Eskom	Standard	Technology

Title: **GENERIC REQUIREMENTS SPECIFICATION FOR A TELECOMMUNICATIONS NETWORK MANAGEMENT SOLUTION**

Unique Identifier:	**240-86458714**
Alternative Reference Number:	**N/A**
Area of Applicability:	**Engineering**
Documentation Type:	**Standard**
Revision:	**3**
Total Pages:	**15**
Next Review Date:	**October 2025**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	Approved by	Authorized by
Bongani Shezi	**Cornelius Naidoo**	**Richard McCurrach**
Senior Engineer Telecoms Technology & Support	**Telecoms T&S COE Manager**	**PTM&C Engineering Senior Manager**
Date: 22 September 2020	Date: 2020/09/30	Date: 1 Oct 2020

Supported by SCOT/SC

Kgomotso Setlhapelo

SCOT/SC Chairperson

Date: 29 September 2020

PCM Reference: **240-53458797 Perform PTM&C Systems Engineering**

SCOT Study Committee Number/Name: **Telecommunications Study Committee**

Content

Figures

Tables

1. Introduction

The network management systems/solutions (NMS') deployed in the network management centre (NMC) within Eskom Telecommunications (ET) for the management of various networks have more commonalities than differences. It is therefore necessary to standardise on the common requirements of these systems and benchmark future systems against this standard, so that future instances can be seamlessly and/or effortlessly integrated into the ET NMC environment.

This document aims to address design and functional requirements that any NMS that is to be procured for deployment by ET NMC shall adhere to and be checked against. Network/Equipment/System management aspects that are equipment, technology and/or OEM specific shall be documented in the relevant accompanying specification/standard.

2. Supporting clauses

2.1 Scope

This document details the minimum requirements that management solutions for deployment at the ET NMC shall adhere to.

Service requirements (including network support) and other related technical requirements are detailed in the 240-135089195 Generic Technical Requirements for Eskom Telecoms Contracts.

Information and network security requirements including remote access controls are detailed in 32-85 Eskom Information Security Policy, 32-214 IT/OT – Third Party Access Control Procedure and 240-55410927 Cyber Security Standard for Operation Technology

Other relevant procedures and/or documentation will be issued to the successful tender.

2.1.1 Purpose

This document is intended for use as part of an enquiry documentation to the market, in procuring any component of management system/solution for the Eskom Telecommunications network.

2.1.2 Applicability

This document shall apply throughout Eskom Holdings Limited Divisions.

2.2 Normative/informative references

Parties using this document shall apply the most recent edition of the documents listed in the following paragraphs.

2.2.1 Normative

[1] ISO 9001, Quality Management Systems.

[2] 240-135089195 Generic Technical Requirements for Eskom Telecoms Contracts

[3] 240-55410927 Cyber Security Standard for Operation Technology

[4] 32-85 Eskom Information Security Policy

[5] 32-214 IT/OT – Third Party Access Control Procedure

2.2.2 Informative

[6] 32-9 Definition of Eskom Documents

[7] 32-644 Eskom Documentation Management Standard

[8] 240-84323647 Network Management Centre Redundancy Standard

2.3 Definitions

2.3.1 General

Definition	Description
Hardware	Hardware encompasses network management solution infrastructure required to run the management system
Network Management System/Solution	Software and hardware used for the operation, administration, and maintenance of the telecommunications network.
Software	Software encompasses software applications, firmware, middleware, operating systems, databases, and related licenses required by the telecommunications' network management system.

2.3.2 Disclosure classification

Controlled disclosure: controlled disclosure to external parties (either enforced by law, or discretionary).

2.4 Abbreviations

Abbreviation	Description
ET	Eskom Telecommunications
Mbps	Megabits per second
NE	Network Element
NMC	Network Management Centre
NMS	Network Management System/Solution
OEM	Original Equipment Manufacturer
OSS	Operational Support Systems
SLA	Service Level Agreement

2.5 Roles and responsibilities

2.5.1 Eskom's responsibilities

a) Create a conducive environment for the supplier by making relevant resources (people and workspace) available

b) Provide network access in accordance with the relevant Eskom security policies/procedures.

c) Provide support functions and services required for the solution

d) Provide technical support and specialist knowledge of the NMC environment (power, cooling, cabling, cabinet space, wiring, Local Area Network (LAN), systems, applications) and the Eskom Telecommunications' Wide Area Network (WAN).

2.5.2 Supplier's responsibilities

a) Design, development, implementation, testing, installation, commissioning, and support of the solution.

b) Training and skills transfer on the operation, administration and maintenance of the solution

c) Handover of solution documents (design, planning, maintenance, administration and operation)

2.6 Process for monitoring

The implementation of this document will primarily be through a procurement/commercial process. Revision to the content of this document will be through the Steering Committee on Technologies (SCOT) governance process. The management of the document will be done according to Eskom's document and records management standards.

2.7 Related/supporting documents

240-135089195 Generic Technical Requirements for Eskom Telecoms Contracts

3. Network Management Solution requirements

3.1 Solution architecture requirements

a) Unless stated otherwise, the supplier shall make both the following options available for solution implementation:

3.1.1 Software-based solution:

3.1.1.1 The supplier shall provide a list of the following resource requirements for their offered solution:

a) Virtualization platform(s) supported

b) Resources required

1) Central Processing Units (CPUs)

2) Processor

3) Random Access Memory (RAM)

4) Hard disk storage

5) Networking requirements

c) All associated software, firmware, middleware and database requirements (these are to be provided with the solution)

d) All associated licenses requirements (these are to be provided with the solution)

3.1.1.2 The supplier shall specify the sizing in terms of the number of elements that the offered solution can manage.

3.1.1.3 The supplier shall specify the threshold of the NMS in terms of maximum number of network elements (NEs) that can be managed before an upgrade in the resources specified is needed.

3.1.1.4 The supplier shall specify the resources required for the upgrade, should the maximum number of NEs be reached, and an upgrade necessitated.

3.1.2 Hardware-based solution:

3.1.2.1 The supplier shall provide the hardware together with associated installation material.

3.1.2.2 This system shall be with a full maintenance service for the duration of the contract. The maintenance shall include all technical support on the hardware, including software, firmware, and hardware updates, and swop out of faulty units.

3.1.2.3 The supplier shall specify the sizing in terms of the number of NEs that the offered solution can manage.

3.1.2.4 The supplier shall specify the threshold of the NMS in terms of maximum number of network elements that can be managed before an upgrade in the resources specified is needed.

3.1.2.5 The supplier shall specify the next level hardware that the offered solution can be upgraded to, should the maximum number of NEs be reached, and an upgrade necessitated.

3.1.2.6 Where applicable, control and on-board memory modules shall be hot-swappable

3.1.2.7 The hardware shall support redundant power supplies (dual feeds).

3.2 Disaster recovery requirements

3.2.1 Availability requirements

As per Figure 1: RPO and RTO illustration below, Recovery Point Objective (RPO) deals with the amount of acceptable data loss whereas the Recovery Time Objective (RTO) deals with the amount of time before the operations are resumed. The former looks backwards (how far back) and the latter looks forward (how soon).

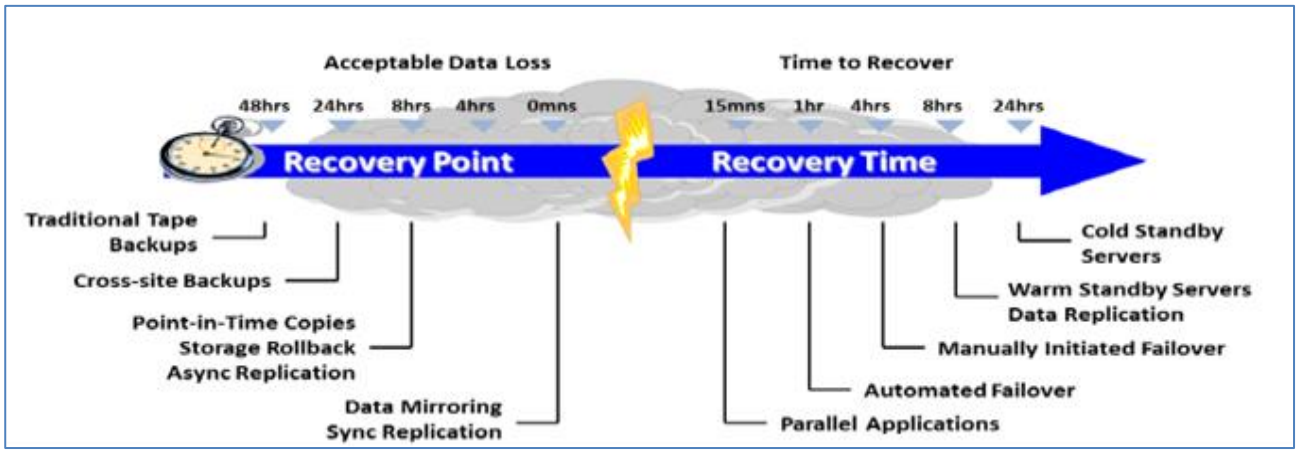

Figure 1: RPO and RTO illustration

Eskom's classification for the required solution based on its criticality is indicated with an X in Table 1: Recovery objectivesbelow. The supplier shall populate the requirements needed to implement the solution, as per the table.

Table 1: Recovery objectives

	Safety & Revenue Critical AND/OR Core Systems	**Mission Critical**	**Business Critical**	**Normal to Non-Essential**
Description/Criteria	Failure of system function may result in injury or death to human beings. Failure to supply electricity AND/OR Failure of system function may impact multiple systems	A system that is critical to the functioning of the organization and the accomplishment of its mission	A system whose reliability and availability is not in any way endangering lives or property, and without which the business can continue operations for a pre-defined time.	All other systems
Recovery Time Objective, (acceptable system lost time)	0 – 1 Hour	8 – 24 hours	< 48 hours	>72 hours

	Safety & Revenue Critical AND/OR Core Systems	**Mission Critical**	**Business Critical**	**Normal to Non-Essential**
Recovery Point Objective, (acceptable lost data)	No data loss	No data loss	Less than a day worth of data loss	>24 hours
Disaster Recovery Strategy	Active – Active Full continuous availability	Active – Hot Standby	Active – Standby (Warm)	Active – Standby (Cold)
Eskom's requirement for this solution (Mark with an X)				
Minimum bandwidth required to implement solution (supplier to specify)				
Maximum latency that solution can withstand (supplier to specify)				
Maximum distance that solution can withstand (supplier to specify)				

3.2.2 Backup strategy

3.2.2.1 The supplier shall propose a backup strategy for the solution. The strategy shall address at minimum:

a) Details on system components that can be backed up (e.g., Operating System file system, database logs and records, application data, flat files, NE configuration, NE database, NE firmware, etc.)

b) Incremental and/or differential and frequency thereof

c) Long term retention mechanism and process (this should address how long files can be backed up, what happens after the duration, overwrite, deletion, export to other media, etc.)

d) Security and integrity of backups, including protection against malware/tampering and handling of corrupt backups and/or lost and/or expired backed-up credentials

e) Backup retrieval and/or staging and/or testing

3.3 System specification

3.3.1 Accessibility

3.3.1.1 The solution shall support secure access via a web browser interface (preferred), and/or Graphical User Interface (GUI) and/or a craft terminal. Access through these interfaces shall offer full functionality of the solution, if limitations exist, they should be clearly stated.

3.3.1.2 The solution shall support concurrent client sessions. The maximum number of concurrent sessions shall be specified.

3.3.1.3 The solution shall support at minimum the following views of the network, with drill-down function, overlaying, grouping and segmentation at each view:

a) Topology view – this would typically show NEs and their interconnections.

b) Physical view – this would typically show the NE with its physical interfaces and modules.

c) Logical view – this would typically show traffic, circuits and/or services. Assisting in tracing and trailing them.

d) Geographical view (where possible) – this would allow for the overlaying of the topology, physical and/or logical views on a map. For this view, the supplier shall indicate whether the maps are built-in within the solution (i.e., offline) or whether GIS integration is required (i.e., online services). If GIS integration is a pre-requisite, the supplier shall give further details of the minimum requirements for integration.

3.3.2 Maintainability

3.3.2.1 The supplier shall provide a software management policy. The policy should at minimum have details on:

a) Software and firmware updates (patches) policy, testing, schedule and frequency

b) Bug and vulnerability (including zero day) assessment, identification and management

c) Software lifecycle management for the lifetime of the solution

3.3.2.2 The supplier shall provide a licence management policy. The policy shall at minimum have details on:

a) How licenses are generated, stored, distributed (and transferred, where licences are transferrable)

b) How licenses are allocated or consumed (by node, service, and/or module)

c) How licenses are accounted for (used vs unused vs available)

d) Detail the licensing model(s) on offer, (i.e., perpetual, subscription, etc.).

e) For licenses that require regular renewal interval, provide details on what happens on license expiration and/or default in payment

f) For licenses that require an “always on” online verification and/or validation, describe what the requirements are, and alternatives thereof.

3.3.3 Integration requirements

The integration into the ET OSS/BSS systems may be required and be developed by the supplier, in such a case the scope of the integration will be given to the supplier through engagements with ET NMC, Business Architecture and/or Technology stakeholders.

3.3.3.1 All supported open standard communication protocols shall be stated

3.3.3.2 Open standard secure protocols shall be implementable for the links between the NMS and the NEs. These shall be stated with a high level description provided.

3.3.3.3 The supplier shall detail and give full descriptions of all the North Bound Interfaces (NBI) available for integration into the Telecoms OSS/BSS

3.3.3.4 The supplier shall detail and give full descriptions of all the South Bound Interfaces (SBI) available for management of other devices

3.3.4 Data Communication Network requirements

The Data Communications Network (DCN) carries critical operations and management data throughout the network and ensures that all the NEs are functioning properly. It also provides the communications channel for management messages and alarms to inform the NMS of problems. It is critical to the overall health of the system, that the NMS continuously monitors all the NEs and that the traffic load is properly distributed

3.3.4.1 The supplier propose the DCN architecture for optimal implementation of the solution. The architecture shall detail at minimum:

a) Bandwidth requirements (NE to Gateway NE, Gateway NE to NMS, NE to NE, NE to NMS, etc)

b) Gateway NE requirements, and the maximum NEs that each gateway can handle

c) In-band / out-of-band configuration, protocols and feature benefits comparison and analysis

3.4 Functional requirements

3.4.1 Fault management

Fault management encompasses fault detection, isolation and the correction of abnormal operation in the telecommunications network. Faults, whether transient or persistent, cause systems to fail meet their operational objectives. Faults manifest themselves as particular events or errors in the operation of the system.

3.4.1.1 The NMS shall support functions to identify, isolate, troubleshoot and resolve faults and errors on its management scope (i.e., NEs, module/card, interface/port, links and services). These functions include, but not limited to:

a) Graphic visualisation of NE, module/card, interface/port, link and service failure;

b) Root-cause analysis and tracing of faults and errors;

c) Alarm severity customization, and suppression (masking);

d) Auto-discovery and viewing of NE, module/card, interface/port, link and service status.

e) Logging of errors and faults based on NE, module/card, interface/port, link and service alarms for examination by system administrators and with support of exporting these logs, without tampering with the logged events.

3.4.2 Configuration management

Configuration management ensures that all the network management solution, associated network elements and services are known and tracked at all times and any future changes to these are known and tracked. It enables functions like root cause analysis, impact analysis, change management, and current state assessment for future state strategy development (network planning).

3.4.2.1 The solution shall at minimum support the following configuration functions:

a) Maintain a configuration management database (CMDB) for setting and maintenance of configuration items and configuration baselines. Single item and bulk items configuration setting (and retrieval), including the creation and use of templates;

b) Configuration Status Accounting (CSA) of the configuration items of the NMS, NEs, module/card, interface/port, links and services are managed and tracked throughout their lifecycle (design/creation, deployment, and operational support) until disposal

c) Evaluate change requests and/or proposals and their subsequent approval or disapproval. This should include modifications to the NMS, NEs, module/card, interface/port, links and services (capacity planning and simulations).

d) Report and record configuration item descriptions and all deviations from the baseline during operation, maintenance and design.

e) Review and assess compliance with established performance requirements, design standards, and functional baselines (threshold setting and trend analysis).

3.4.3 Accounting management

Accounting Management is concerned with collecting resource consumption data to enable capacity planning and trend analysis, cost allocation, auditing and billing. It provides a key process to connect available performance and configuration data to business and operational targets.

3.4.3.1 The solution shall at minimum support the following accounting functions:

a) Trend analysis, simulations and/or capacity planning

b) Collating and reporting on inventory data, resource usage metrics including maintenance windows

c) Audit trail

d) Customer & service association (and support of user defined associations)

3.4.4 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. Its role is to gather and analyse statistical data for the purpose of monitoring and correcting the behaviour and effectiveness of the network, network elements, or other equipment and to aid in planning, provisioning, maintenance and the measurement of quality.

3.4.4.1 The solution shall at minimum support the following real-time and historical performance functions:

a) Definition and monitoring of performance measurements and thresholds (e.g., packet loss, latency, jitter, errored seconds, etc.)

b) Device and module/card health data monitoring, such as overall throughput, per-(sub) interface utilization, response time, CPU load, memory consumption, errors

c) Network, link and end-to-end service performance monitoring, such as utilization and errors per interface/link/service, quality of service (QoS). This shall be supported for real-time monitoring and also for historical (user configurable periods).

d) Support for automation of monthly service performance reports with an option to include out-of-service (maintenance windows).

e) Support for exporting and/or archiving of performance data to local and/or network storage and to email recipients

3.4.5 Security management

Security Management is a Network Management function that is about protecting both the network as a whole and the individual devices against intentional or accidental abuse, unauthorized access and communication loss.

Security Management is also responsible to set constraints per managed element, according to standards & specifications.

3.4.5.1 The solution shall at minimum support the following security management functions:

a) Authentication:

1) Local authentication (for fall back authentication method only) and remote authentication, for remote authentication, integration to TACACS, active directory (AD) and/or Lightweight Directory Access Protocol (LDAP) shall be supported

2) Strong authentication through the support of password expiration, and enforcement of strong passwords.

3) Multi-factor authentication that requires the usage of two or more authentication factors (e.g., combination of a knowledge factor and/or a possession factor and/or inherence factor, etc.).

4) User account management enabling the administrator to: Add users and roles, define priviledges, restrict user access to the network, monitor login and logout of users, force users to logout, lock user accounts, etc.

b) Authorisation

1) Role based access (per role, per user) – each role, and/or user, may have access to specific functions / views / network objects.

2) Role creation and removal (by the administrator)

3) Multiple users per role.

c) Segmentation of the network, by splitting the managed network into logical domains that can then be assigned to roles or users in order to restrict access to domains and NE

d) Secure Communication ensuring that the protocols used are secure and are configured with their secure features enabled.

3.4.5.2 The NMS shall be hardened. This includes activities such as:

a) Removal of unnecessary services and software packages that run on the server.

b) Database & OS customisation, to remove default security values

c) Elimination of plain text passwords and replacement with encrypted ones.

d) Ensuring custom SNMP credentials are used, instead of the default public/private credentials.

e) Ensuring that only secure protocols are used for communication with the NEs, e.g. Secure FTP (SFTP) instead of FTP, Secure Shell (SSH) instead of Telnet, etc.

4. Authorization

This document has been seen and accepted by:

Name and surname	Designation
Cornelius Naidoo	Telecomms T&S Middle Manager – PTM&C
Barry Clayton	Chief Engineer – Tx Secondary Plant, Work Planning and Centralised Services
Mfundiso Hina	Senior Manager – Eskom Telecommunications (Acting)
Lenah Mothata	Senior Manager – Grids
Botse Sikhwitshi	Senior Manager – Group Security (Acting)
Maureen Mokone	Senior Manager – GIT
Prudence Madiba	Senior Manager – Gx
Sikelela Mkhabela	Senior Manager – Dx

5. Revisions

Date	Rev	Compiler	Remarks
Oct 2020	3	B. Shezi	Revised the document based on learnings from other NMS deployments. The revision will ensure that the entire network management solution offered is designed, implemented and transferred to the operational area.

Date	Rev	Compiler	Remarks
Aug 2018	2	B. Shezi	Revised to incorporate learnings from NMS deployments and enquiries issued.
Feb 2015	1	E. Shabalala	First issue

6. Development team

The following people were involved in the development of this document:

- Bongani Shezi

7. Acknowledgements

The following people were consulted during the development of this document:

- Donald Moshoeshoe
- Eric Mabotja
- Jacques Schutte
- Kevin Plasket
- Kgomotso Setlhapelo
- Krupa Jose
- Matthew Taljaard
- Nontokozo Xulu
- Oscar Ngwenya
- Riyaz Gangat
- Sandy Nxumalo
- Tejin Gosai
- Vanessa Naidu
- Zwelandile Mbebe

Annex A – Schedule A/B

Item	Description	Schedule A (Eskom's requirement for this solution, indicate with an X)	Schedule B (Supplier's compliance statement)	Supplier's Reference/Comment (Supporting evidence)
3.1	**Solution architecture requirements**	State Compliance & Provide Evidence		
3.1.1	Software-based solution			
3.1.2	Hardware-based solution			
3.2	**Disaster recovery requirements**	State Compliance & Provide Evidence		
3.2.1	Availability requirements (including completion of Table 1: Recovery Objectives)			

Description/Criteria	Safety & Revenue Critical AND/OR Core Systems	Mission Critical	Business Critical	Normal to Non-Essential
RTO	0 – 1 Hour	8 – 24 hours	< 48 hours	>72 hours
RPO	No data loss	No data loss	Less than a day worth of data loss	>24 hours
DR Strategy	Active – Active	Active – Hot Standby	Active – Standby (Warm)	Active – Standby (Cold)
Eskom's requirement for this solution (Eskom to indicate, X)				
Minimum bandwidth required(supplier to specify)				
Maximum latency (supplier to specify)				
Maximum distance (supplier to specify)				

Item	Description	Schedule A (Eskom's requirement for this solution, indicate with an X)	Schedule B (Supplier's compliance statement)	Supplier's Reference/Comment (Supporting evidence)
3.2.2	Backup strategy			
3.3	**System specification**	State Compliance & Provide Evidence		
3.3.1	Accessibility			
3.3.2	Maintainability			
3.3.3	Integration requirements			
3.3.4	Data Communication Network requirements			
3.4	**Functional requirements**	State Compliance & Provide Evidence		
3.4.1	Fault management			
3.4.2	Configuration management			
3.4.3	Accounting management			
3.4.4	Performance management			
3.4.5	Security management			