

## **Annexure A**

Broadband OSS and ITSM Functional Requirements

## Contents

1. Background.....	3
2. Introduction .....	3
3. Network Inventory Management.....	3
3.1. Network asset location and tracking .....	3
3.2. Network Topology Visualisation and Orchestration .....	4
3.3. Capacity, Configuration and Change Management.....	4
3.4. Audit trail and reporting .....	4
4. Service Fulfilment.....	4
4.1. Order management .....	4
4.2. Service design and creation.....	5
4.3. Service provisioning and activation.....	5
4.4. Service modification and deactivation.....	5
4.5. NVF and SDN Management .....	5
4.6. Automation and self-organising networks (SON).....	6
4.7. Reporting and analytics .....	6
5. Workforce Management.....	6
5.1. Work order management .....	6
5.2. Field technical teams' management.....	6
5.3. Resource scheduling and allocation .....	6
5.4. Collaboration and communication.....	7
5.5. Cost and capacity management .....	7
6. Service Assurance .....	7
6.1. Network monitoring and visibility.....	7
6.2. Fault Management.....	7
6.3. Performance management .....	8
6.4. Incident management .....	8

6.5. Service quality management.....	8
6.6. Integration and interoperability.....	8
6.7. Security management.....	9
7. Trouble Ticketing.....	9
7.1. Ticket creation .....	9
7.2. Ticket categorisation and classification .....	9
7.3. Ticket assignment and escalation .....	9
7.4. SLA management and monitoring.....	10
7.5. Network monitoring.....	10
7.6. Reporting, analytics and integration.....	10
8. Information Technology Service Management (ITSM) Requirements .....	10
8.1. Service Request Management.....	11
8.2. Configuration Management Database (CMDB).....	11
8.3. Incident Management .....	11
8.4. Problem Management .....	11
8.5. Change Management .....	12
8.6. SLM and Knowledge Management.....	12
8.7. Release and Deployment Management.....	12
8.8. Asset Management, Automation and Orchestration .....	13
8.9. The user interface, Reporting and Analytics.....	13
8.10. Integration, Security and Compliance .....	13
8.11. Backup, Disaster Recovery and Business Continuity .....	14

## **1. Background**

SENTECH require an operational support system to manage and support its Broadband services, which include WIFI hotspots, 5G, IoT, and Cloud services. The company is rolling out a broadband network throughout the country on behalf of the state as part of the South Africa Connectivity project to underserved areas utilising fixed wireless (FW) technologies and VSAT via KA-band. SENTECH provides infrastructure services from the core to the WI-FI hotspot, which consists of backhaul, distribution, and fixed wireless access network connectivity. Sentech does NOT provide WI-FI services to the end users; this is done by the internet service providers (ISPs). The entity is installing a 5G network after piloting successful use cases, which will be commercialised soon. There are currently no cloud service offerings or software-defined networks, but the proposed system must-have the capability.

This system will be used for service fulfilment, service assurance, and managing the field support teams for broadband networks (FW, VSAT, 5G) and services. There is currently a technical team of about 250 potential users, with about 50 engineers and the rest operational and maintenance teams. The system is required to manage the network infrastructure and equipments, and environments related to a broadband site.

The ITSM module is required to manage ICT infrastructure and services and will mainly be utilised by the internal IT team of about 50 members. It must automate rudimental IT service requests, have a self-service portal for users and integrate with visualisation tools like Power BI.

## **2. Introduction**

OSS refers to the systems that support the day-to-day operations of a telecommunications network service provider to manage and control network infrastructure. It focuses on automating and streamlining network management, service provisioning, network configuration and maintenance, ensuring efficient and reliable performance.

The system must comply with the Telecommunication Management Forum (TMF) Next Generation Operational Support Systems (NGOSS) architecture framework to manage next-generation networks like 5G, cloud infrastructure, virtualisation and software-defined networks (SDN). The processes and relationship between applications for the system (OSS) must comply with the Telecommunication Applications Map (TAM). TMF's Open Digital Architecture (ODA) and Open API standards are recommended to ensure interoperability and simplify and reduce integration costs.

This document outlines the functional requirements for the system across the different domains and should cater for all teams, from service design to service assurance.

### **3. Network Inventory Management**

The system should maintain an accurate inventory of all network elements, and these are functional requirements:

#### **3.1. Network asset location and tracking**

- 3.1.1. Maintain a detailed inventory of all physical network assets like switches, routers, and other network equipment.
- 3.1.2. Manage logical resources like IP (V4 & V6) addresses, VLANs, subnets, virtual circuits and transport paths.
- 3.1.3. Manage virtual assets (VNFs, cloud resources, etc) utilised to offer services.
- 3.1.4. Capture and record the hierarchical relationship between different network resources.
- 3.1.5. Track the physical location of resources by showing them on a geographical map to enable efficient management of network resources.
- 3.1.6. Discover network elements and their configurations automatically to maintain up-to-date records.
- 3.1.7. Update the inventory dynamically as changes of network elements such as addition, removal, or modification happen.
- 3.1.8. Synchronise with network elements to ensure the live status of the state of equipment.
- 3.1.9. Import inventory from another system via API or manual CSV imports.

#### **3.2. Network Topology Visualisation and Orchestration**

- 3.2.1. Provide graphic visualisation of the network topology, showing interconnections between devices and network paths.
- 3.2.2. Show a multi-layered view of physical and logical topology, illustrating how services are mapped onto the physical infrastructure
- 3.2.3. Ability to drill down from a top layer for detailed information (site level to specific port).
- 3.2.4. Enable end-to-end orchestration of services across both physical and virtualised environments, managing services across multiple network layers and domains.

#### **3.3. Capacity, Configuration and Change Management**

- 3.3.1. Track the utilisation levels of network resources to assist with capacity planning
- 3.3.2. Trigger alerts when resources are approaching capacity limits

- 3.3.3. Maintain historical record of configurations for all network elements to enable rollback if required.
- 3.3.4. Track changes to physical and logical inventory, with details on who made the change, what was changed and the timestamp for the change.
- 3.3.5. Support change management process workflow to control changes
- 3.3.6. Provide real-time dynamic allocation and optimisation of network resources for 5G and network function virtualisation to ensure efficient use of resources and speed service delivery.

### **3.4. Audit trail and reporting**

- 3.4.1. Generate detailed audit logs of all actions performed on the network inventory
- 3.4.2. Generate reports on resource usage, inventory status and available resources.

## **4. Service Fulfilment**

Streamlining and automating processes associated with ordering, provisioning and activating customer services.

### **4.1. Order management**

- 4.1.1. Capture customer orders accurately and validate them against business rules, service eligibility and customer profiles.
- 4.1.2. Track orders from initiation to completion and provide status updates for internal users and customers.
- 4.1.3. Prioritise orders based on customer type, SLAs and business needs.
- 4.1.4. Detect incomplete or delayed orders and escalate for resolution.
- 4.1.5. Integrate with existing CRM tools / software

### **4.2. Service design and creation**

- 4.2.1. Maintain a catalogue of customer services, including service type.
- 4.2.2. Enable users to design service configurations using custom design or preferred templates.
- 4.2.3. Support using standardised service templates to speed up service delivery.

### **4.3. Service provisioning and activation**

- 4.3.1. Enable the provision of services, including configuration of network elements, customer premises equipment and software components.

- 4.3.2. Ensure services are activated after network configuration and resource allocation prerequisite are met.
- 4.3.3. Manage all workflows involving multiple systems and processes to ensure service provisioning.
- 4.3.4. Provide rollback mechanisms to reverse service provisioning if errors are detected in the workflow.
- 4.3.5. Perform tests on newly activated services to ensure verification.
- 4.3.6. Trigger billing once the service is activated and share the customer information with CRM.

#### **4.4. Service modification and deactivation**

- 4.4.1. Provide capabilities to modify existing customer service seamlessly without disruptions.
- 4.4.2. Manage the deactivation of services, ensure network resources are available, and adjust billing accordingly.

#### **4.5. NVF and SDN Management**

- 4.5.1. Support the complete cycle management of virtualised network functions (NVF), including creation, deployment, scaling, performance monitoring and retirement.
- 4.5.2. Integrate with software-defined networking (SDN) controllers to enable programmable and flexible control over network flows.
- 4.5.3. Facilitate the orchestration of NVFs to dynamically deploy network services across distributed environments, including edge and cloud computing platforms.

#### **4.6. Automation and self-organising networks (SON)**

- 4.6.1. Automate repetitive and routine network tasks for provisioning, configuration, and monitoring, reducing manual intervention and minimising errors.
- 4.6.2. Integrate SON features to enable 5G networks to automatically optimise performance, balance load, manage interference and perform self-healing.
- 4.6.3. Support closes-loop automation, real-time data from the network used to trigger configuration changes, adjustments and corrective actions automatically.

#### **4.7. Reporting and analytics**

- 4.7.1. Generate reports on service fulfilment performance, including average order completion times, errors, and resource utilisation.
- 4.7.2. Track customer satisfaction through order accuracy, lead time to service activation, and first-time success rate.

## **5. Workforce Management**

Workforce management objectives are to optimise the use of human resources, comply with regulations and legislation, and meet service needs while being cost-efficient.

### **5.1. Work order management**

- 5.1.1. Create work orders linked to network faults, schedule maintenance and customer activation requests and assign unique reference numbers.
- 5.1.2. Prioritise work orders based on the severity of network failures and SLAs
- 5.1.3. Provide live updates on the status of work orders, showing progress and completion.

### **5.2. Field technical teams' management**

- 5.2.1. Enable field technical personnel to receive job cards, report status, and provide updates via mobile devices.
- 5.2.2. Track the location of field resources and optimise travel routes.
- 5.2.3. Provide live status updates of all job cards and resources available for job allocations.
- 5.2.4. Track field resources' working hours and time to complete tasks and reconcile based on allocated rates.

### **5.3. Resource scheduling and allocation**

- 5.3.1. Assign tasks to the right employees based on their skills, availability, and proximity to the task location.
- 5.3.2. Match resources with available jobs based on their competencies.
- 5.3.3. Ensure fair distribution of workload to all available resources.
- 5.3.4. Support changes in work schedules due to unexpected, unplanned changes.

### **5.4. Collaboration and communication**

- 5.4.1. Enable communication between field support teams and the dispatching team.
- 5.4.2. Provide a collaboration tool to resolve complex network incidents
- 5.4.3. Offer a platform for knowledge management and support for field technical teams.

### **5.5. Cost and capacity management**

- 5.5.1. Monitor and track operational labour costs to control and optimise operational expenses.
- 5.5.2. Align workforce assignment to budget allocations to ensure efficient use of financial resources.
- 5.5.3. Monitor workforce capacity to ensure optimal utilisation of resources.



- 5.5.4. Track performance indicators like completion rates, schedule adherence, and time spent on site.

## **6. Service Assurance**

Service assurance ensures the optimal functioning of services by continuously monitoring, managing and improving network performance, availability and quality.

### **6.1. Network monitoring and visibility**

- 6.1.1. Provide monitoring and visibility of all network elements, resources and services across the network.
- 6.1.2. Detect real-time anomalies, equipment and service failures, and network faults.
- 6.1.3. Offer multi-layer visibility across the network's physical, virtual and service layers.
- 6.1.4. Capability to monitor at granular levels and customer-specific networks and services.

### **6.2. Fault Management**

- 6.2.1. Detect faults and generate alarms when there is degradation in service and or network performance.
- 6.2.2. Send notifications and alerts when network alarms are generated via multiple channels (email, SMS, etc).
- 6.2.3. Provide root cause analysis and isolation of network faults.
- 6.2.4. Classify alarms based on severity and business impact.
- 6.2.5. Follow a predefined fault escalation process when sending alerts.
- 6.2.6. Enable predefined automated actions to ensure service continuity.

### **6.3. Performance management**

- 6.3.1. Monitor key-defined parameters to ensure network and service performance meet targets.
- 6.3.2. Store network performance data and enable in-depth network performance analysis and trending
- 6.3.3. Enforce performance thresholds based on SLAs and trigger alarms when performance drops below the set targets.
- 6.3.4. Support proactive resource allocation and optimisation to avoid performance degradation.
- 6.3.5. Provide customisable dashboards that show the live performance of customer networks and performance analysis and reports.
- 6.3.6. Generate network performance reports based on preconfigured schedules.

## **6.4. Incident management**

- 6.4.1. Log incident automatically as triggered by a network fault and assign a unique reference number.
- 6.4.2. Allow manual logging of incidents and issue a unique reference number.
- 6.4.3. Categorise the incident based on severity (minor, major, critical) and type (hardware, software, etc).
- 6.4.4. Classify the incident based on impact and SLA.
- 6.4.5. Enable escalation of incidents to the next level of support
- 6.4.6. Provide options to suspend the incident and stop the counter
- 6.4.7. Close the incident with root cause analysis
- 6.4.8. Enable the creation of a change request from the incident

## **6.5. Service quality management**

- 6.5.1. Monitor customer network and services based on defined parameters.
- 6.5.2. Provide an option for testing and validating services before deployment to minimise customer impact.
- 6.5.3. Capability to anticipate potential network failures based on historical data.

## **6.6. Integration and interoperability**

- 6.6.1. Integrate with network elements from different vendors and across various technologies, supporting multi-protocol and multi-domain environments.
- 6.6.2. Enable integration of third-party systems using standardised APIs and interfaces, allowing for better orchestration and automation.
- 6.6.3. Support management and monitoring of virtual and software-defined networks seamlessly and provide dynamic control of services.

## **6.7. Security management**

- 6.7.1. Monitor and detect network security threats, like DDoS attacks and data breaches.
- 6.7.2. Manage and control access to network resources based on job profiles and locations.
- 6.7.3. Support adherence to regulatory and compliance standards, ensuring operations are aligned with data privacy and security requirements.

## **7. Trouble Ticketing**

Trouble ticket enables customers to report network-related incidents or any other service query using various channels.

## **7.1. Ticket creation**

- 7.1.1. Enable manual creation of tickets through a user interface for the network monitoring team, specifying pre-selected fields to populate with drop-down options.
- 7.1.2. Enable customers to create tickets via multiple channels (web portal, app, messaging, etc) for service-related issues (billing errors, service outages, etc).
- 7.1.3. Generate tickets automatically when service assurance systems detect network and service anomalies.
- 7.1.4. Allow for bulk ticket creation of affected customers in a specific service area.
- 7.1.5. Issue a unique reference number for each trouble ticket and enable grouping of tickets affected by the same network outage.

## **7.2. Ticket categorisation and classification**

- 7.2.1. Enable service-specific categorisation of tickets.
- 7.2.2. Categorise all tickets geographically per region, town, PoP or base station.
- 7.2.3. Classify tickets by fault types (service outage, congestion, device failure, etc).

## **7.3. Ticket assignment and escalation**

- 7.3.1. Route and assign tickets automatically based on service type, fault location and resource availability.
- 7.3.2. Route and assign tickets to support teams with the necessary skills based on specific service types.
- 7.3.3. Assign tickets to correct field technical teams for onsite support when escalated to that region.
- 7.3.4. Enable automatic escalation based on time, severity, impact, and non-responsiveness, with notifications sent to the next management level.

## **7.4. SLA management and monitoring**

- 7.4.1. Track and escalate SLA violations based on service types, priorities, and customer contracts to relevant support teams and notification to management.
- 7.4.2. Manage different SLAs based on customer and product types and network service
- 7.4.3. Enable real-time tracking of ticket progress against SLAs and highlight those close to the violation.

## **7.5. Network monitoring**

- 7.5.1. Integrate with monitoring tools and systems to generate tickets for service degradation, equipment failures, capacity issues and network outages.
- 7.5.2. Group multiple tickets related to the exact root cause into a single incident for easy handling.
- 7.5.3. Notify customers in the affected area when an incident is created and resolved.
- 7.5.4. Integrate with workforce management to assign tickets to available resources based on skills, proximity and availability.
- 7.5.5. Integrate with the inventory system to track the availability and use of spare parts during repairs.
- 7.5.6. Provide an interface for operation teams to view, update tickets and report on progress on the go.

## **7.6. Reporting, analytics and integration**

- 7.6.1. Generate reports on crucial service metrics (MTTR, etc) for internal use and regulatory reporting.
- 7.6.2. Track individual and team performance metrics related to the number of tickets resolved, average time to restore, etc.
- 7.6.3. Provide a live dashboard for management to view trouble tickets generated and status updates.
- 7.6.4. Analyse historical ticket data to identify trends, recurring issues and underperforming areas.
- 7.6.5. Integrate with the billing system to link customer trouble tickets to billing issues
- 7.6.6. Integrate with CRM to pull customer details and track interactions.

## **8. Information Technology Service Management (ITSM) Requirements**

The system must cater to effective IT service delivery, management, and continuous improvement by handling the complete lifecycle of IT services.

### **8.1. Service Request Management**

- 8.1.1. Offer a catalogue of IT services, enabling users to browse and request services.
- 8.1.2. Automate the fulfilment process of service requests, ensuring that approvals, deployments and notifications are triggered automatically.
- 8.1.3. Provide a self-service portal for users to submit, track and manage their service requests and incidents.

- 8.1.4. Track service level management for requests and ensure compliance with predefined timelines.

## **8.2. Configuration Management Database (CMDB)**

- 8.2.1. Maintain a detailed database of all IT configuration items (CIs), including hardware, software, network components, and their relationships.
- 8.2.2. Ability to model and visualise relationships between configuration items, their relationships and dependencies.
- 8.2.3. Track changes made to configuration items with detailed audit logs and timestamps.
- 8.2.4. Evaluate how incidents, problems and network changes affect other configuration items and IT services.

## **8.3. Incident Management**

- 8.3.1. Ability to log and track network incidents with unique identifiers, timestamps and detailed descriptions.
- 8.3.2. Categorise incidents automatically based on pre-defined criteria
- 8.3.3. Assign incident priorities based on severity, impact, and urgency. Link incident priority to trigger escalations and specific actions.
- 8.3.4. Escalate open incidents automatically to next-level support and management based on timeframes, severity and impact.
- 8.3.5. Notify users and IT staff of incidents via emails, messaging or push notifications, with the ability to track responses and status updates/
- 8.3.6. Track the resolution of the incident, ensure proper closure process after resolution, and seek customer satisfaction feedback.

## **8.4. Problem Management**

- 8.4.1. Ability to identify and log recurring incidents as IT problem
- 8.4.2. Provide tools for investigating and documenting the root causes of the IT problems (RCA).
- 8.4.3. Store known workarounds and already developed solutions to known problems and make them accessible to IT personnel.
- 8.4.4. Enable workflows for managing the investigation and resolution of problems, tracking progress and closure.

## **8.5. Change Management**

- 8.5.1. Enable the submission of change requests with predefined templates on required information.
- 8.5.2. Implement a multi-level approval process for evaluating and authorising changes based on risk, impact, priority and business justification.
- 8.5.3. Provide a change calendar that allows changes to be scheduled based on available windows, avoiding conflicts with prior changes or critical business operations.
- 8.5.4. Analyse changes' risk and potential impact, including dependency mapping to other systems or services.
- 8.5.5. Provide a rollback plan option for each change should implementation issues arise.
- 8.5.6. Record the results of implemented changes, either successful or unsuccessful.

## **8.6. SLM and Knowledge Management**

- 8.6.1. Define SLAs for different services and measure compliance based on response time, resolution, and customer satisfaction.
- 8.6.2. Monitor and enforce SLAs, triggering alerts and escalations if service level breaches are detected.
- 8.6.3. Generate SLA performance reports with performance trends.
- 8.6.4. Enable IT personnel to create and manage a knowledge base for troubleshooting guides, workarounds, FAQs and solutions to common problems.
- 8.6.5. Integrate knowledge base with the incident, problem, and change management processes to resolve anomalies faster.

## **8.7. Release and Deployment Management**

- 8.7.1. Plan and manage software and hardware releases to ensure they are scheduled to minimise impact on business operations.
- 8.7.2. Manage test and staging environments to validate releases before deploying them to production.
- 8.7.3. Ensure the relevant stakeholders approve all network releases before deployment.
- 8.7.4. Maintain a history of all release versions, network changes, fixes, updates and upgrades.

## **8.8. Asset Management, Automation and Orchestration**

- 8.8.1. Maintain a complete inventory of all IT assets (hardware, software, licenses, etc) with details like commission dates, warranty and status.
- 8.8.2. Track assets throughout their lifecycle, from procurement to decommissioning, including maintenance and upgrades.
- 8.8.3. Monitor licenses, track usage and ensure compliance with vendor agreements.
- 8.8.4. Automate routine tasks and approvals using customisable workflows.
- 8.8.5. Integrate with equipment and network monitoring tools to raise alerts when critical events are detected.
- 8.8.6. Automate service request fulfilments of routine user requirements to reduce manual intervention.

## **8.9. The user interface, Reporting and Analytics**

- 8.9.1. Provide a clean, intuitive interface that IT personnel and end-users can navigate easily.
- 8.9.2. Enable end-users to report incidents and issue service requests via multiple channels (portal, email, chat, etc).
- 8.9.3. Provide mobile access to the ITSM system for users and IT personnel.
- 8.9.4. Provide real-time dashboards to display performance indicators based on predefined needs.
- 8.9.5. Provide reports on various ITSM activities with performance trends.

## **8.10. Integration, Security and Compliance**

- 8.10.1. Integrate with enterprise systems like ERP, CRM, monitoring tools and DevOps tools to streamline ITSM workflows.
- 8.10.2. Integrate with custom and external applications using open APIs.
- 8.10.3. Implement role-based access control (RBAC) permissions, ensuring users have access only to the functionalities and data relevant to their roles.
- 8.10.4. Enforce multi-factor authentication (MFA) for system access to privileged users.
- 8.10.5. Ensure sensitive data are encrypted in transit and at rest using secure protocols.
- 8.10.6. Maintain detailed audit logs of all system activities and generate reports on compliance with standards and regulations.
- 8.10.7. Enable enforcement of security policies in line with organisational security guidelines.
- 8.10.8. Ensure all system modules comply with industry standards and ITIL principles.

## **8.11. Backup, Disaster Recovery and Business Continuity**

- 8.11.1. Implement automatic and regular backups to ensure data recovery during failures.
- 8.11.2. Ensure all backup data is encrypted and stored securely, onsite and offsite, with access controls in place.
- 8.11.3. Develop and test a disaster recovery plan to ensure services continue during significant failures and disasters
- 8.11.4. Implement failover mechanisms to ensure continuity of services when there are hardware or software failures.