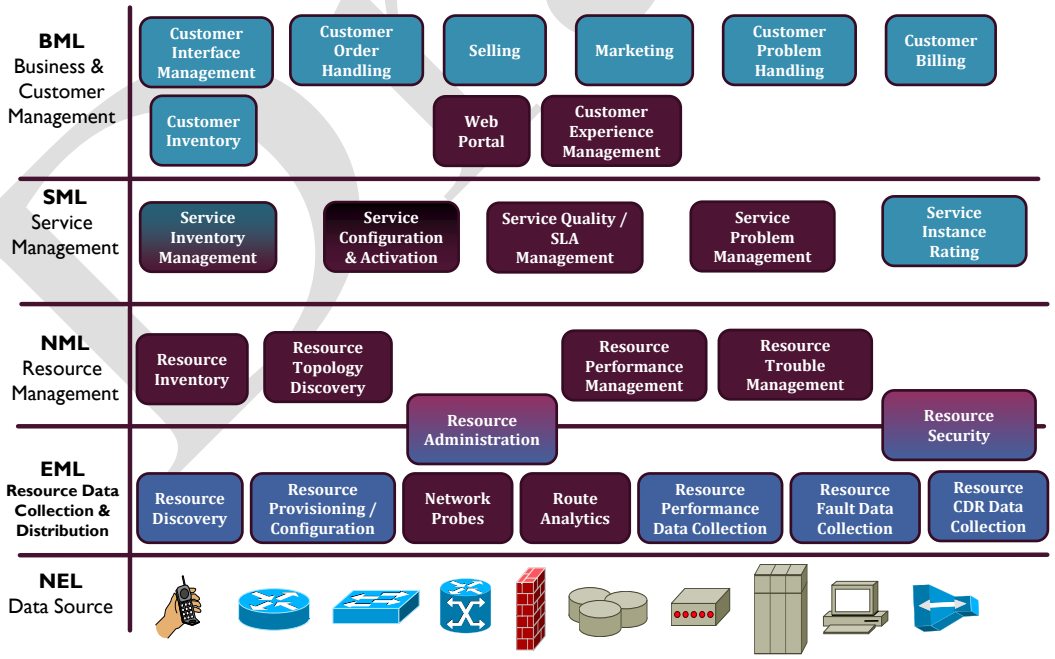

Figure-6 TMN/ eTOM Building Blocks for TMN

2.4.1 Resource refers to a full or part of a network element (e.g. Router), application (e.g. Software) or compute (e.g. Server) or logical resources (e.g. bandwidth) having a specific role in the Telecom network.

2.4.2 The functions of the EML namely Resource discovery, Resource provisioning / configuration, Resource performance data collection, Resource Fault data collection and Resource CDR Data collection are performed by the eMS. Some of the Resource Administration and Resource Security features are also performed by the eMS. The EML functions of Network Probes and Route Analytics could be part of the eMS or NMS depending upon the purchaser's requirement.

2.4.3 The overall system map is given in Figure-7. All the functions described in the figure covering the EML, NML, SML and BML Layers in a telecom network are performed by three systems namely the OSS/BSS System (Or Customer Relationship Management Systems), NMS System and eMS Systems. In certain deployments there is a separate provisioning system, which performs the provisioning functions which is part of the NMS and OSS/BSS system. However this document covers only the provisioning aspects related to NMS systems.

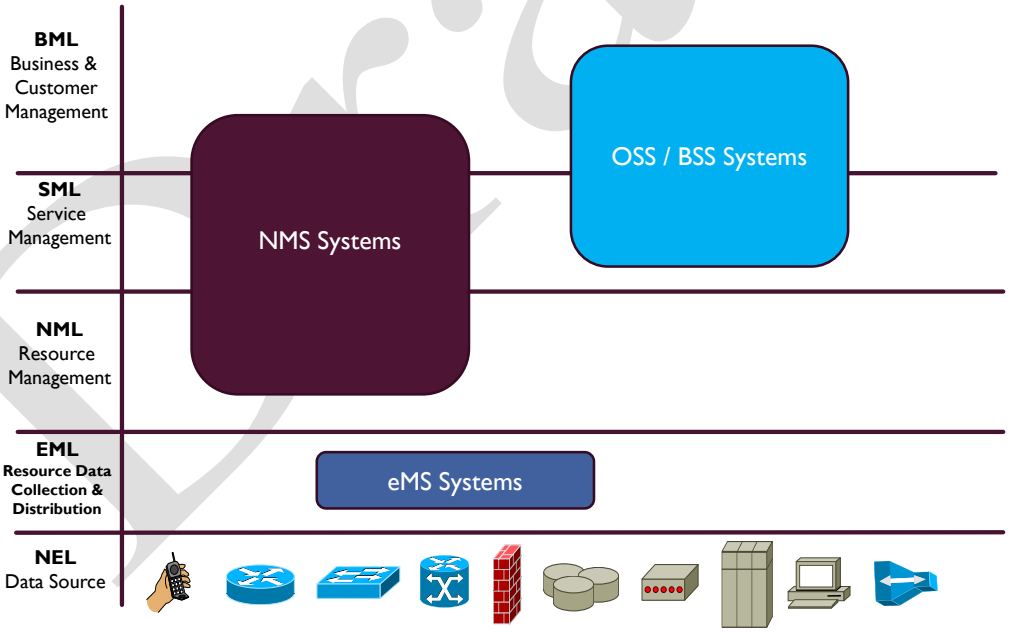

Figure-7 Overall system Map

2.5 Functions to be performed by the NMS

The NMS functions include the following as per Figure-6. This is based on the horizontal and vertical layered architecture as in Figure-2 and clause 2.1.6 respectively. However, actual implementation may be as per the requirements of the user especially in respect of SML and BML.

a) NML Functions
   i) Resource Administration
   ii) Resource Inventory
   iii) Resource Topology Discovery
   iv) Resource Performance Management
   v) Resource Trouble Management
   vi) Resource Security
b) SML Functions
   i) Service Quality / SLA Management
   ii) Service Problem Management
   iii) Service Configuration & Activation
c) BML Functions
   i) Customer Experience Management
   ii) Web Portal
d) EML Functions
   i) Route Analytics
   ii) Network & Device Probes

3.0 FUNCTIONAL REQUIREMENTS :

The Management Functions to be supported by the NMS described in this section consist of requirements as per ITU-T M.3400. Functions of NMS are based on FCAPS (Fault, Configuration, Accounting, and Performance & Security) which are known as Function Groups. The NMS shall support the following Management Function groups. These Function Groups are further subdivided into Management Function sets which are included under individual function group. The implementation of management set can be done by a single device/software or with multiple devices/software.

3.1 Fault Management:

Fault management is the set of functions that detect, isolate, and correct malfunctions in a telecommunications network, compensate for environmental changes, and include maintaining and examining error logs, accepting and acting on error detection notifications, tracing and identifying faults including self-faults, correcting faults, reporting error conditions, and localizing and tracing faults by examining and correlating the underlying database information.

3.1.1 Resource Trouble Management

3.1.1.1 It is expected that the eMS carries out the first level of alarm collection and filtration and pass on the filtered alarms to the NMS.

3.1.1.2 The NMS shall define the Alarm Policy to the extent that which event shall raise an alarm of urgent nature or other different nature etc. NMS shall assist eMS to categorize an alarm into various categories. It shall assist the eMS in defining the filtering rules for the alarms and events for individual Network Element.

3.1.1.3 The NMS shall carry out the analysis of the events in the networks and shall correlate the events to determine the root cause based on correlation and next level of filtering of alarms. The NMS shall assist in defining the policy for carrying out the root cause analysis. The NMS

shall have provision to add manual root-cause analysis after the user has carried out the same to its Knowledge database in an automatic manner.

3.1.1.4 The NMS shall present only the root cause to user as an alarm. It shall be configurable whether to present all alarms along with the root cause or some selected alarms only.

3.1.1.5 The NMS shall have provision for modification of alarm status from urgent to non-urgent or to be acknowledged to acknowledged etc.

3.1.1.6 The NMS shall define the destination of alarm reporting. It could be a centralized location for all the alarms or it could vary based on type of alarm. The NMS shall also support reporting of critical alarms to a non NMS location in the form of e-mail message, SMS, etc.

3.1.1.7 The NMS shall detect the failure of a Network Element and report it to a NMS or non NMS location which is configurable through an alarm or message (e-mail, SMS etc.).

3.1.1.8 The NMS shall support presentation of alarms summary on demand or at configurable intervals to a NMS and/or non NMS location.

3.1.1.9 The NMS shall have provision for customizing the events trigger by alarm.

3.1.1.10 The NMS shall support visual indication for alarms in form of an Alarm Panel or on NMS user screen with option of audio indication.

3.1.1.11 All alarm related information (e.g. alarm receive-time start-time, clear-time, acknowledge-time etc.) shall be logged with time and date-stamped.

3.1.1.12 The Alarm/event shall be logged to system file which shall not be possible to be modified except for the size of the file.

3.1.1.13 The NMS shall be able to display and print the detailed alarm logs with location, time and date of occurrence, duration of the faults, and event history information.

3.1.1.14 The NMS shall show operators using the NMS terminals precisely which network users, customers or processes are affected by a fault.

3.1.1.15 The NMS shall be able to display alarm and events specified by the following criteria:

a) Alarm types

b) Time interval

c) Vendor

d) Technology

e) Customer

f) Service

g) Location

3.1.1.16 The NMS shall allow escalation of alarms in case the same is not attended within a configurable time frame. Escalation shall increase the severity, list them in a separate group, raise it to next level of administrator, etc.

3.1.1.17 The NMS shall have provision for determination of the fault in a network. It shall have the capability of fault localization upto a part of the network (e.g. up to a single or a group of NEs).

3.1.1.18 The NMS shall have provision to invoke the diagnostic tools via eMS and eMS shall run it locally.

3.1.1.19 The NMS shall have provision for definition of the fault localization policy which shall be used to provide the assistance to the user involved in fault localisation or running the diagnostics on a part of the network or Network Element up to port level. It shall have a user upgradable database to add a new rule to the policy.

3.1.1.20 The NMS shall automate the complete procedure of any particular type of testing using macros.

3.1.1.21 The NMS shall have control over the NEs over which the tests are being executed from the NMS through the eMS. Ideally no Local Craft Terminal shall be able to execute any operation once the test is being run on a NE under the control of NMS. However the user shall be able to configure the priority of local craft terminal / eMS over NMS and vice-versa for any given set of commands.

3.1.1.22 The NMS shall correlate the test results and identify any fault on the basis of the correlation results.

3.1.1.23 The NMS shall be able to place a NE, which may be alarmed or non-alarmed, into maintenance mode for purposes of maintenance, troubleshooting and/or repair. Alarms received from the NE which are in maintenance mode shall be ignored.

3.1.1.24 The NMS shall support priority messages to interrupt input or output message of lower priority.

3.1.1.25 AI / ML Capabilities of NMS: Purchaser may specify the any or all of the following AI/ML capabilities required in the NMS while making procurement as mentioned under clause 10.3.

i. NMS shall support Alarm correlation by leveraging AI/ML capabilities to quickly isolate network issues and identify root cause analysis with minimal human intervention or manual rule-based policy configurations to determine the underlying cause of a fault or an issue, propose/recommend corrective actions to resolve the fault/issue.

ii. NMS shall leverage machine learning algorithms to correlate performance management data and alarms to identify the root cause of network issues thereby reducing the time taken for root cause analysis.

iii. NMS shall use machine learning algorithms for anomaly detection, enabling the system to identify unusual patterns indicative of potential issues.

iv. NMS shall dynamically adjust to the changing network conditions to avoid false positives.

v. NMS shall provide predictive analytics to forecast potential incidents based on historical and real-time data.

vi. NMS shall incorporate feedback loops to continuously improve the accuracy of root cause analysis.

vii. NMS shall leverage AI/ML capabilities for Performance Optimization and analyse network performance data, including traffic patterns, bandwidth utilization, and latency metrics, to optimize network configurations and resource allocation.

3.1.2 Service Problem Management [Optional Requirement]

Service Problem Management refers to functions that respond immediately to group of customer-affecting service problems or failures in order to minimize their effects on a group of customers, and to invoke the restoration of the service, or provide an alternate service as

soon as possible automatically or through manual commands based on other conditions like network configurations, availability of resources, capability of underlying infrastructure etc.

3.1.2.1 The NMS shall support the testing of the services through the respective eMS. It shall be able to carry out the service testing for group of customers.

3.1.2.2 The NMS shall initiate and manage service alarm event records.

3.1.2.3 The NMS shall perform service alarm event notification localization analysis.

3.1.2.4 The NMS shall correlate and filter service alarm event records.

3.1.2.5 The NMS shall report service alarm event record status changes to other processes.

3.1.2.6 The NMS shall manage service alarm event record trouble conditions.

3.1.2.7 Service alarm event notification analysis encompasses the identification of the service alarm event in terms of reporting entity and nature of the service alarm event.

3.1.2.8 The NMS shall analyze the service alarm events based on a number of criteria and then suppress redundant, transient or implied service alarm events by means of filtering and correlation.

3.1.2.9 The NMS shall generate a trouble ticket on any configurable event of service fault/degradation.

3.1.2.10 The NMS shall provide the management of trouble ticket status. The status changes like the trouble ticker has been attended or is being attended etc., shall be available in the status report.

3.1.2.11 The NMS shall provide interrogation of trouble ticket information by the users or the BML over standard North Bound interface.

3.1.2.12 The NMS shall create a new service problem report as a result of service alarm event notification analysis, and subsequent creation of new service alarm event records, undertaken by the survey & analyze service problem processes.

3.1.2.13 If the service problem report is created as a result of a notification or request from processes other than the service problem processes, NMS shall create service problem report responsible for converting the received information into a form suitable for the service problem

management processes.

3.1.2.14 The NMS shall report/notify the opened trouble ticket to the pre designated location as per the policy configured.

3.1.2.15 The NMS shall report service problem processes to monitor the status of service problem reports, provide notifications of any changes and provide management reports.

3.1.2.16 The NMS shall also processes record, analyze and assess the service problem report status changes to provide management reports and any specialized summaries of the efficiency and effectiveness of the overall service problem management process.

3.1.2.17 The NMS shall diagnose service problem processes to identify the root cause of the specific service problem.

3.1.2.18 The NMS shall verify whether the service configuration matches the appropriate product features and perform diagnostics against the specific services;

3.1.2.19 The NMS shall run tests against the specific services and start & stop audits against specific services

3.1.2.20 The NMS shall also schedule routine testing of the specific services

3.1.2.21 The NMS shall correct & resolve service problem processes to restore the service to a normal operational state as efficiently as possible. Based on the nature of the service failure leading to the associated service alarm event notification, automatic restoration procedures shall be triggered.

3.1.2.22 The NMS shall give customizable alarms triggered to alert the appropriate personnel to either take action or raise service incidents or both allowing them to focus on the most critical issues immediately.

3.1.2.23 Depending on the nature of the specific service failure, NMS shall re-assign services or re-configure service parameters as per need automatically or through manual commands based on other conditions like network configurations, availability of resources, capability of underlying infrastructure etc.

3.1.2.24 The NMS shall track & manage service problem processes to ensure that testing, repair and restoration activities are assigned, coordinated and tracked efficiently, and that escalation is invoked as required for

any open service problem reports

3.1.2.25 The NMS shall assist to schedule, assign and coordinate repair and restoration activities and generate the respective resource problem report. NMS shall also assist in necessary tracking of the execution progress and shall modify information in an existing service problem report based on assignments.

3.2 Configuration Management :

Configuration Management provides functions to exercise control over NE's as well as identify, collect data from and provide data to NEs. Configuration Management shall support the following function set groups.

3.2.1 Resource Inventory :

3.2.1.1 The NMS shall provide the complete view of the network elements and the interconnecting links.

3.2.1.2 The NMS shall be able to discover and keep the device information up to logical interface level.

3.2.1.3 The NMS shall be able to store and/or display all the devices based on their make & model.

3.2.1.4 The NMS shall be able to keep track on any change in the network inventory reported chronologically.

3.2.1.5 The NMS shall provide the inventory information to the OSS/BSS so that the OSS/BSS is able to create and activate a service to the customer automatically. This shall also assist OSS/BSS in providing the network inventory to which the OSS/BSS shall add the customer identification and maintain this information in its database.

3.2.1.6 The NMS shall be able to generate report based on the available device inventory up to logical interface level.

3.2.1.7 The NMS shall be able to generate reports based on changes made in the Network Inventory.

3.2.2 Resource Topology discovery

3.2.2.1 The NMS shall be able to determine the layout of a particular network with network elements (Resources) in a Geographical map.

3.2.2.2 The NMS shall auto discover the network elements and the links to include them in the visual/graphical map of the domain. NEs need to support this feature (auto discovery) through their eMS otherwise NEs shall introduce (register) themselves to the NMS.

3.2.2.3 The Visual Maps shall display the elements and the links in different colour depending upon the status of the links. It is preferable that green colour for healthy and amber/yellow colour for degraded condition and red for unhealthy condition is used.

3.2.2.4 The NMS shall indicate the absence or presence of any physical module in hardware elements. It shall also indicate the usage of module i.e. how many ports are in use, which interface is in use and which are free to be used etc.

3.2.2.5 The NMS shall provide the ability to drill down to the individual element, then to subsystem, then to card and then to port level configuration template from the domain Map by clicking on the icon of the network element.

3.2.3 Service Configuration and Activation

Provisioning consists of procedures which are necessary to bring an equipment into service, excluding installation. Once the unit is ready for service, the supporting programs are initialized via the NMS. The state of the unit (e.g. in-service, out-of-service, standby, reserved) and selected parameters may also be controlled by provisioning functions. It is expected that all these operations are carried out on the NE's through their respective eMS's through standard open interface. Provisioning shall include the following functions

3.2.3.1 The NMS shall support request for, and report the assignments of resources, as appropriate. These resources may be NEs, a group of NEs, or logical resources such as bandwidth or service logic programs.

3.2.3.2 The NMS shall provide availability status of resources, selection and assignment of those resources, requests for the resources to change service state requests for network resources reservation (to eMS) and collect response regarding selected resources and the associated service features. It shall support requests for selection and assignment

of resources and service features that meet any designated selection criteria.

3.2.3.3 The NMS shall support confirmation of execution of all requested actions. It shall support pending reports as appropriate.

3.2.3.4 The NMS shall provide access to information concerning NE resources that are assigned to services or that are currently available for assignment. It shall monitor utilization levels of resources and sends notifications when utilization exceeds configurable thresholds. It shall respond to requests for utilization information.

3.2.3.5 The NMS shall support loading of software to activate service-specific features in NE components such as the downloading of software features to line cards at the time of activation of service. Loading includes support of reporting the results of testing that the load is successful and of back-out of the software features if the load is not successfully completed.

3.2.3.6 The NMS shall provide information about individual NE connections and the removal of NE connections if end-to-end connections cannot be completed. It shall support notification of changes that result from differences between assigned and installed NE configurations

3.2.3.7 The NMS shall support I/O logic command handling tool to perform various tasks such as configuration, functional change, administration, creation, deletion etc., of the Network Data which shall be residing at NMS and also in the network elements, in a centralized operation and maintenance environment

3.2.3.8 The NMS shall support configuration of the various network elements like creating, viewing, and editing. The NMS shall also store the configurations of the network elements from where it can be retrieved in case of failure.

3.2.3.9 The NMS shall back-out from an operation if not completed successfully i.e. the NMS shall delete all creation/modification from all involved network elements for all the commands which has been carried out as part of a task which was not completed successfully and involved many network Elements and commands. However clear alarm shall be generated in such cases where it may not be able to 100%

back-out.

3.2.3.10 The NMS shall execute any command at any time by attaching a time tag to the command and it shall be executed when the Network real time matches the time tag. It shall be possible to define both time and date. If no date is mentioned, the command shall be executed daily at the time indicated.

3.2.3.11 The NMS shall provide access to status and shall receive requests to change status of network and its components.

3.2.3.12 The NMS shall provide status of service resources and carry out requests for transitions after determining the legality and effect of requested state changes.

3.2.3.13 Automatic notification of change of state may be initiated by the NE such as a change from "enabled" to "disabled" in the event of a failure.

3.2.3.14 The NMS shall suggest through alarms/notifications for the exclusion of faulty equipment from operation. After exclusion, NMS may assist in rearranging equipments or re-routing of the traffic.

3.2.3.15 The NMS shall enable the entry of a proposed configuration in order to automatically analyze the feasibility of that design before implementing it.

3.2.3.16 The NMS shall aid in determining the correctness of the parameters before they are committed to a command/operation. If the operator gives/selects wrong parameters, the NMS shall prompt the user about the wrong value.

3.2.3.17 The NMS shall support software download to the NE. Loading includes initialization and testing that the loading is successful and roll-back of the software if the loading is not successfully completed.

3.2.3.18 The NMS shall provide a single GUI for configuration management across heterogeneous devices from multiple vendors.

3.2.3.19 The NMS shall support discrete configuration file management

3.2.3.20 The NMS shall maintain an active archive of configuration files for the managed network devices with modifications made in them.

3.2.3.21 The NMS shall support recover back feature in case all the components involved in configuration are not able to be configured due to any reason.

3.2.3.22 The NMS shall provide a comprehensive audit of network changes reported chronologically.

3.2.3.23 The NMS shall maintain records of modifications in the areas of hardware and configurations.

3.2.3.24 The NMS shall buffer recent commands and be re-displayed, re-edited and re-issued on request.

3.2.3.25 The NMS shall support macro command/subroutine facility to carry out the same kind of operation on a group of interfaces by a single command. It shall be possible to generate a macro program which integrates the various operations in an intelligent sequence to carry out complex tasks of creation, modification and deletion of entities like Trunks, Software control of Elements etc. It shall also support import of Macro programs/routines from a program written as a text file from an external storage media.

3.2.3.26 It shall be possible through a single Man-Machine Command to obtain a list and the total number of equipment of a particular domain in a state (e.g. In-service, blocked etc.).

3.2.3.27 Where several man-machine terminals are in use on a single network element a mechanism shall be available to avoid clashes of command.

3.2.3.28 The execution of any command shall not result in malfunctioning or/and over loading of the network.

3.2.3.29 Command errors detected by the network shall be indicated by the output of error messages.

Note: Following NMS requirements are applicable to specific technologies which may be considered depending upon the actual network requirement.

3.2.3.30 The NMS shall assist the user in verifying the connectivity from one end to other end in applicable technologies before the operation is carried out on multiple Network Elements.

3.2.3.31 The NMS shall support to assign priority services for restoration in the event of a catastrophic failure, e.g. hospitals, police and emergency services etc., in applicable technologies.

3.2.3.32 The NMS shall carry out the cross-connections to be established in NEs or groups of NEs in applicable technologies.

3.2.3.33 The NMS shall allow for connection with different NEs or network interfaces through respective eMS's to establish an end-to-end circuit connection in applicable technologies.

Note: Following NMS requirements are customer oriented which may be considered for NMS for managing services to end customers.

3.2.3.34 The NMS shall allow the design of network, based on customer location, requested service features, etc. It shall also determine the most efficient routing based on generic criteria for routing, such as traversing the least number of nodes, and customer specific criteria, such as alternate path routing in case of applicable technologies.

3.2.3.35 The NMS shall support requests for a directory address e.g. telephone number, IP address, etc., as applicable.

3.2.3.36 The NMS shall support requests that the specified service and/or feature(s) be activated, changed, or deactivated as a result of the negotiated customer solution.

3.2.3.37 The NMS shall provide access to a database for the logging and tracking of service requests to ensure that all requests for service are met in a timely manner.

3.2.4 Provisioning Management

These functions may be performed by the NMS itself or through an integrated Provisioning Management system/module.

3.2.4.1 The NMS shall support single GUI based provisioning system which provisions network and end user services from a single screen.

3.2.4.2 The NMS shall support consistent and simplified service activation methodology across services.

3.2.4.3 The NMS shall simple network / service provisioning for all the services.

3.2.4.4 The NMS shall maintain a detailed association of the resources for each of the services deployed.

3.2.4.5 The NMS shall maintain a real-time database of the existing customer / services / resources i.e. NE's/Slot/Port – the object chain involved in providing services.

3.2.4.6 The NMS shall handle end-to-end service provisioning from one single point of provisioning platform regardless of whether the system manages a single family or different family products.

3.2.4.7 The NMS shall provide GUI-based features for all applications such as system configuration, service provisioning etc.

3.2.4.8 The NMS shall be configurable from the GUI for all services.

Note: Following NMS requirements are applicable to specific technologies which may be seen depending upon the actual network requirement.

3.2.4.9 NMS shall maintain a complete inventory of end customers being served and automatically associate services against customers in this list for applicable technologies

3.2.4.10 The NMS shall automatically capture all the configurations from the existing network and make an inventory of end customers out of it for applicable technologies.

3.3 Performance Management

Performance Management provides functions to evaluate and report upon the behaviour of telecommunication equipment and the effectiveness of the network or network element. The NMS shall gather and analyse statistical data for the purpose of monitoring and correcting the behaviour and effectiveness of the network, NEs or other equipment through the respective eMS's. The NMS shall aid in planning, provisioning, maintenance and the measurement of quality.

3.3.1 Resource Performance Management

3.3.1.1 The NMS shall be able to establish Performance Monitoring (PM) policy such as the values of threshold settings and schedules for data collection for specific kinds of circuits. These settings are to be applied during activation of such circuits. Different policies are likely to be

created for special service circuits of various kinds, for message circuits, and for facilities.

3.3.1.2 The NMS shall report the root-cause of PM threshold crossing alerts and other PM events.

3.3.1.3 NMS shall provide aggregated and correlated end-to-end current and history of PM information to detect and aid in the localization of network faults and impairments. It shall also provide access to trending information, which supports the extrapolation of historical data to predict future performance and to identify persistent or worsening impairments.

3.3.1.4 The NMS shall report of trends that are detected by processing the historical data of an NE or group of NEs. The NMS shall be able to store historical data of at least past three months.

3.3.1.5 The NMS shall support the reporting of results of the continuous detection, collection, and reporting of performance primitives, i.e. data or measurements, associated with a transmission, traffic, or service entity.

3.3.1.6 The NMS shall be able to store all the performance and traffic statistics for at least 3 month. It shall also be possible to generate daily, weekly, monthly reports for the individual element as well as complete domain. The report generation shall be supported for text and graphic reports.

3.3.1.7 The NMS shall carry out the systematic Health Monitoring of the elements of the Network. It shall be possible to check on the health of the card of any network element.

3.3.1.8 The NMS shall provide recommendations for performance improvement including corrective actions.

3.3.1.9 The NMS shall provide traffic forecasting based on history.

3.3.1.10 The NMS shall provide reports to characterize end-to-end performance of dedicated digital networks, which includes Network Interface-to-Network Interface, and Network Interface-to-Inter-Network Interface (point of termination), in relation to long-term (i.e. 30 or more days) accuracy and availability objectives.

3.3.1.11 The NMS shall monitor NE quality and availability performance parameters in order to support service assurance and/or service

offerings.

3.3.1.12 The NMS shall monitor network performance quality and availability in order to support service assurance and service offerings.

3.3.1.13 The NMS shall monitor if the performance data, such as a count, has been compromised or invalidated by re-initialization (for example, the resetting of a clock), or internal equipment failure

3.3.1.14 The NMS shall support scheduling of the Performance measurement, collection, storage and transfer of the performance statistics. It shall also support presentation of the performance statistics in graphical and text mode as and when requested and at repeated interval automatically.

3.3.1.15 The NMS shall also provide real-time data/statistics on all the network elements under maintenance-mode or in fault state in a single command and in a single console

3.3.1.16 It shall be possible to get display and print-out of the measurement results on demand at any time during the measurement period.

Note: Following requirements are specific to management of traffic oriented networks.

3.3.1.17 The NMS shall provide graphical display of percentage of Link utilization and the network element resource in applicable technologies. The traffic observation shall indicate, for each type of service and for each type of call processing / call handling unit the number of units installed, number of units in service, call attempts, calls processed, calls answered etc., in applicable technologies.

3.3.1.18 The NMS shall have plans for anticipated conditions of congestion (for example, burst traffic that are typical to a region and focused demands that result from promotions and surveys) as applicable.

3.3.1.19 The NMS shall provide current traffic status information of a sub network and its major components in applicable technologies.

3.3.1.20 The NMS shall report current performance measurements of the traffic being offered and carried by one or more NEs. These measurements relate to the assessment of the current performance of the network and

the traffic being offered and carried.

3.3.1.21 The NMS shall provide for, at least the following types of supervision in applicable technologies:

a) Automatic detection of congestion on the incoming routes, the final backbone routes, the signaling devices and control units.
b) Continuous supervision of Power Supply Units (PSU).
c) Continuous supervision of tones for levels, etc.
d) Automatic detection of any abnormalities in processing.
e) Detection of trunks that are incapacitated for accepting traffic.
f) Supervision of automatically blocked devices to ensure that conditions leading to traffic overload are not created.

3.3.1.22 The NMS shall allow creating and modifying routing patterns if applicable to relieve network congestion due to unusually high offered load, an unusual distribution of offered load, or one or more unprotected faults.

3.3.1.23 The NMS shall be able to create and manage the schedule for traffic measurement and other data that support traffic measurements and traffic control.

3.3.1.24 The NMS shall provide traffic exception analysis in order to detect and report on exceptional conditions due to unusual demand or reduced capacity. It shall provide sufficient supporting information to reveal the extent of congestion and to support a determination of remedial action.

3.3.1.25 The NMS shall provide traffic capacity analysis to estimate the level of offered traffic that can be carried by the current resources at the desired level of QOS wherever applicable.

3.3.1.26 The NMS shall provide following analysis for individual NE in applicable technologies:

a) NE(s) performance characterization
b) NE(s) traffic exception analysis
c) NE(s) traffic capacity analysis

3.3.1.27 The NMS shall be capable of measuring the slips on interfaces, designated through Man-Machine Commands in applicable technologies.

3.3.2 **Service Quality / Service Level Agreement [SLA] Management [Optional requirement]**

The NMS shall perform the following Service Quality / SLA Management Requirements. These functions may be performed by the NMS or through an integrated SLA Management system.

3.3.2.1 The NMS shall have features to enable service quality management

3.3.2.2 The NMS shall provide customer service performance summary by evaluating the performance of a particular transport service or group of services.

3.3.2.3 The NMS shall be able to retrieve, generate and print reports and graphs on Service Performance Management data based on real time, time intervals, daily, weekly, monthly, annually or specific period, for all NEs and its resources by using the built-in report capabilities of the System.

3.3.2.4 The NMS shall enable correlation of Service Performance Measurement with the fault management module with the following:

a) Customer profile
b) Customer services
c) Logical network infrastructure
d) Physical network infrastructure
e) Class of Service / Type of Service

3.3.2.5 The NMS shall provide the monitoring and tracking tool for services with Service Level Agreement (SLA) for Service Assurance Management

3.3.2.6 The NMS shall also provide automated calculation of service achievement, management and operational report for SLA and Non-SLA services.

3.3.2.7 The NMS shall have a built-in report authoring tool to customize Service performance reports.

3.3.2.8 The NMS shall provide full visibility in real time on service quality and experience through consolidated services views.

3.3.2.9 The NMS shall maintain service quality by collecting key performance indicators (KPIs) from different sources such as network performance and fault management, network surveillance or passive probes, active

probes, customer experience applications, traffic management, as well as trouble ticketing systems.

3.3.2.10 The NMS shall use different KPIs to compute service key quality indicators (KQIs) according to resource and service dependencies.

3.3.2.11 KQIs shall be made available in a dashboard to allow operations to immediately detect issues damaging the user experience.

3.3.2.12 The NMS shall provide consolidated, synthetic views, which provide an “at-a-glance view” of the services and the associated user experience across different services, in terms of service availability, accessibility, retain-ability, security, and support QoE indicators.

3.3.2.13 The NMS shall allow to see the service quality, in terms of availability, accessibility, retainability, supportability, and security as well as the associated specific KQIs.

3.3.2.14 The NMS shall provide a web interface for the customers to login and verify their SLA related parameters.

3.3.2.15 The NMS shall provide visibility of the service quality delivered across the Network together with the ability to manage end customer SLAs.

3.3.2.16 The NMS shall support the following features:

a) Dynamic service monitoring overview
b) Service problem investigation
c) Service quality impact analysis
d) Real-time status views.
e) Generates SLA violation alarms and notifications.
f) Service quality trend reporting - historical reports on how key parameters have varied over user defined reporting periods.
g) Produces periodic service level conformance reports

3.3.2.17 The NMS shall have the capability to model services and report the overall Quality of Service and Service Level Agreement and SLA fulfilment.

3.3.2.18 The NMS shall have the capability to extend support to additional services required in the future.

3.3.2.19 The NMS shall provide service metrics to be defined using Key Quality Indicators (KQIs).

3.3.2.20 The NMS shall provide resource metrics to be defined using Key

Performance Indicators (KPIs).

3.3.2.21 The NMS shall provide a GUI that allows KQIs and KPIs to be configured easily using point-and-click techniques.

3.3.2.22 The NMS shall have the capability to use various mathematical and logical operations for calculating KQI and KPI metrics

3.3.2.23 The NMS shall allow the configuration of a variety of data sources including:

a) Performance data source for key network measures
b) Fault data sources for relevant alarms
c) Operational data sources like trouble tickets

3.3.2.24 The NMS shall allow defining thresholds to detect SLA violations.

3.3.2.25 The NMS shall generate service quality alerts when anomalies are detected based on a comparison to historical KQI trends.

3.3.2.26 The NMS shall allow different thresholds to be configured for different times of day.

3.3.2.27 The NMS shall have configurable interfaces to collect data from various data sources like eMS's.

3.3.2.28 The NMS shall allow privileged user to specify the list of resources from which to collect data, the list of measurements to collect, and the collection interval if required.

3.3.2.29 The NMS shall use trouble ticket data to compute key KQIs like the MTTR.

3.3.2.30 The NMS shall compute availability KQIs using the fault data source.

3.3.2.31 The NMS shall calculate availability KQIs to monitor for SLA violations.

3.3.2.32 The NMS shall generate SLA violation information in real time when a KQI/KPI threshold is violated.

3.3.2.33 The NMS shall aggregate Service Quality Records (KPI/KQI Reports) over time on a per customer/service basis.

3.3.2.34 The NMS shall create historical trends based on quality parameters.

3.3.2.35 In response to a threshold violation, the NMS shall provide following automatic task:

a) Generate an alert.
b) Forward an email/SMS.
c) Execute a customized script.

3.3.2.36 The NMS shall provide viewing and editing of Service Definitions.

3.3.2.37 The NMS shall provide a dashboard view on a browser front-end. The dashboard view can be configured so that it can be personalized for different users

3.3.2.38 The NMS's dashboard shall provide instant visibility to potential alerts in the services.

3.3.2.39 The NMS's dashboard view shall allow a user to view detailed service quality metrics on a per customer basis upon seeing an alert.

3.3.2.40 The NMS shall provide user-configurable reports indicating SLA compliance on a per-customer basis.

3.3.2.41 The NMS shall provide option for the scheduling of reports.

3.3.2.42 The NMS shall provide reports to users via a web-based interface.

3.3.2.43 The NMS shall generate management reports providing information on the following:

a) Customer network configuration and changes
b) Faults and achievement against the SLAs

3.3.2.44 The NMS shall deliver network management reports through the web portal.

3.3.2.45 The NMS shall generate detailed and summary reports for all the above parameters.

3.3.2.46 The NMS shall provide customer his network topology as well as alarms on his network in a user friendly format.

3.3.2.47 The NMS shall store all collected service quality data with a timestamp including the date and time received.

3.3.2.48 The NMS shall support the computation and aggregation of KPI and KQI metrics indicative of the quality of service (QoS) for various services and applications delivered over the network infrastructure.

3.3.2.49 The NMS shall support root cause analysis of QoS violations through 'drill down' analysis of KQI and KPI metric data. Root cause analysis includes the presentation of failure modes / cause codes and identification of failure distribution by location, service/device type, subscriber type or other dimensions as appropriate to the monitored services.

3.3.2.50 The NMS shall monitor the service from both its internal perspective i.e.

how the service is coping across the network as well as that of its customers and partners.

3.3.2.51 The NMS shall provide a real-time availability based service management view.

3.3.2.52 The NMS shall allow building service models, integrating business service status from data sources or event sources, and display customized business service views, scorecards, and dashboards in real time.

3.3.2.53 The NMS shall provide service visualization capability, by integrating data from event sources or data sources to show the status of various services and the impact of outages.

3.3.2.54 The NMS shall allow creating custom business service views. The module provides a graphical user interface (GUI) that allows to logically linking services and business requirements within the service model.

3.3.2.55 The NMS shall provide dynamic visualization of key performance indicators to show the health and performance of critical business services.

Note: Following NMS requirements are applicable to specific technologies which may be considered depending upon the actual network requirement.

3.3.2.56 The NMS shall provide customer traffic performance on a leased circuit, a group of leased circuits, a hunt group, a leased physical or virtual network, etc., as applicable.

3.3.2.57 The SLA Reports include latency, packet loss, jitter, error apart from the availability and the link utilization reports for applicable technologies.

3.3.2.58 The NMS shall allow customer to view reports pertaining to traffic in QoS paths for applicable technologies.

3.3.3 Customer Experience Management [Optional Requirement]

Customer Experience Management (CEM) refers to assuring optimal quality of experience to customers while using the services. The NMS

shall have the following CEM functionalities.

3.3.3.1 The CEM shall carry out the following performance measurements as per ITU-T M.20 in applicable technologies for monitoring and recording of parameters.

a) Connection establishment (e.g. call set-up delays, successful and failed call requests).

b) Connection retention.

c) Connection quality.

d) Cooperation with fault (or maintenance) management to establish possible failure of a resource and with configuration management to change routing and load control parameters/limits for links, etc.

e) Initiation of test calls to monitor SLA parameters

3.3.3.2 The CEM shall provide reporting on service quality and user experience and compare with defined service-level objectives.

3.3.3.3 The CEM shall define service levels to have the overall view of service availability and accessibility percentages over time, and showing the frequency at which service quality or user experience is degraded

3.3.3.4 The CEM shall define the levels of service by capturing service-specific achievements such as worst number of dropped calls in peak hours for voice, percentage of text messages with transfer delay above 60 seconds for Short Message Service (SMS), ratio of unsuccessful session setup for video streaming, and others

3.3.3.5 The CEM shall support integration with application-level probes with insight into customer activity, drilling down to application-level interactions.

3.3.3.6 The CEM shall capture QoE parameters captured by application-level probes for each application-level interaction for every single subscriber.

3.3.3.7 The CEM shall display charts of most relevant QoE network indicators onto the dashboard to efficiently monitor customers' experience.

3.3.3.8 The CEM shall make available network-level key performance indicators (KPIs) and service level key quality indicators (KQIs) and associated reports.

3.3.3.9 The CEM shall provide accurate and timely image of services, which can be drilled down by subscriber, device type, node, service path,

location, and more.

3.3.3.10 The CEM shall monitor Performance Management information of a customer, such as grades of service options, performance monitoring thresholds, or the possible conditions under which rebates are awarded when service quality goals are not met.

3.3.3.11 The CEM shall provide streaming reproduction indicators for media streaming service.

3.3.3.12 The CEM shall provide node-level key performance indicators (KPIs) and service-level key quality indicators (KQIs) and statistics. These can be segmented by service, network, subnet, network element, and also by the path taken by the user's service throughout the operator's network.

Note: Following NMS requirements are applicable to specific technologies which may be considered depending upon the actual network requirement.

3.3.3.13 The CEM shall provide RANAP indicators, TCP-level indicators, PDP context indicators, ICMP analysis, DNS indicators, Latency, IP throughput for Data bearer-level QoE indicators etc., based on the service being managed as applicable.

3.3.3.14 The CEM shall provide service specific indicators, end-to-end indicators, HTTP service indicators, IP-level indicators, Data transfer indicators Web browsing (HTTP) as applicable.

3.3.3.15 The CEM shall provide end-to-end indicators, file sharing service indicators, IP-level indicators, data transfer indicators for file sharing service, email service indicators, data transfer indicators for email service.

3.4 Security Management

Security Management provides for the management of security. In addition, security of management is required for all Management Functional Areas and for all TMN transactions. Security of management appears as part of the Security Function in ITU-T

M.3010. Security of Management functionality includes Security services for communications and Security event detection and reporting.

3.4.1 Resource Security

3.4.1.1 All access to NMS shall be though login and password and all operations shall be logged.

3.4.1.2 It shall include operator authentication, command, and menu restriction and operator privileges.

3.4.1.3 The NMS shall allow the System administrator to define the level of access to the network capabilities or features for each assigned password. The NMS shall block the access to the operator in case of unauthorized commands being tried for five consecutive times. The NMS shall also not allow the entry into the NMS in case wrong password is provided more than three consecutive times during the login.

3.4.1.4 The supervisor shall be able to monitor and log all operator activities in the NMS and Local Management Terminal.

3.4.1.5 The dynamic password facility shall be provided in which the user may change his password at any time.

3.4.1.6 The NMS shall have the feature of idle time disconnection which shall be configurable.

3.4.1.7 The NMS shall have the facility of restricting the use of certain commands or procedures to certain passwords and terminals.

3.4.1.8 The NMS shall provide a time-stamped audit log of all transactions, indicating operator login ID, etc.

3.4.1.9 The NMS shall be able to define the access levels the users have to the resources. The basic access levels are:

a) Read.
b) Write.
c) Delete.
d) Modify.

3.4.1.10 The NMS shall be capable of generating reports based on the security alerts.

3.4.1.11 The NMS shall support automatic password aging. The system shall provide an automated procedure for aging passwords and allowing the user to assign their new password. The NMS shall allow the system administrator to configure the maximum age of the password based on user or user profile. For example, system administrator's passwords shall expire every 30 days, and all other users' password shall expire every 90 days.

3.4.1.12 The NMS shall date and time stamp all database entries. The system shall put a date and time stamp on all entries made into the database. The system shall also add an identifier indicating the program or user that made the database entry.

3.4.1.13 The NMS shall provide secure maintenance windows accessible by only authorized users to makes changes to system data (e.g., Lookup table modifications, etc.).

3.4.1.14 The NMS shall have the ability for configurable debugging logs and trace activities on the system/solution.

3.4.1.15 The NMS shall support ability to set group and user permissions

3.4.1.16 All Commands which are executed over the NMS program or data shall be logged in a file (read only) and it shall be possible to retrieve the same on demand whenever required, using Man-Machine Commands. The file usage of up to 50%, 75% and 90% (configurable) shall generate alarms of suitable category prompting the user to initiate the backup operation.

3.4.1.17 The NMS shall support segregation of the commands/operations into at least five classes; the authorisation to these command classes shall be based on combination of terminal Id, login, password, time of day and type of day.

3.4.2 Security Information Event Management [SIEM] Security features [Optional Requirement]

3.4.2.1 The SIEM shall support analysis of significant shifts in revenue that might indicate fraud or theft of service.

3.4.2.2 The SIEM shall support determination of need, monitoring and analysis of alarm systems that support structures that house network

equipment. These alarms may include power, HVAC (Heating, Ventilation, and Air Conditioning), fire, flood, and open-door-or-cabinet systems.

3.4.2.3 The SIEM shall support for the reading of usage data and customer profiles from other functions for recording of service irregularities or anomalies such as billing and usage abnormalities. It provides access to such records.

3.4.2.4 The SIEM shall support for investigation of customer and internal users including usage patterns indicate possible fraud or theft of service. It shall include requests for credit checking, and employment record checking, etc.

3.4.2.5 The SIEM shall support for the collection of audit trail information and the recording of anomalies or abnormalities that may indicate a breach of security or theft of customer services through employee action. It provides access to such data.

3.4.2.6 The SIEM shall have provision for security alarm information that indicates network security violations.

3.4.2.7 The SIEM shall support for signs of software intrusion (e.g. the presence of a known virus) in the NMS. It can be regularly scheduled and/or they may be triggered by security events.

3.4.2.8 The SIEM shall support report information about security alarms so that containment and recovery activities can be initiated. It shall include the reporting of environment alarms (e.g. fire or moisture) and intrusion detection alarms.

3.4.2.9 The SIEM shall support protection of storage of business data (e.g. backup).

3.4.2.10 The SIEM shall support provision for exception reports such as security alarms.

3.4.2.11 The SIEM shall support for actions to limit the security breach such as isolation of equipment or data so that corruption is not propagated and support for restoration of any corrupted data or equipment.

3.4.2.12 The SIEM shall support for actions to limit the security breach (e.g. remove user's access privileges, etc.) and support for restoration of any corrupted data or equipment.

3.4.2.13 The SIEM shall support the identification of an intruder (for example, by analyzing security logs, monitoring targets of intrusion or feeding misinformation to a suspected intruder).

3.4.2.14 The SIEM shall support restoration from backup files in order to restore service after detection of a security violation. This also includes the customer data including billing, service profile etc.

3.4.2.15 The SIEM shall generate a list of all customer/ network/ network elements public keys and access control certificates for the current time period that are known or suspected of being invalid due to security violation (e.g. stolen secret keys) or administrative procedures (e.g. a customer has moved elsewhere).

3.4.2.16 The SIEM shall allow the severance of connections with a customer/ internal user in an attempt to contain data and system corruption as the result of a detected security violation.

3.4.2.17 The SIEM shall store the network configuration data that can be used in support of intrusion recovery. It shall allow for backup of such data, and for restoration of such backed up data upon request.

3.4.2.18 The SIEM shall support methods and procedures to be used in restoring the network in the event of a security breach and the resulting corruption of data or due to a natural calamity damaging the whole NMS site.

3.4.2.19 The SIEM shall support methods and procedures for audit trail information to be collected and evaluated to identify possible and/or potential security violations by individuals or groups of users.

3.4.2.20 The SIEM shall support policy for the monitoring, evaluating, and correlating security alarms.

3.4.2.21 The SIEM shall support for the collection of security alarm information that indicates network security violations.

3.4.2.22 The SIEM shall protect the network and the network management system against intentional or accidental abuse, unauthorized access and loss of communication.

3.4.2.23 The SIEM shall support log transaction between Clients/Agent & Engine shall support SSL/encryption.

3.4.2.24 The SIEM shall have capability to gather information on real-time

threats and zero day attacks through signatures issued by anti-virus or IDS vendors or audit logs and add this information as intelligence feed in to the solution via patches.

3.4.2.25 The SIEM shall support archival information and summary information to be provided separately.

3.4.2.26 The SIEM shall maintains audit trail for the management activities of individual users accessing and using the application.

3.4.2.27 The SIEM shall support capability to create and assign role-based views.

3.4.2.28 The SIEM shall support mechanism for protection of unauthorized access on the Log Database.

3.4.2.29 The SIEM shall support incident status and escalation and a record of action taken shall be maintained.

3.4.2.30 The SIEM shall support Robust & scalable architecture to handle high volume of data with high Events per second.

3.4.3 SIEM LOG Capturing/Analysis [Optional Requirement]

3.4.3.1 The SIEM shall support collection of logs via either of the following methods:

a) Syslog over UDP/TCP.
b) SyslogNG
c) Check Point LEA.
d) SNMP
e) ODBC (to pull events from a remote database).
f) FTP (to pull a flat file of events from a remote device that can't directly write to the network).
g) Windows Event Logging Protocol.
h) XML

3.4.3.2 The SIEM shall support collection of log data during database backup, de-fragmentation and other management scenarios, without any disruption to service.

3.4.3.3 RAW logs shall be Authenticated (time-stamped), encrypted and compressed before being written to log storage. Encryption can be achieved through OS capability.

3.4.3.4 The SIEM shall support log compression capability for storage optimization (compression level at least 50%). It can be achieved through OS capability.

3.4.3.5 The SIEM Database shall use Write Once Read Many (WORM). Once the logs are written to the disk/database no one including database/system administrator can alter the stored RAW logs.

3.4.3.6 The SIEM shall use purpose built object oriented database for storing IP related information and not relational databases. The storage system has flat file system to store log data.

3.4.3.7 Parting of logs or filtering of logs shall not be done at any stage of log collection or log storage.

3.4.3.8 The SIEM shall support Single Global View of all the data across sites/geographies.

3.4.3.9 The SIEM shall collect raw data in real-time to a Central Database from any IP device including home grown, customized and proprietary applications.

3.4.3.10 Historical records and database query done shall be within the SIEM. No third party tool shall be required to access the database.

3.4.3.11 The SIEM shall support compliance to Regulations with data archival.

3.4.3.12 The SIEM shall use log parsing only using XML and shall not use any other proprietary parsing mechanisms.

3.4.3.13 The SIEM shall support two factor authentications to login to the system.

3.4.3.14 The SIEM shall support watch list feature to monitor desired data like specific IP addresses, usernames and other data.

3.4.4 **SIEM Altering and Viewing Requirements [Optional Requirement]**

3.4.4.1 The SIEM shall support full playback of events that have occurred to ensure comprehensive trend and historical analysis and reporting.

3.4.4.2 The SIEM shall support email alerts and integration capabilities to third party ticketing engines and forward alerts via Syslog or SNMP.

3.4.4.3 The SIEM shall categorize all event collected by device into event taxonomies for easier classification and management.

3.4.4.4 The SIEM shall support Distributed viewing and delegation of user

rights across devices and access to individual components of the application.

3.4.4.5 The SIEM shall support Alert suppression for specific events.

3.4.4.6 The SIEM shall allow creating baselines of network activity and shall provide a mechanism to raise alerts when baselines are crossed.

3.4.4.7 The SIEM shall support Email of scheduled reports to recipients.

3.4.4.8 Email notifications shall contain the content of the report capable of being saved as HTML and/or PDF.

3.4.4.9 The SIEM shall support configurable automated actions in response to security problem, sending E-mail Notifications, SMTP notification, SYSLOG notification, SNMP Notification to operators.

3.4.4.10 The SIEM shall support facility to view summary of all dashboard views for the entire enterprise.

3.4.4.11 The SIEM shall support provision of view filter when displaying the logs related to specific IP address, specific service or specific time duration.

3.4.4.12 The SIEM shall support event display window for all alerts.

3.4.4.13 The SIEM shall support web based (both http and https) user interface for device performance monitoring and analysis with SSL connectivity to backend appliances.

3.4.5 SIEM Correlation Requirements [Optional Requirement]

3.4.5.1 The SIEM shall support correlation of logs from all the devices within an enterprise and all security scenarios like spoofing, authentication failure, etc. Multi-device, multi-event and multi-site correlation across the enterprise.

3.4.5.2 The SIEM shall support correlation using suitable correlation engine

3.4.5.3 The SIEM shall display summarization of events.

3.4.5.4 The rules shall allow import/export in XML format. SIEM shall provide a GUI based application for creating new correlation rules/modifying existing rules.

3.4.5.5 The SIEM shall support capability to correlate all the fields in a log without normalizing the logs at collection points.

3.4.5.6 The SIEM shall support wizard based interface for rule creation. The rules shall support logical operators for specifying various conditions in

rules.

3.4.5.7 The SIEM shall support system leverage information about enterprise assets and known vulnerability to identify false-positive IDS messages and to browse assets and vulnerabilities.

3.4.6 **SIEM Forensic Capabilities [Optional Requirement]**

3.4.6.1 The SIEM shall support flexible dashboard interface customized to user preferences allowing the examination of a specific event or a holistic view of the systems within the enterprise.

3.4.6.2 The SIEM shall support Quick and easy access to real-time as well as historical operational data.

3.4.6.3 The SIEM shall provide tool for comprehensive trend and historical analysis of logs and their reporting.

3.4.6.4 The SIEM shall support the following categories of predefined graphs and queries:

a) Firewall, including Top Firewall Interface, File Access through Firewall, and Login Failure Summary.
b) Database, such as Login Activity, Authorization Level and Authorization Level by User.
c) Intrusion detection, including Top Attack Signatures, Attack Type by Severity Level, and IDS Signature Summary.
d) Operations, such as Device Activity Analysis, Activity by Event Category, and Network over Time.
e) User, including Privilege Users Monitoring, Configuration Change Details and Activity by Specific Username.

3.5 Resource / System Administration

3.5.1 System administration functions shall include backup, recovery, installation, automatic fail-over, account maintenance and logging for all components of NMS

3.5.2 The NMS shall provide the single point capability for backup and recover the application and databases. The NMS shall have suitable Backup mechanism for taking backup of NMS data of at least one month. The backup device shall be a read/write CD/DVD/ MOD (magneto-optical disk) drive or some other state of the art backup

device. It shall be possible to take back up at any interval either automatically and under operator control. Incremental backup over a configurable period in steps of 12 hour shall be possible. It shall be possible to test the full backup with stand by arm of NMS. The system shall support:

a) Electronic Document Workflow Feed
b) Backup strategy
c) Nightly archive
d) Weekly backup w/monthly offsite backup

3.5.3 The NMS shall provide the system administrator with the capability to monitor the processes running on the system.

3.5.4 The NMS shall provide capability for remote system administration. The system shall provide the ability for system administrators to logon and administer the system from location other than the system console. It shall be possible to disable this feature.

3.5.5 The NMS shall track users. The system shall be able to identify upon request all users that are currently active on the application.

3.5.6 The NMS shall have the ability to upload existing network resources (logical and addressable physical resources) into the data store.

3.6 Other Requirements

3.6.1 Route Analytics [Optional Requirement]

Route Analytics is an EML layer module provided in the NMS for analysis of the information from IP transport networks like Interface diagnostics, Route to node, IP route, Spanning tree info, Router info, and Switch info

3.6.1.1 The NMS shall support the selection of an appropriate path for circuits/route that cross node boundaries based on routing design, facility design and demand forecast.

3.6.1.2 The NMS shall analyze the trap and provide the information like trap rate etc.

3.6.1.3 The NMS shall help to improve time to repair by capturing problem information before the network changes in a way that removes the data, for faster problem analytics, quickly find where hosts with

problems are connected to the network, enabling faster problem resolution, and tune the management environment for efficient operation

3.6.2 **Network & Device Probes [Optional Requirement]**

3.6.2.1 The system should have wide range of network probes and collectors from a variety of data sources like network devices, customer end devices etc. to know the network and customer end device performance

3.6.2.2 It shall provide the data for the measurement of the Quality of Service and Root cause analysis

3.6.3 **Web Portal**

The Web Portal will Organize, consolidate, and automate all service management functions. The access of the web portal may be through internet with suitable firewall etc., or through VPN or through a dedicated overlay network of remote and local terminals.

3.6.3.1 The Web Portal shall get a real-time window into how services perform by using its ability to draw information and metrics directly into the dashboards from underlying systems and devices.

3.6.3.2 When there is an issue with network or service performance, its problem resolution capabilities shall act, in addition to its end-to-end service monitoring features

3.6.3.3 The web portal shall have the feature to drill down to the individual element, then to subsystem, then to card and then to port level configuration template from the domain Map by clicking on the icon of the network element.

3.6.3.4 Drill-down capabilities shall enable to descend through the layers of information to the underlying systems, which will launch integrated views into the unified dashboard

3.6.3.5 The Portal shall be Web GUI based, easy to learn and use, easy to input the commands and to interpret the outputs.

3.6.3.6 The web portal shall be in English. The man machine commands and response shall also be in English.

3.6.3.7 The Portal shall have an open-ended structure such that any new function or requirement added shall have no influence on the existing ones. The language structure shall be such that subsets can be created. Product API shall be provided for future expansion and/ or integration of new features.

3.6.3.8 The Portal shall provide facilities for editing, cancelling and stopping, the completion of commands.

3.6.3.9 The Portal shall have facility for restricting the use of certain commands or procedures to certain users/terminals based on the set privileges.

3.6.3.10 The Portal shall be implemented in such a way that errors in commands or control actions shall not cause the network to stop or unduly alter the network configuration.

3.6.3.11 Sufficient checks and safeguards shall be built in to the implementation of the commands from the portal so as to ensure reliable operation of the network.

3.6.4 NMS Reporting

3.6.4.1 The NMS shall allow modification of existing reports and creation of new reports (through wizard).

3.6.4.2 Reports shall be available in the following exported formats:

a) PDF
b) CSV
c) HTML

3.6.4.3 The NMS shall support capability to schedule reports. All raw log format fields shall be available for query.

3.6.4.4 The NMS shall provide process for creating adhoc queries. This process shall use standard syntax such as wildcards and regular expressions.

3.6.4.5 The NMS shall allow applying filters and sorting to query results.

3.7 Hardware Requirements

A typical NMS network architecture is given below.

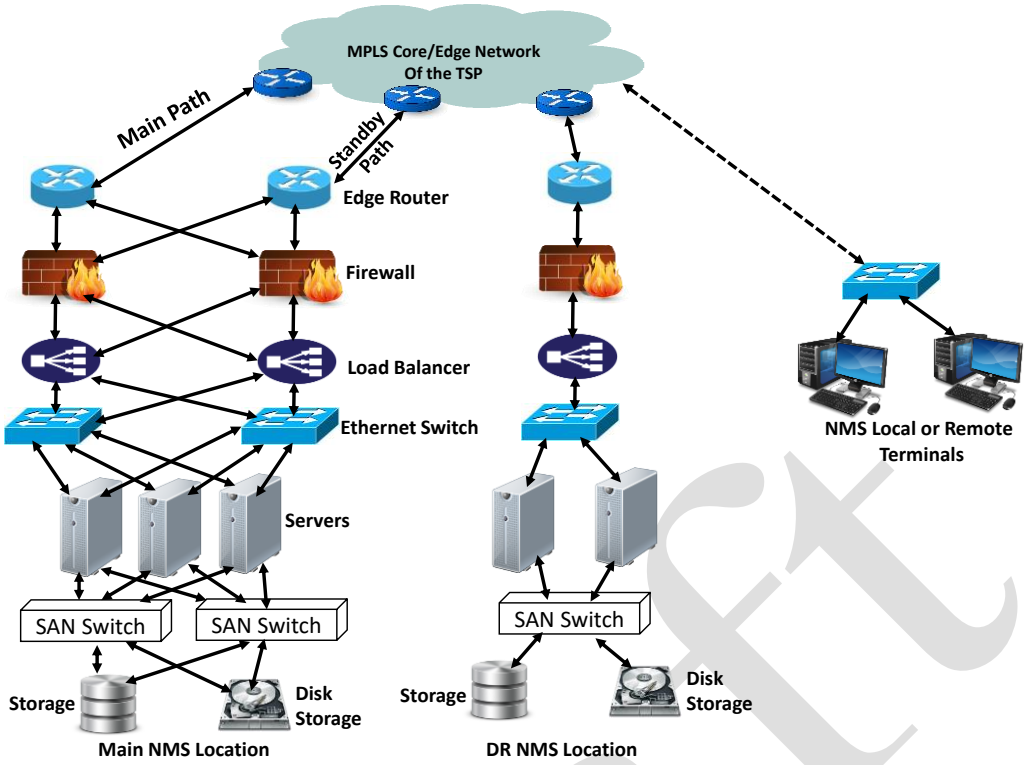

Figure-8 Typical Hardware Architecture

3.7.1 The MPLS Core/Edge network of the TSP is shown in Figure-8.

3.7.2 For the Firewall requirements, the latest TEC standard on Firewall available on TEC website (https://tec.gov.in/standards-specifications) may be referred. The type of firewall required shall be specified by the purchaser.

3.7.3 For the Load Balancer requirements, the latest TEC standard on Load Balancer available on TEC website (https://tec.gov.in/standards-specifications) may be referred. The Category of Load Balancer required shall be specified by the purchaser.

3.7.4 For the Ethernet Switch requirements, the latest TEC standard on Ethernet Switch available on TEC website (https://tec.gov.in/standards-specifications) may be referred. The Category of Switch required shall be specified by the purchaser.

3.7.5 The NMS Server hardware configurations can be referred from the latest TEC standard on NMS Server available on TEC website (https://tec.gov.in/standards-specifications). The Category of Server and type of Server required shall be specified by the purchaser.

3.7.6 For the Storage hardware requirements, the latest TEC standard on

Storage hardware available on TEC website (https://tec.gov.in/standards-specifications)may be referred. The type of Storage hardware required shall be specified by the purchaser.

3.7.7 The NMS solution shall run in high availability mode with redundancy i.e. N+1 (Active or Passive) configuration

3.7.8 All SW applications shall run in a redundant active – standby pair of hosts with automatic switchover in case active server or its applications have any failure.

3.7.9 Hardware Sizing Guidelines: Hardware sizing is based on the following CPU utilization metric (CPU Utilization = 100 – CPU Idle)%. Peak CPU Utilization shall not exceed 75% at any time, on 24x7 basis. Average CPU Utilization over any hour, measured at 5 minute intervals, shall not exceed 60%. The hardware sizing indicated is minimum and indicative.

3.7.10 The servers shall be able to provide a response to the interrogation command for node status within 4 seconds when all the operators are accessing the NMS concurrently either from local or remote terminal.

3.7.11 The implementation of the hardware and software configuration shall allow for future expansion and be able to handle maintenance with minimum disruption to the Main NMS.

3.7.12 The design of the NMS system shall not be dependent on single machine setup, which shall have an impact on the Main NMS during upgrading. Scalability of the NMS system shall not be limited to increasing the processing power of single hardware. The NMS system shall fully utilize the performance of multiple hardware, and at the same time reducing the cost and downtime of the system while upgrading.

3.7.13 The NMS system shall have the capacity for fail-over with duplication of processes. Any failure in the individual module shall have a minimum impact on the entire NMS system.

3.7.14 NMS system shall support flexibility for optimal load distribution on servers.

3.7.15 NMS system shall be linearly scalable and it shall be possible to add additional servers/databases with the growth in number of subscribers.

3.7.16 The NMS system shall be able to scale hardware expansions.

3.7.17 NMS system shall be scalable horizontally and vertically.

3.7.18 NMS system performance shall not degrade as all the users use the system simultaneously.

3.7.19 Users running reports shall not affect system performance.

3.7.20 NMS shall support specified transactions per day/per hour/per minute as applicable as below:

a) X activations

b) Y faults per day

c) Z network elements or circuits

3.7.21 The NMS system shall properly maintain the data. Data consistency checks and cleansing shall be performed on a regular basis to prevent corruption.

3.7.22 The NMS system shall be able to recover point-in-time due to hardware or software failure(s).

3.7.23 The NMS system shall allow the disconnection of a redundant system with no adverse impact on the Network or to the NMS itself.

3.7.24 The NMS system shall support unattended automatic shutdown and restart of core processes in case of component failure.

3.7.25 The NMS system shall support ability for auto restart after application failure or power-up.

3.7.26 The NMS system shall maintain data integrity in case of failure of a single component.

3.7.27 NMS system design shall support automatic rerouting and reconnection. For example, if a server supporting a client application fails, the client shall be able to reconnect and reroute through an alternative path.

3.7.28 The NMS system shall notify the system operators of critical errors that impact the normal operation of the system. The system shall notify the operators via defined alerts/messages sent to the data center console.

3.7.29 The NMS system shall generate error message data for every error condition that can occur within the application.

3.7.30 It shall be possible to connect NMS to the IP network. The NMS and eMS may be part of the common VPN providing the inherent security required for the Management information in addition to the login and Password based authorization for the operators of the Network

Manager. The connectivity between eMS and the NMS shall be TCP/IP based with the Data Link layer being the Ethernet. However in case the connectivity between eMS and NMS is not supported over TCP/IP interface then suitable converters shall be provided for transporting the Management information over the IP network

3.8 Software Requirements

3.8.1 The NMS shall support the following tasks under the software management function

a) Loading of new system software.
b) Manage different versions of software.
c) Capability of managing multiple versions of software for individual elements.
d) Installation of software patches.
e) Examine contents of all system memory and disk memory.

3.8.2 At the time of downloading the software, the message shall be displayed that the software has been downloaded successfully or failed and at what stage.

3.8.3 The NMS shall support FTP for downloading of Software, configuration, patches etc., to the Network Element.

3.8.4 The NMS shall support version control process/software

3.8.5 The NMS shall support ability to uninstall a release

3.8.6 The NMS shall enable operations like changing the system configuration, reconfiguration of input and output devices, loading a new software package, etc. Both automatic and manual reconfiguration capabilities shall be available.

3.8.7 All Application Functions shall be able to use high availability features of the Operating System.

3.8.8 The NMS shall support mechanisms to detect resource shortages such as CPU, processes, disk, etc.

3.8.9 The NMS shall allow a workstation/PC based monitoring tool for high volume processes which can do the following:

a) Halting of tasks
b) Altering of periodic schedule

c) Requesting status information

d) Changing the status of jobs in bulk

e) Starting volume processing applications on demand

3.8.10 The diagnostic program shall also be locally available and shall be able to run even in case any module or link with NMS goes down.

3.8.11 On a faulty condition, NMS shall support the diagnostics of the NMS elements.

3.8.12 The NMS shall monitor its own hardware and software and shall present the performance-related information.

3.8.13 Audio/visual alarm indication shall be given when the processor load exceeds a certain configurable pre-set value.

3.8.14 In case a fault is detected requiring reloading of the program/software, this shall be carried out automatically. In case of manual re-loading, it shall be possible to stop and start at any particular point in the program. It shall be possible to load a designated file or group of files of the entire software.

3.8.15 The NMS shall have RDBMS for a common data repository. Persistent data shall be maintained in a commercially available relational database management system (RDBMS). Access to all RDBMS stored procedures shall be available through ODBC, JDBC, BDE, C and Active X.

3.8.16 The NMS shall provide a hot standby mechanism among the production (or primary) and backup database servers across LAN and WAN.

3.8.17 RDBMS shall also be capable of operating in a standby or clustered environment with multiple standby (backup) system.

3.8.18 The NMS shall support built-in feature for graceful switchover and switchback between the primary and the standby databases (without any direct intervention from the database administrators).

3.8.19 The NMS shall support a means to transport and apply the logical copy of the changes in the primary database to the standby database.

3.8.20 The NMS shall support automatic synchronization between the network and the database.

3.8.21 A file-based interface shall be available with the following

a) An import file format.

b) A protocol for importing files into the managed environment.

c) A mechanism for importing files.

d) An export file format.

e) Protocols for exporting files out of the managed environment.

3.8.22 The main NMS shall update disaster recovery (DR) NMS at regular interval & this interval shall be configurable in steps of at least 30 minutes.

3.8.23 Actions to initiate Switchover to DR site and Switchback from DR to main site shall initiated manually. Switchover or Switchback shall be completed in 4 hours.

3.8.24 The NMS shall provide feasible solution for DR like log transfer, application level DR/replication manager and other best practices.

3.8.25 When the Main NMS fails, the DR NMS shall take over the functions of the Main with minimum loss of data or functionality related to the update interval / transfer period. The replication solution shall be designed to have negligible impact on the server & storage resources of the Main NMS environment.

3.8.26 During regular updates, only incremental data pertaining to the previous interval shall be transferred. However, it shall also be possible to mirror the whole database during slack hours any number of times during the day at prescribed hours through manual commands of network manager.

3.8.27 The connectivity of operator terminals at main site and terminals at remote sites shall be provided in such a way that during failure of main site connectivity of the terminals is automatically transferred to the Disaster recovery (DR) site & vice versa. However, during complete unavailability of the main site, the onsite terminals of the DR site shall take over the control. The engineering of the main & DR system shall be done in such a way that the connectivity of remote terminals to system remains available under all circumstances and no functionality is lost.

3.8.28 It shall be possible to define and redefine the DR policy at any time as per the requirement.

3.8.29 It shall be possible to monitor the health of DR system from main system and vice – versa continuously or under operator command at the choice of the network manager.

3.8.30 In case of main NMS becoming un-operational, it shall be possible to transfer the control manually to the DR NMS. The control shall not come back automatically to main NMS & it shall take over the control under the operator command.

3.8.31 It shall be possible to test the DR NMS live at any time with minimum loss of data or service (Synchronization time difference data).

3.8.32 The NMS shall have the capability to synchronize with an NTP network synchronization source.

3.8.33 NMS shall meet the IPv6 requirements.

4.0 INTERFACE REQUIREMENTS

4.1 The NMS systems shall have the South Bound Interfaces towards the eMS systems. The standard protocol namely SNMP, XML, TEXT, CORBA and TL-1 shall be available to interface with different eMS systems having one of these open standard interfaces.

4.2 The NMS systems will have the North Bound Interfaces towards other NMS systems, OSS/BSS Systems and ERP Systems. These interfaces shall be as per standard interfaces SNMP (All versions), XML, TEXT, ODBC, JDBC, CORBA etc., based on the requirement of the OSS/BSS/ERP Systems.

5.0 QUALITY REQUIREMENTS (QR):

No requirements specified

6.0 EMI/EMC REQUIREMENTS

No Requirements Specified.

7.0 SAFETY REQUIREMENTS

No Requirements Specified

8.0 SECURITY REQUIREMENTS

The security management function of the FCAPS functional requirement is covered under section 3.4

9.0 VARIOUS REQUIREMENTS OF THE CATEGORY/CONFIGURATION OF THE PRODUCT

9.1 Minimum Equipments required for Type Approval:

The following minimum equipments shall be offered for Type Approval.

9.1.1 The NMS software in a suitable server hardware. Any of the requirements shown as optional in the GR, if offered for testing shall be indicated by the applicant. These shall be mentioned in the Type Approval certificate.

9.1.2 Three routers or any other Network Elements along with their eMS.

CHAPTER -2

10.0 INFORMATION FOR THE PROCURER OF PRODUCT

This section describes the information for the procurer of the product which relates to the documentations, deployment guidelines, checklist to be taken care of at the time of tender etc.

10.1 Documentation:

10.1.1 All literature and instructions required shall be made available in English language.

10.1.2 The documents shall comprise of System description documents, Operation documents and Training documents

10.1.3 **System description documents:**

The following system description documents shall be supplied along with the system.

10.1.3.1 Over-all system specification and description of the software

10.1.3.2 Detailed description of software describing the principles, functions, and interactions with hardware, structure of the program and data.

10.1.3.3 Detailed description of each individual software package indicating its functions and its linkage with the other packages, hardware, and data

10.1.3.4 Graphical description of the system. In addition to the narrative description a functional description of the system using the functional Specification

10.1.4 **System operation documents:**

The following system operation documents shall be available.

10.1.4.1 Installation manuals and testing procedures

10.1.4.2 Precautions for installation, operations and maintenance

10.1.4.3 Operating and Maintenance manual of the system

10.1.4.4 Man-machine language manual

10.1.5 **Training Documents**

10.1.5.1 Training manuals and documents necessary for organizing training in installation, operation and maintenance and repair of the system shall be made available.

10.1.5.2 Any provisional document, if supplied, shall be clearly indicated. The

updates of all provisional documents shall be provided immediately following the issue of such updates.

10.1.5.3 The structure and scope of each document shall be clearly described.

10.1.5.4 The documents shall be well structured with detailed cross-referencing and indexing enabling easy identification of necessary information.

10.1.5.5 All diagrams, illustrations and tables shall be consistent with the relevant text.

10.2 NMS Deployment Guidelines

10.2.1 If a DR is planned, it shall normally be geographically separated. The Main as well as the DR NMS is to be connected on normal and standby link with IP network.

10.2.2 It is recommended that the DR NMS site have processing capacity of 100 % of the production capacity, so that in case of any natural or manmade DR instance, all functionalities related to all the applications shall continue to work.

10.2.3 NMS for different networks (e.g. IP network, circuit switched network, transmission network, etc.) can be put under single OSS. This is ideal deployment to start with. The function of NMS is described in this document. However many of these functions are related to the capability of the eMS/NE and eMS/ NE shall be capable to support those functions.

10.2.4 eMS of individual networks without full eMS capabilities can be integrated into one or more big umbrella NMS (with the eMS capabilities and shall be able to communicate with the NEs directly) for providing full eMS-NMS functions. Such umbrella NMS(s) and also other NMSs can be put under single OSS of service provider. Such deployment is useful when existing NEs with less number of functionalities eMS needed to be integrated with NMS. In this case, it is essential to develop and deploy the proxy/ mediation device which could enable the communication between NMS and NE over proprietary interface. Normally the proxy/ mediation function is performed by eMS. This deployment is suitable for small networks and has limitation in scalability to support the expansion of network.

10.2.5 In case the NMS of a network does not have some features (like performance management, etc.), such NMSs (actually the upgraded eMSs) can be put under one umbrella OSS of the service provider for providing full NMS-OSS functions. This deployment is envisaged for the scenario where the individual networks have grown up with eMS only without integration to a full NMS. In this case, OSS shall also perform NMS functions. However since the some NMS functions can be specific to a particular type of network and since the OSS is network independent, this deployment becomes very complex in cases where OSS is required to manage multiple networks and also to provide NMS functions to all/ some of them.

10.2.6 The NMS shall store both raw service quality data for a period of 3 months and normalized data in a historical log for a period of one year. However the exact period of storage shall be specified by the service provider.

10.2.7 The NMS is considered to be mission critical system and the whole system should be able to operate 24x7 basis with over 99.99% availability. High availability and fail-over capability shall be one of the main design focuses.

10.2.8 It shall be ensured that in case of any link failure, the NMS connectivity to network is not disrupted and there is minimal loss of NMS data from the network. In absence of the NMS or eMS the Network shall continue to provide the services without any deterioration.

10.2.9 The automatic switchover from Main NMS to DR NMS may require additional networking requirements which may be taken care while network design.

10.2.10 Wherever e-mail / SMS alert is mentioned in this document requires PLMN / Internet connectivity which shall be ensured by the Service Provider.

10.3 Items to be Specified while Tendering:

The following information shall be specified by the purchaser while tendering the items:

10.3.1 The purchaser may make the requirements more explanatory wherever

required based on the type of network / networks proposed to be managed.

10.3.2 The exact requirement for number of concurrent users and maximum users of the system with the future scalability.

10.3.3 The requirement of redundancy of the NMS network elements shall be decided by the purchaser. Purchaser can procure the NMS servers alone also with or without the SAN Switch and Storage components.

10.3.4 The tendering authority shall indicate the redundancy requirement for Firewall, Load Balancer, Ethernet switch, SAN Switch etc., as shown in the figure-8.

10.3.5 The tendering authority shall indicate whether separate storage is required as shown in the figure-8 or the storage in the NMS server is adequate or a separate server is required.

10.3.6 For category of the Server and other items to be specified, the latest TEC standard on Server available on TEC website (https://tec.gov.in/standards-specifications) may be referred.

10.3.7 The number of transactions per day/per hour/per minute to be supported as per clause 3.7.20.

10.3.8 Category of the various hardware components as per clause 3.7

10.3.9 Number of licenses required in terms of the CPU Core or named licenses or data size for the Database and the number of local/remote NMS terminals.

10.3.10 details of technologies / vendors equipment's for which auto discovery of the NE's is required as per clause 3.2.2.2

10.3.11 In case the remote terminal locations from where the NMS is accessed do not have IP VPN connectivity with the NMS, requirement of DCN shall be indicated at the time of tendering by the Purchaser.

10.3.12 requirement of the following Optional Modules based on need with further customization where required

10.3.12.1 Service Problem Management as per clause 3.1.2

10.3.12.2 Service Quality/SLA Management requirements as per clause 3.3.2

10.3.12.3 Customer Experience Management as per clause 3.3.3

10.3.12.4 SIEM Security Features as per clause 3.4.2

10.3.12.5 SIEM LOG Capturing / Analysis as per clause 3.4.3

10.3.12.6 SIEM Altering and Viewing Requirements as per clause 3.4.4

10.3.12.7 SIEM Correlation Requirements as per clause 3.4.5

10.3.12.8 SIEM Forensic Capabilities as per clause 3.4.6

10.3.12.9 Route Analytics as per clause 3.6.1

10.3.12.10 Network & Device probes as per clause 3.6.2. In case this module is required details of the network elements required to be probed and their interface supported shall be specified.

10.3.12.11 NMS North Bound interfaces to be supported as per clause 4.2

10.3.12.12 Wherever applicable technology is mentioned, these clauses need to be modified / amended based on the type of networks to be managed.

10.3.12.13 This document provides the details of generic requirements for the NMS and purchaser can modify and customize any requirement based on the networks and services to be managed.

10.3.12.14 The purchaser may provide additional performance monitoring parameters in clause 3.3 as required based on the NE's being monitored.

10.3.12.15 The purchaser may specify the AI/ML capabilities for the NMS required as mentioned in clause 3.1.1.25.

11.0 SPECIFIC ITEMS TO BE MENTIONED IN THE CERTIFICATE

11.1 The following items shall be specified in the Certificate:

11.1.1 Name/Model of the NMS

11.1.2 Version of the NMS software

11.1.3 Operating Systems supported

11.1.4 Category of Server used while testing the NMS

11.1.5 Optional requirements/features offered for type approval

11.1.6 NEs used for testing NMS requirements

ABBREVIATIONS

For the purpose of this document the following abbreviations apply:

Abbreviation	*Expanded Form*
API	Application programming interface
BDE	Borland Database Engine
BLA	Business Level Agreement
BML	Business Management Layer
BSS	Business Support System
CD	Compact Disk
CDR	Call Detail Record
CEM	Customer Experience Management
CORBA	Common Object Request Broker Architecture
CPU	Central Processing Unit
CRM	Customer Relationship Management
CSV	Comma Separated Value
DNS	Domain Name System
DoT	Department of Telecommunication
DR	Disaster Recovery
DVD	Digital Versatile Disk
EML	Element management layer
eMS	Element Management System
ERP	Enterprise Resource Planning
e-TOM	Enhanced Telecom Operations Map
FCAPS	Fault, Configuration, Asset/ Accounting, Performance and Security Management
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTML	Hyper Text Mark-up language
HTTP	Hyper Text transfer protocol
HTTPS	Secure HTTP
HVAC	Heating Ventilation & Air Conditioning
ICMP	Internet Control Message Protocol
I/O	Input Output

IP	Internet Protocol
IPv6	IP version 6
IR	Interface Requirement
ISO	International Organizational for Standardization
ITU	International Telecommunication Union
ITU-T	International Telecommunications Union Telecommunication
JDBC	Java Database Connectivity
KPI	Key Performance Indicator
KQI	Key Quality Indicator
LAN	Local Area Network
MDO	Magneto Optical Disk
MPLS	Multi-protocol Label Switching.
MTTR	Mean Time To Repair
NE	Network Elements
NEL	Network Element Layer
NML	Network management layer
NMS	Network Management System
OAM	Operations Administration & Management
ODBC	Open Database Connectivity
OSS	Operational support system
PM	Performance Monitoring
PSU	Power Supply Unit
QR	Quality Requirement
QoS	Quality of Service
RANAP	Radio Access Network Application Part
RDBMS	Relational Data Base Management System
SAN	Storage Area Network
SIEM	Security Information Event Management
SLA	Service level agreement
SML	Service management layer
SMTP	Simple Mail Transfer Protocol
SMO	Service Management & Operation
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer

TCP	Transmission Control Protocol
TEC	Telecommunication Engineering Centre
TMN	Telecomm. Management Network
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide Access Network
XML	Extensible mark-up language

======== End of the document ========

ANNEXURE

Template for submitting Comments on draft Standard titled "NMS"

(Draft Standard No. TEC 48100:202x)

Name of Manufacturer/Stakeholder:

Organization:

Contact details:

Clause No.	Clause	Comments	Justification for proposed change

The comments in above format may be submitted via Email to dirit2.tec-dot@gov.in, adic1.tec@gov.in and adit2.tec-dot@gov.in latest by 09.09.2025.