Vodacom Business
Enterprise Customer Support Guide

2020
June

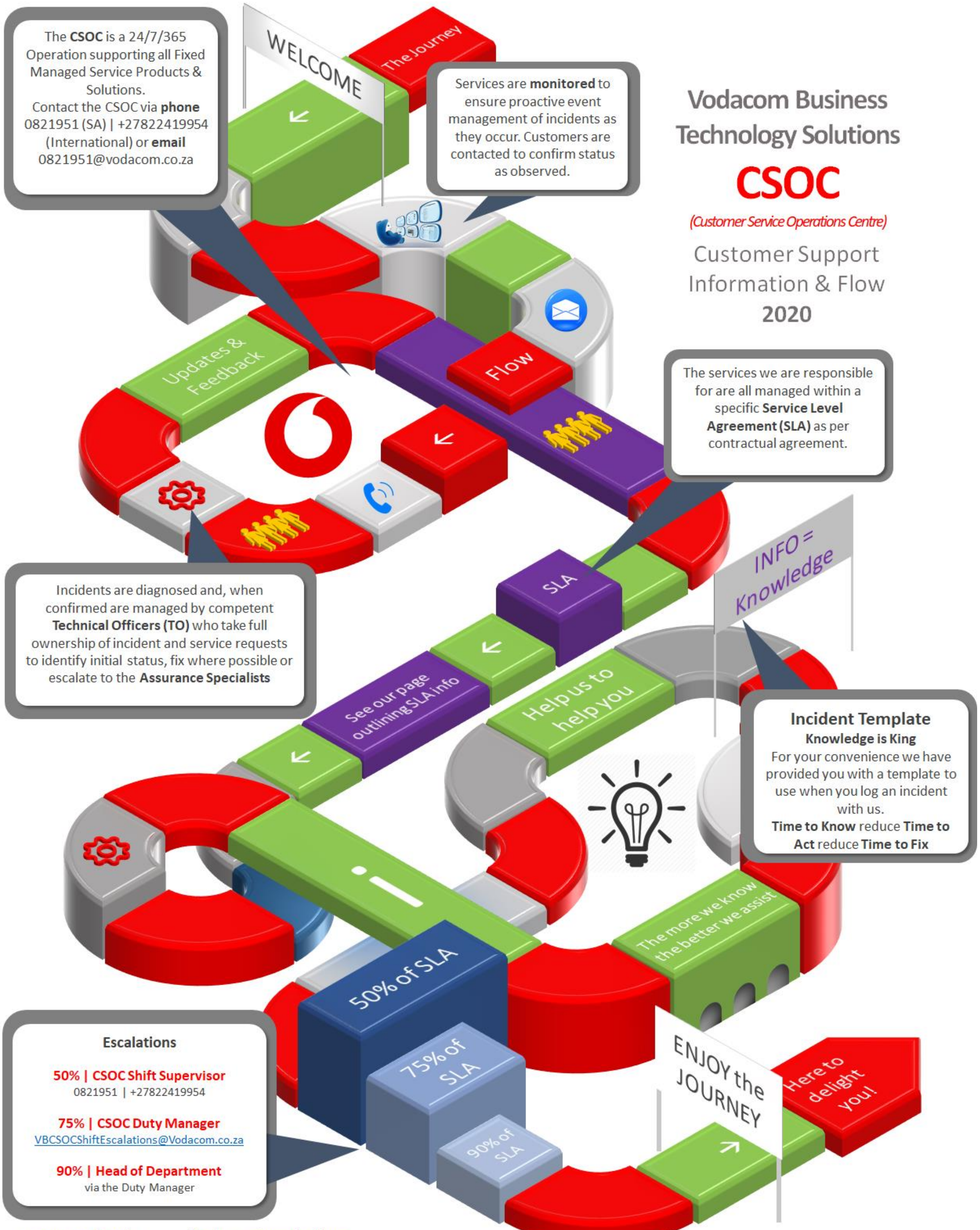
Vodacom Business Technology Solutions

CSOC

(Customer Service Operations Centre)

Customer Support Information & Flow

2020



The **CSOC** is a 24/7/365 Operation supporting all Fixed Managed Service Products & Solutions.
Contact the CSOC via **phone** 0821951 (SA) | +27822419954 (International) or **email** 0821951@vodacom.co.za

Services are **monitored** to ensure proactive event management of incidents as they occur. Customers are contacted to confirm status as observed.

The services we are responsible for are all managed within a specific **Service Level Agreement (SLA)** as per contractual agreement.

Incidents are diagnosed and, when confirmed are managed by competent **Technical Officers (TO)** who take full ownership of incident and service requests to identify initial status, fix where possible or escalate to the **Assurance Specialists**

Incident Template
Knowledge is King
For your convenience we have provided you with a template to use when you log an incident with us.
Time to Know reduce **Time to Act** reduce **Time to Fix**

Escalations

50% | CSOC Shift Supervisor
0821951 | +27822419954

75% | CSOC Duty Manager
VBCSOCShiftEscalations@Vodacom.co.za

90% | Head of Department
via the Duty Manager

Our Purpose and Promise

We are the technology support extension of Vodacom Business.
We are the single point of contact for all the Fixed Managed Services Products and Solutions purchased from Vodacom Business.

We value our customers and we take your business seriously. We have adopted and implemented a culture of **Extreme Ownership**. Our technical support teams are professional individuals who not only give you the best service in the industry but also leave you with a smile on your face at every contact point.

If you feel we have delighted or disappointed you in any way, please feel free to summarize your experience (good or bad) in 5 to 10 bullet points and send directly to the Executive Head of the Customer Service Operations Centre at: carel.denysschen@vodacom.co.za

www.vodacombusiness.co.za
0821951@vodacom.co.za
0821951 (Local)
+27822419954 (International)

Vodacom
Stay Safe

Table of Contents

Introduction

The purpose of this document is to describe the standard practices in place and procedures to be followed for all services delivered to the Customer, and managed by Vodacom Business through the Customer Service Operations Centre (CSOC). This Customer Support Guide serves as a practical reference and is intended to answer questions related to the operational processes by which a Vodacom Business customer's fixed line services are managed.

1. The CSOC

Vodacom Business aims to deliver high quality management and support services through the CSOC. The CSOC manage customers' services and the associated contracted service levels for all services offered within the Vodacom Business product range. The CSOC operates 24 hours per day, 7 days a week and 365 days of the year to manage customer services.

1.1 (TSD) Technical Service Desk with Assurance

a. The teams of technical officers are on duty 24/7/365. With predefined shift schedules and standby rosters to ensure commitment and focus to customer service.
b. The SD is the first line for support and troubleshooting. This service to our customers is available to register incidents and service requests as reported by the monitoring systems and customer.
c. This team respond to event management through the Vodacom Business monitoring systems and they identify and take ownership of any incidents logged.
d. The team is responsible for providing accurate initial assessment of reported incidents and service requests including categorisation and prioritisation of service requests.
e. The SD takes ownership of incidents and service requests from initiation until resolution.
f. They report outages to the relevant 3rd party vendors, manage vendor escalations and communicate progress to the customer.
g. Provide the customer with updates on the progress of incident or service request resolution.
h. Assurance Technical Officers Specialising in Networks, Security, Hosting and VOIP.

1.2 Monitoring Team

This specialist monitoring team constantly monitor alarms triggered by possible service affecting events. These alarms are followed up with customer notifications and calls to determine affected site electricity availability. Customer edge (CE) Devices managed by Vodacom Business on behalf of the customer, will be polled by the Fault Management tool. ICMP pings are sent with a frequency of 20 seconds and SNMP every 5 minutes. If an ICMP ping fails, the tool will send a set of retries. If the retries fail, an alarm is generated.

2. Operational and Performance Management Procedures

The management and monitoring of the Customer network is done by our Customer Service Operations Centre (CSOC). Vodacom Business Services follows a best practice ITIL® approach to managing Customer services. The CSOC is highly skilled in various disciplines, including ITIL and technology specific certifications and is the first point of call for incident and service management.

Fixed line services are monitored, events are logged and tracked through Service Requests (SR's) as well as incidents managed to resolution through the Service Desk and Assurance departments.

- ➢ The CSOC provides a full set of OSS/BSS solutions across the full range of Network Management and Performance management systems to ensure a professional end to end display of the entire network specific for customer design and solutions.
- ➢ The results are presented in graphical reports and are available on the Vodacom Business Web portal **http://www.vodacombusiness.co.za/business/home**

2.1 Logging a Service Request

a. Vodacom Business is committed to proactively monitoring all managed services. We aim to isolate and resolve incidents before they cause any major disruption to services, thereby minimising the impact on the customer's network. However, in the event of a service disruption or outage, this should be reported immediately to the CSOC.

b. Service disruptions or failures can be reported to the CSOC through the following mediums:

   - ➢ **Phone:** 082 1951 (Local within RSA) and +27 82 241 9954 (International)
   - ➢ **Email:** 0821951@vodacom.co.za

c. Only authorised customer contacts that are registered with Vodacom Business will be able to log calls on behalf of the customer.

d. The following information is required when contacting the CSOC via telephone or email: Incident Logging Template below Appendix 2.

e. Upon receipt of this information the CSOC SD technical officer will log a service request in the Vodacom Business service request management tool. The customer will be provided with a service request reference number and for all subsequent calls made for the open service request this reference number must be quoted.

f. The logging of a service request triggers the Incident Management and Request Fulfilment process.

2.2 Incident Management and Request Fulfilment

The Incident Management and Request Fulfilment process handles events that affect the normal operation of an existing service and the fulfilment of requests for minor configuration changes to existing services. The Service Levels as agreed upon in the customer specific Service Level Agreement (SLA) are monitored and adhered to for incidents as well as requests.

a) Opening a SR (Service Request)

i. The CSOC technical officer will log the incident in the SRM (Service Request Management) System as per service request priority levels. If the incident SR (Service Request) already exists, the history of that ticket will be updated when follow up contact is made.

ii. If the CSOC technical officer acknowledges an alarm and logs it in the SRM tool before the customer has made contact, the CSOC technical officer will contact the customer authorised contact by telephone or email to inform them of the incident and to provide the Service Request reference number. For all subsequent calls made for the open service request this reference number must be used.

b) Incident Investigation, Diagnosis and Resolution:

i. CSOC SD will utilise the information provided by the customer and information gathered from related incidents and tools to determine the appropriate resolution. If a resolution cannot be found, the SR will be escalated to CSOC 2nd line support, thereby transferring ownership of the SR in the process. If the incident specialist is a 3rd party supplier or partner, or if the incident is isolated to a service provider incident, the service provider incident reporting process will be triggered.

ii. CSOC assurance will take ownership of a SR escalated to them. The assurance specialist will attempt to resolve the fault. If they require further technical assistance, they will use the services of the Escalation/Infrastructure team to find resolution. The ownership of the SR remains with the assurance team.

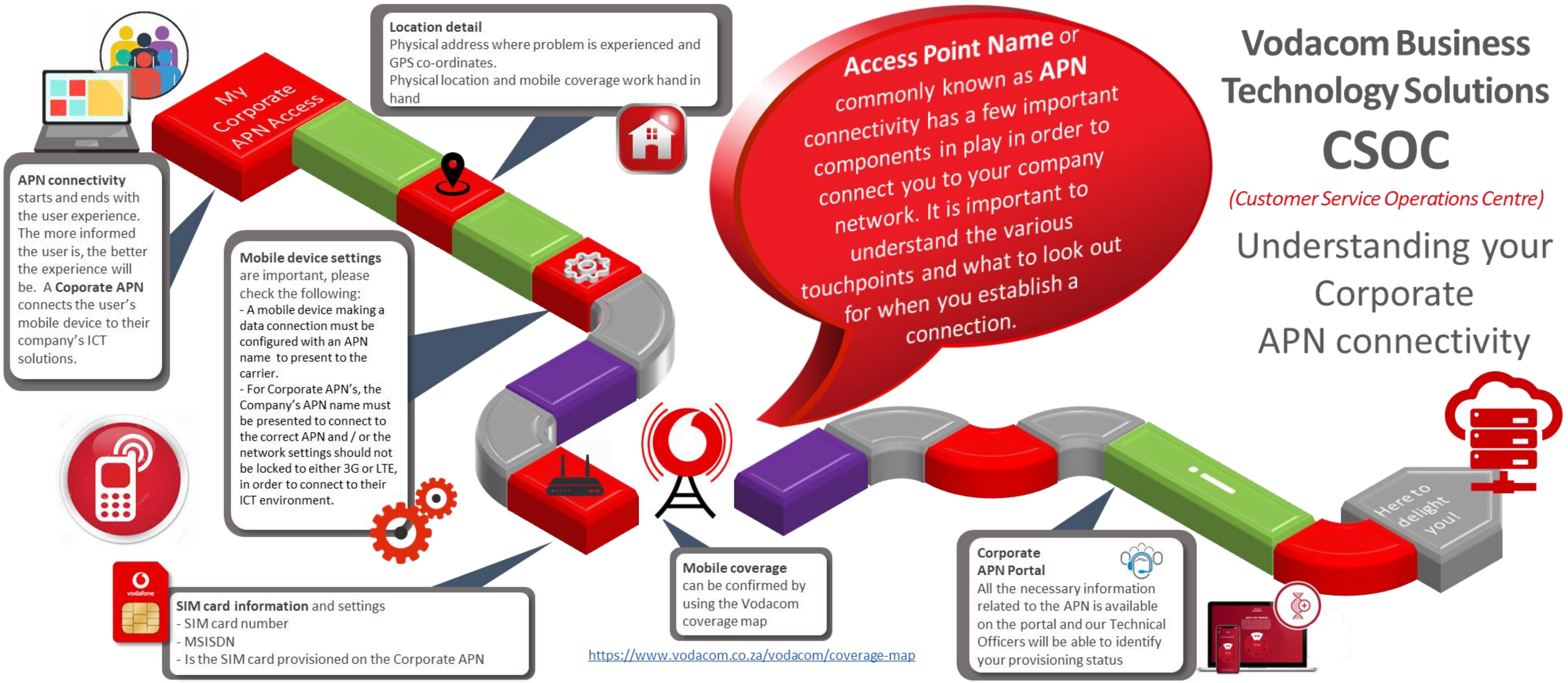
iii. The senior network engineers that form part of the Escalations Team will consult on Service Requests which are escalated to them however ownership of the SR will remain with 2nd line support. The Escalations Team will find a resolution for the incident; they will perform the resolution and provide feedback to the assurance team that owns the SR.

c) Service Request Closure

i. The actions taken by the CSOC SD & Assurance support, or the escalation team will be recorded against the SR reference number once a resolution has been found and the service tested to ensure the incident has been resolved.

ii. If the customer is satisfied with the resolution, the SR will be closed on the SRM system.

2.3 Understanding your Corporate APN connectivity



APN connectivity starts and ends with the user experience. The more informed the user is, the better the experience will be. A **Coporate APN** connects the user's mobile device to their company's ICT solutions.

Location detail
Physical address where problem is experienced and GPS co-ordinates.
Physical location and mobile coverage work hand in hand

Mobile device settings are important, please check the following:
- A mobile device making a data connection must be configured with an APN name to present to the carrier.
- For Corporate APN's, the Company's APN name must be presented to connect to the correct APN and / or the network settings should not be locked to either 3G or LTE, in order to connect to their ICT environment.

SIM card information and settings
- SIM card number
- MSISDN
- Is the SIM card provisioned on the Corporate APN

Mobile coverage can be confirmed by using the Vodacom coverage map

https://www.vodacom.co.za/vodacom/coverage-map

Corporate APN Portal
All the necessary information related to the APN is available on the portal and our Technical Officers will be able to identify your provisioning status

Access Point Name or commonly known as **APN** connectivity has a few important components in play in order to connect you to your company network. It is important to understand the various touchpoints and what to look out for when you establish a connection.

Vodacom Business Technology Solutions

CSOC

(Customer Service Operations Centre)

Understanding your Corporate APN connectivity

APN Technology

An APN exists in the GSM Network and is the gateway between a GPRS, 3G or 4G network and your company's corporate network. It also has other uses such as connectivity for various IoT solutions. It allows a mobile device to authenticate and connect on a specific network using the GSM technology. It allows connectivity between the mobile end user and another computer network wherever the end user is located, and where they have a mobile connection with a GSM network.

Two types of APN connectivity exists, **Corporate APN** and Public APN. **Corporate APNs** are used by companies to allow remote users to connect to their corporate IT systems. Public APNs are used by Joe Public to connect from a mobile device to the World Wide Web.

Vodacom Business via the CSOC is responsible to support your Corporate APN service.

It is important for us to ensure you understand the components involved and inter-technology dependencies required to provide the service, and we are pleased to present to you this document to explain some of the details behind APN technology.

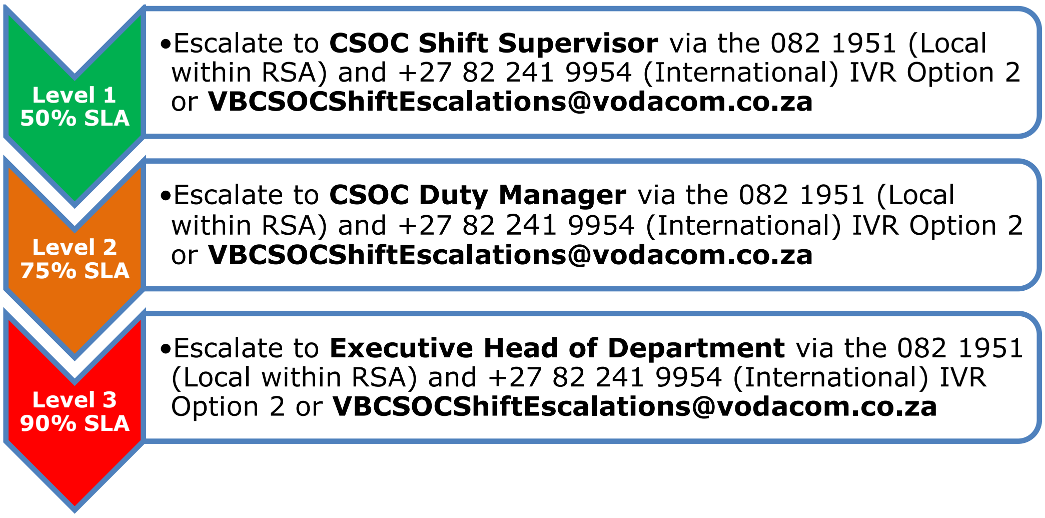
www.vodacombusiness.co.za
0821951@vodacom.co.za
0821951 (Local)
+27822419954 (International)

Vodacom Stay Safe

SR Priority Levels		
Level	**Target times**	**Description**
0 – Infrastructure	Notification 30min TTR – Per Specific SLA Escalations: 50%=2hrs 75%=3hrs	An infrastructure failure has occurred that is affecting multiple customers' services. CSOC will respond to **Priority 0 incidents** immediately and will update all customers with bulk notifications every 30 minutes, or negotiated period, on the progress and status of the call. Escalations will happen as per the escalation process.
1 – Critical	Notification 30min TTR – 4hrs Escalations: 50%=2hrs 75%=3hrs	Overall loss of service due to a network outage or system failure on business-critical systems with potential loss of income if the services are not restored within 4 elapsed hours. CSOC will respond to **Priority 1 incidents** as per SLA and will update the customer every 30 minutes, or negotiated period, on the progress and status of the call. Escalations will happen as per the escalation process.
2 – Severe	Notification 30min TTR – 8hrs Escalations: 50%=4hrs 75%=6hrs	Fractional loss or interruption of customer's service, i.e. customer experiences slow responses, service degradation. With potential loss of income if the service is not restored within 8 elapsed hours. CSOC will respond to **Priority 2 incidents** within 30 minutes and will update the customer every 60 minutes, or negotiated period, on the progress and status of the call. Escalations will happen as per the escalation process.
3 – Medium	Notification 30min TTR – 16 Escalations: 50%=8hrs 75%=12hrs	Additions or changes to rule sets or minor service disruptions to single users – nonbusiness critical, with no potential loss of income. The service will be restored within **16 business hours**. CSOC will respond to **Priority 3 incidents** within 4 hours and will update the customer every 4 hours, or negotiated period, on the progress and status of the call. Escalations will happen as per the escalation process.
4 – Low	Notification 30min TTR – best effort Escalations: None	**Non-service affecting** requests and enquiries. Ad hoc telephone calls and resolution will be determined by the amount of work that needs to be performed. The customer will be updated on Priority 4 incident or requests as negotiated.

2.4 Escalation Procedure

In the event that the customer feels an incident is not being treated with the necessary urgency, the customer may request to escalate this incident to the next management level.



Level 1
50% SLA

- Escalate to **CSOC Shift Supervisor** via the 082 1951 (Local within RSA) and +27 82 241 9954 (International) IVR Option 2 or **VBCSOCShiftEscalations@vodacom.co.za**

Level 2
75% SLA

- Escalate to **CSOC Duty Manager** via the 082 1951 (Local within RSA) and +27 82 241 9954 (International) IVR Option 2 or **VBCSOCShiftEscalations@vodacom.co.za**

Level 3
90% SLA

- Escalate to **Executive Head of Department** via the 082 1951 (Local within RSA) and +27 82 241 9954 (International) IVR Option 2 or **VBCSOCShiftEscalations@vodacom.co.za**

Customer Service Operations Centre (CSOC)

Escalation Matrix

For Business Partners, Account Managers and Service Managers

(All escalations - Business hours, Afterhours and Weekends, to follow this process)

CSOC First Point of Contact (ALL HOURS)	
1st Line Support and Incident Management	
Email	0821951@vodacom.co.za
Telephone	082 1951
CSOC First Escalation (ALL HOURS)	
Shift Supervisor	
Email	VBCSOCShiftEscalations@vodacom.co.za
Telephone	082 1951, Option **2** *for Escalations* • *3 x Shift Supervisors during Business Hours,* • *1 x Shift Supervisor After Hours & Weekends*
CSOC Second Escalation (ALL HOURS)	
Service Desk Manager and Standby Duty Manager	
Business Hours	Service Desk Manager
After Hours	CSOC Supervisor on duty and Standby Duty Manager
Note:	Incident Management and Escalations need to be managed as per agreed service description and within the guidelines as outlined in the Customer Support Guide.

Customer Service Operations Centre (CSOC) Contact List

CSOC Service Desk	
Manager: Service Desk	**Ebrahim Aziz (DoA)**
Email	Ebrahim.Aziz@vcontractor.co.za
Telephone	079 524 9998
CSOC Assurance and Escalations	
Manager: Assurance and Escalations	**Mark Prinsloo**
Email	Mark.Prinsloo@vodacom.co.za
Telephone	082 992 7420
Executive Head of Division: CSOC	
EHOD: CSOC	**Carel de Nysschen**
Email	Carel.DeNysschen@vodacom.co.za
Telephone	082 991 0642

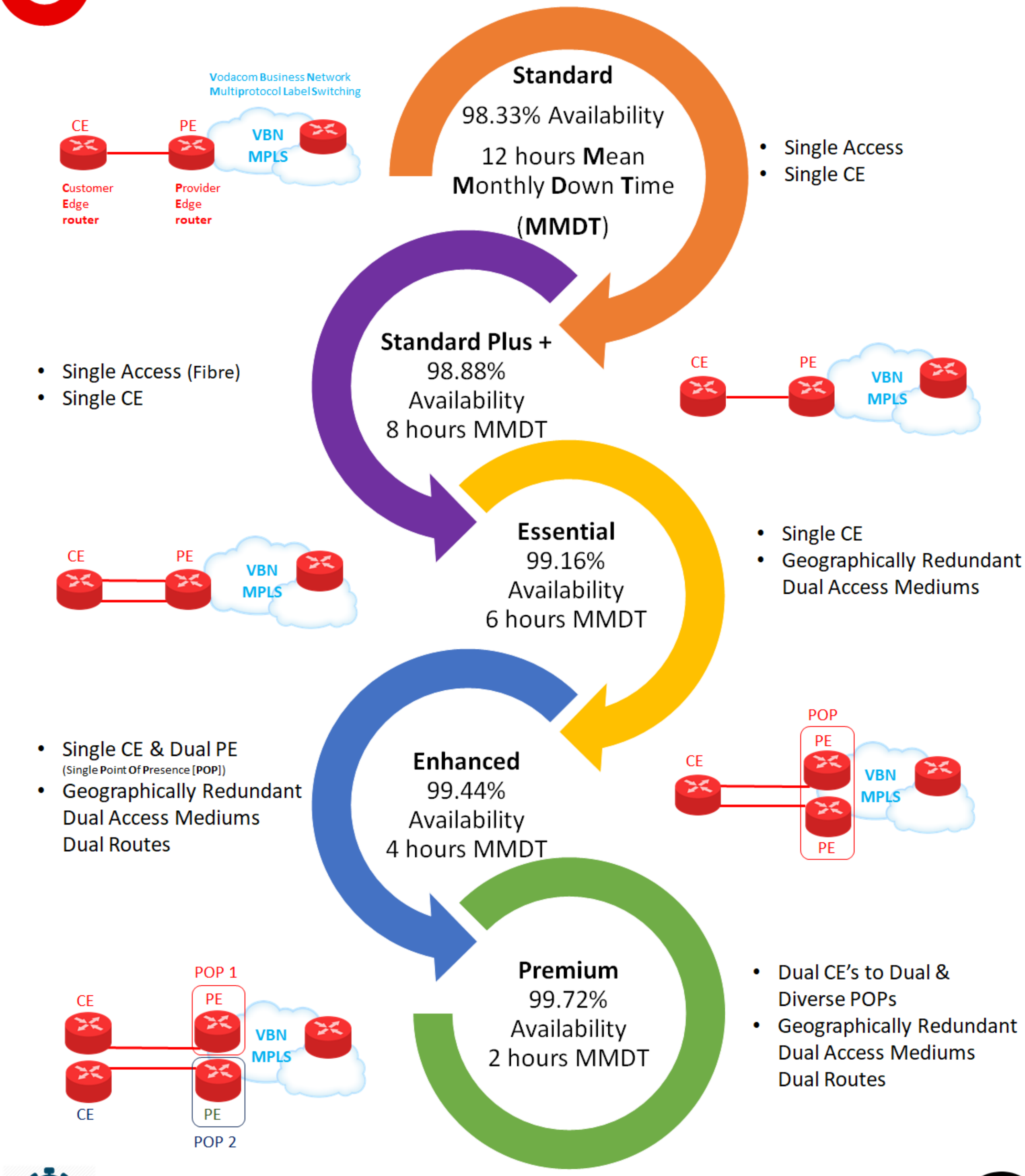
2.5 Service Level Management

a. Service Level Management and reporting is viewed as fundamental to the management of services and contracts. The intention is to ensure an optimal service level with minimum risk to the customer business. Service Level Measurement, fault and performance monitoring begins once a service is active.

b. When there is a dedicated Service Manager then Service level reviews will be scheduled with the customer representatives at agreed intervals. In this session, the service targets will be reviewed and actions to be taken to ensure that targets are met will be discussed, and status of open actions presented. Service Level Reports are generated at the end of a month. The first report can be requested at the month end following the month in which the service was commenced.

c. Vodacom Business provides product specific SLA's detailing measurable metrics and operational guidelines that govern the different products. A general SLA is also provided in the contract pack that encompasses overall operational targets for the solution including response and resolution targets. Timescales are agreed between Vodacom Business and the customer for the stages of incident handling, based upon these response and resolution targets.

Service Level Agreement (SLA)



Standard
98.33% Availability
12 hours **M**ean **M**onthly **D**own **T**ime (**MMDT**)

- Single Access
- Single CE

Standard Plus +
98.88% Availability
8 hours MMDT

- Single Access (Fibre)
- Single CE

Essential
99.16% Availability
6 hours MMDT

- Single CE
- Geographically Redundant Dual Access Mediums

Enhanced
99.44% Availability
4 hours MMDT

- Single CE & Dual PE (Single Point Of Presence [POP])
- Geographically Redundant Dual Access Mediums Dual Routes

Premium
99.72% Availability
2 hours MMDT

- Dual CE's to Dual & Diverse POPs
- Geographically Redundant Dual Access Mediums Dual Routes

Core Network
Always redundant core links on a protected core network

Vodacom Business Fixed Managed Services - Access Network

2.6 Reporting Services

a. Reporting on Major Incidents affecting multiple customers within 48 hours (2 business days -excluding weekends and public holidays) after resolution.
b. Experiencing major incidents in the network initiates many activities to ensure the incident is resolved immediately. The report can take up to 48hours (2 business days -excluding weekends and public holidays) to compile and distribute to all effected customers.
c. Reporting of specific customer requests for RFO (Reason for Outage) within 5 business days.
d. Requests for RFO (Reason for outage) reports by specific customers involve the compilation of all related information and adhere to standard service request delivery within 5 business days.

3. Change Management

Vodacom Business operates a formal change management practice, to protect the robustness of the Vodacom Business network infrastructure and the customer network and to ensure traceability of network changes. The formal change control process encompasses Vodacom Business network changes. These network changes are initiated internally and from 3rd party providers and notifications to customers regarding the changes are initiated that may affect the customer.

3.1 Classification of Changes

A change can be categorised as:

a. Pre-Approved Change: it is low impact, performed repetitively, requires no assessment or approval on each individual change. These changes carry no risk to the network, should they be implemented. Pre-approved changes have a minimal service impact.
b. Standard Change: A change to a configuration item (CI), substantial or critical impact, requires assessment and approval by CI Owner and Change Manager.
c. Emergency Change: A change to a CI that has substantial impact, but is of critical priority, thus requires fast tracked approval with CAB. An emergency change may carry a very high risk if it is implemented

3.2 Customer Requested Changes

RFC (Request for change). When a customer requests a change to their existing solution.

a. The CSOC technical officer that receives the request for change (RFC) will assess the impact of the change.
b. If there is a commercial impact to the change, the technical officer will direct this request to the customers’ account manager, and the change will follow the normal order process.
c. As the change is pre-approved (customer requested), the CSOC technical officer will go ahead with implementation of the change. Date and time of implementation will be agreed with customer.
d. The customer will be notified once the change has been completed, and proper post-implementation testing will be done.

Severity	Definition	Type of Changes	MTTR
1 (Minor)	Any change requested by the customer that **will not affect** services, and can be implemented immediately, with no scheduled down time required.	• SNMP configuration • NetFlow Configuration • DHCP Configuration • Access Control List • NAT configurations • Bandwidth statement • Static Routing that's not Business affecting • QOS configurations	Within one Business day
2 (Major)	Any change requested by the customer that **will affect** services, and can be implemented immediately, with no scheduled down time required.	• Interface IP change • LAN/WAN • Configurations/Changing of BGP routing • Configuration/Changing of EIGRP routing • Inter VRF routing • Complex APN MPLS routing on some clients • Configuring/changing Policy/Route Maps	As customer agreed

3.3 Vodacom Infrastructure and 3rd Party Changes

a. The Change Administrator that receives the request for change (RFC) will analyse the impact of the change and categorise it accordingly.
b. The Vodacom Business Change Manager is responsible for the approval of all minor changes. The Vodacom Business Change Advisory Board (CAB) is responsible for the approval of all major changes.
c. Major Emergency Changes require an Emergency Change Advisory Board (ECAB), while Minor Emergency Changes are approved by the Vodacom Change Manager.
d. The change approval window runs over a 2-week period. All RFC's must be submitted by close of business on a Friday. Only these RFC's will be considered for the next period and the Tuesday CAB.

3.4 Change Implementation and Closure

a. The approved change will be scheduled within the Vodacom Business change window. The Vodacom Business change window is daily from 23H00 until 04H00, with allowed downtime starting after 00H00.
b. If the customer wishes for the change to be postponed, this must be communicated to the CSOC. Vodacom Business will endeavour to re-plan the change, excluding Emergency Changes.
c. An Implementation Plan, Test Plan and Roll-back Plan will be designed for the planned change.
d. All stakeholders will be notified of the success or failure of the changes once it has been implemented.
e. Once the change has been completed, it will be reviewed to evaluate the success of the implementation.

3.5 Network Change Notification

a. All planned changes will be communicated to the affected stakeholders including the approval or rejection, schedule and outcome.

b. The customer will be notified of approved changes and completed changes.

c. An RFC that will have impact on a single customer will require notification to be sent to the customer 2 business days prior to the change implementation date.

d. An RFC that impacts multiple customers will have to be communicated to the affected customers 7 business days prior to the change implementation date.

3.6 Failover testing

Vodacom offers failover testing to customers. Customer may arrange for testing the robustness of their dual access linked sites. Testing links that are configured to fail over seamlessly to the secondary access link, when the primary access link fails. Vodacom will conduct a standard set of tests to confirm accessibility to the Customer VPN network or any specified tests by the customer.

Customers are requested to send failover testing requests to **0821951@vodacom.co.za** at least 7 days prior commencement of the tests to allow for scheduling and preparation. Customers may also elect a Customer Technical Contact that can be present during such testing and confirm the success of the testing. Testing will be conducted outside business hours to prevent disruption to customer business. Customers will receive the completed Failover Test Plan Document with recorded test results after testing has been completed.

Failover testing window:

Description	Start time	End time
Single failover and revert to normal	22h30	04h00
24hour failover and revert to normal	22h30	Next day 22h30

Standard Tests

- Manually disabling the primary link and confirm traffic flow on secondary link
- Test reachability of the managed Vodacom Customer Edge device
- Revert configuration back to normal

Customized tests may be requested by the customer.

4. Security Management

Vodacom Business will require access to the customer sites and vice versa during service provisioning and service support. Vodacom Business will comply with the security policy as dictated by the customer in gaining access to their sites and as such the customer is required to comply with the Vodacom Business Security Policies.

4.1 Access Control – Vodacom premises

a. Access to Vodacom Business information, systems and hosting architecture is governed by a Security Policy, which dictates the following:
   i. Access by Internal Staff only
   ii. The designated owner of the information asset shall take responsibility for all access granted. The owner (customer) of the IT equipment on Vodacom premises shall ensure that all access to the resource granted is appropriate and justified.
   iii. All the Vodacom Business information systems privileges shall be promptly terminated at the time when an employee, consultant or contractor or any other temporary worker ceases to provide services to Vodacom.

4.2 Third Party Access – Vodacom premises

a. The customer shall be given access privileges to the IT equipment only after Vodacom Business management has determined that they have legitimate business need. These privileges shall be enabled only for the specific time period required performing the approved tasks and on condition that a Non-Disclosure Agreement and user security acceptance form has been signed.

b. The customer shall provide any information reasonably necessary to assist Vodacom Business in evaluating security issues relating to the authorised employee.

c. The customer shall notify Vodacom Business in writing promptly upon a change in the user base for the work performed over the network connection or whenever in Vodacom's opinion a change in the connection and/or functional requirements of the network connection is necessary.

4.3 Visitors Access – Vodacom premises

a. Visitors must obtain approval for access to any of Vodacom's IT equipment from the Information Owner and a Non-Disclosure Agreement has been signed. The hosting party/person shall be responsible for ensuring that required approval is obtained before any access is granted.

b. Visitors shall be accompanied by the hosting personnel and monitored by security personnel responsible for the Server room.

4.4 Site Access Authorisation to customer sites

a. Access during Provisioning

i. During Solution Project Provisioning the Project Manager will be in contact with the customer site contacts to approve access to the site for installation purposes. The Project Manager will provide the customer with all required names and details of the installation team.

ii. Vodacom Business will require the customer to ensure that Vodacom Business has a correct and up-to-date list of site contacts and to ensure that the installers will have access to the site on the agreed date and time.

b. Access for support purposes

i. Access to the customer sites may be required for replacement or repair of equipment, during the incident management process. The CSOC engineer that owns the incident will contact the Customer Site Contact, to arrange access to the site for the support team. The CSOC engineer will provide the customer with all required names and details of the support team.

ii. In order for Vodacom to provide the expected and required levels of support the customer is to ensure that Vodacom Business has a correct and up-to-date list of site contacts and to ensure that the support team will have access to the site on the agreed date and time.

5. Problem Management

Vodacom Business has a Problem Management process in place responsible for managing the lifecycle of all problems. The goal is to prevent the adverse impacts of Incidents and Problems on Vodacom Business that are caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors (following the ITIL problem management framework). A problem manager would be assigned to the identified problem(s) and assist in resolution of cross functional problems and participate in problem management task teams. Problem Management differs from Incident Management, in that the goal is prevention of incidents, by resolving the root cause problem. A problem is defined as a condition often identified as a result of multiple Incidents that exhibit common symptoms. Problems can also

be identified from a single significant Incident, indicative of a single error, for which the cause is unknown, but for which the impact is significant.
Once the root cause of a Problem has been diagnosed, and a workaround found, the former problem becomes a Known Error. Resolving a Known Error would generally necessitate a Request for Change, triggering the Vodacom Business Change Management Process.

6. Reporting and Availability Management

a. Vodacom Business Reporting responsibilities are fully specified in the customer specific customer agreement
b. Request for Ad Hoc reports should be logged with the CSOC and where possible we will endeavour to provide these reports in a mutually agreed upon timeframe.
c. All reporting data (data points) will be stored and be accessible to the customer during the Term (lifetime of the Master Agreement).
d. Availability reports are available to the Customer through the Vodacom Business self-service portal
e. All IP devices managed by Vodacom Business, on behalf of the Customer will be polled by the Performance Management Tool with a frequency of 5 minutes. The performance management tool will report on the availability of a device. Reports can be generated, with an aggregation of 5 minutes to an hour. 5 Minutes statistics are stored for 6 days, and 1-hour statistics are stored up to a year.

7. Customer Satisfaction Surveys

Random but formal survey interviews will be conducted at regular intervals by our Customer Satisfaction Analysts.

8. Incident Notifications

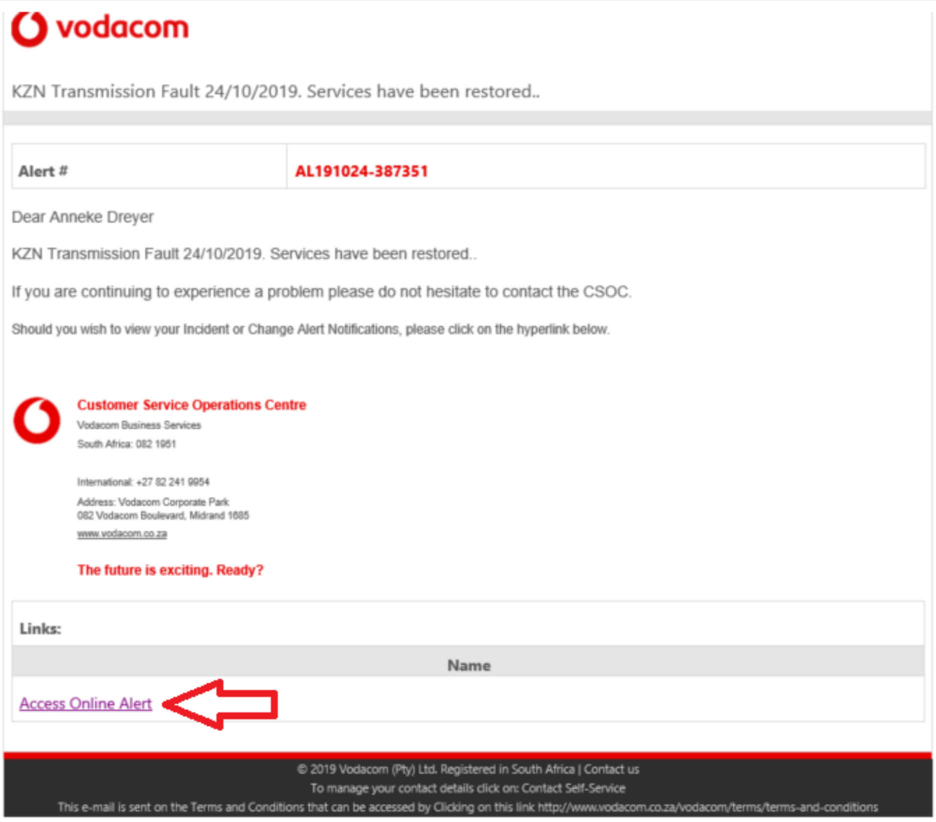
There are two types of Incident Notifications:

1. Major Incident notifications for multiple customer impacting incidents that are sent by the VB CSOC Communications Team
2. Incident notifications for incidents that are individual site impacting that are sent by the CSOC Service Desk

9. Major Incidents - Multiple Customer Impacting Incident Notifications

This notification is sent both by SMS and email. The information contained in SMS notifications are limited to the number of characters that can be sent in a SMS (140) whereas email notifications contain more detail. The VB CSOC Communications Team will endeavour to send out the first notification within 30 minutes however the nature of the incident will determine the extent of the investigation before a notification can be sent out. Update SMS and emails are sent every 45 minutes. The customer will only receive these notifications if it has been identified that their sites are impacted and if the technical contacts have been flagged for notifications in Siebel. The notification will contain as much information as we have and where possible it will contain information as to the general location of the incident.

Example of email sent:



KZN Transmission Fault 24/10/2019. Services have been restored..

Alert #	AL191024-387351

Dear Anneke Dreyer

KZN Transmission Fault 24/10/2019. Services have been restored..

If you are continuing to experience a problem please do not hesitate to contact the CSOC.

Should you wish to view your Incident or Change Alert Notifications, please click on the hyperlink below.

Customer Service Operations Centre
Vodacom Business Services
South Africa: 082 1951

International: +27 82 241 9954
Address: Vodacom Corporate Park
082 Vodacom Boulevard, Midrand 1685
www.vodacom.co.za

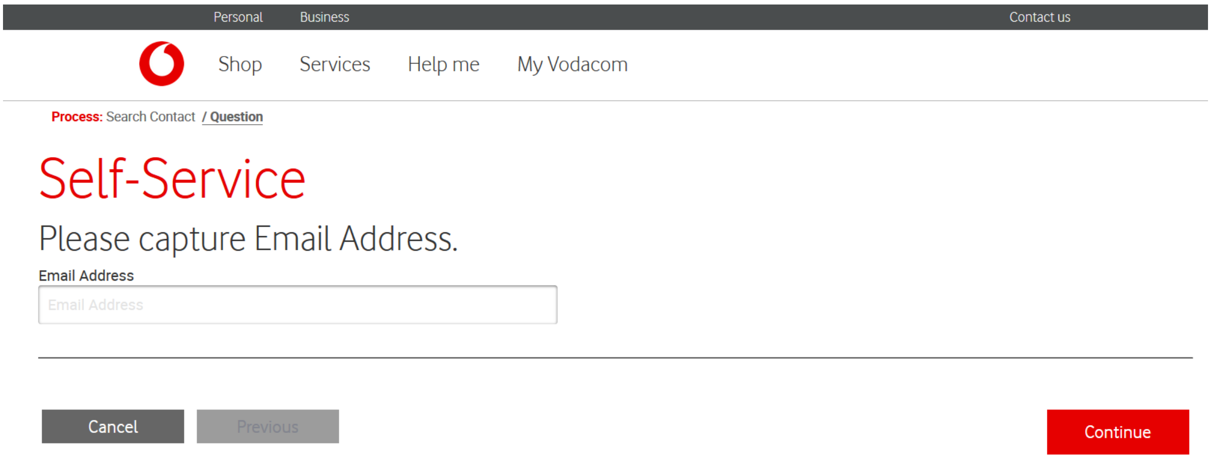
The future is exciting. Ready?

Links:

Name
Access Online Alert

© 2019 Vodacom (Pty) Ltd. Registered in South Africa | Contact us
To manage your contact details click on: Contact Self-Service
This e-mail is sent on the Terms and Conditions that can be accessed by Clicking on this link http://www.vodacom.co.za/vodacom/terms/terms-and-conditions

The Access Online Link below it available for your convenience. The link to Self-Service – Login using Email Address and OTP When the Access Online Alert link is clicked, follow the Self-Service login requirements (OTP (One-Time-Pin) required) for further details to related registered incidents, Contact details management and notification profiles.

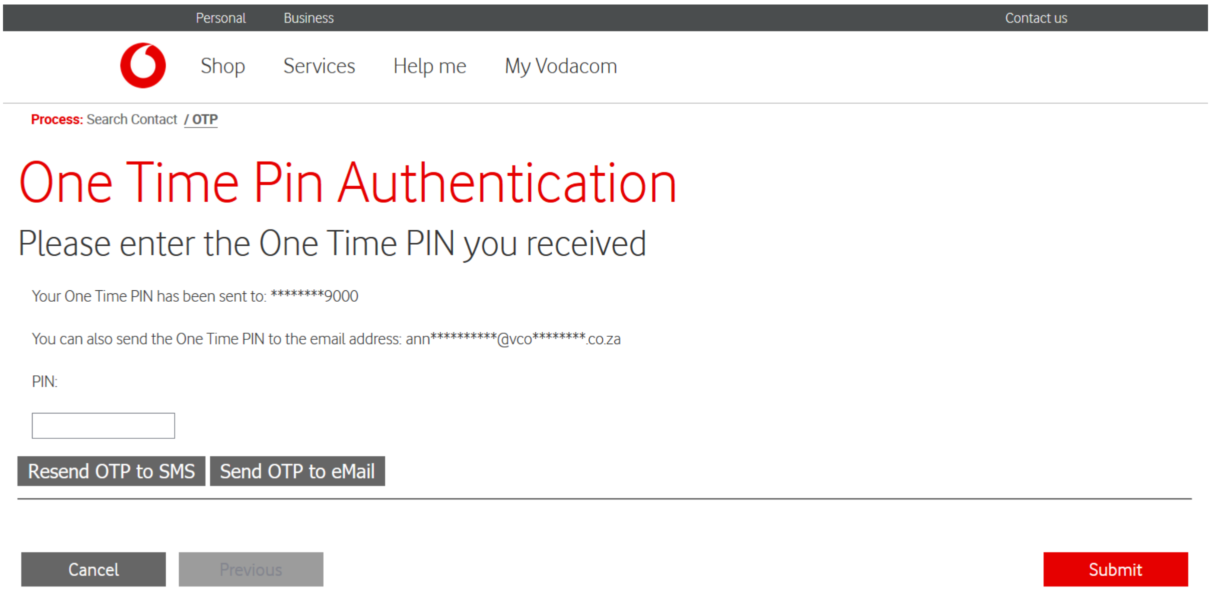


Process: Search Contact / Question

Self-Service

Please capture Email Address.

Email Address: Email Address



Process: Search Contact / OTP

One Time Pin Authentication

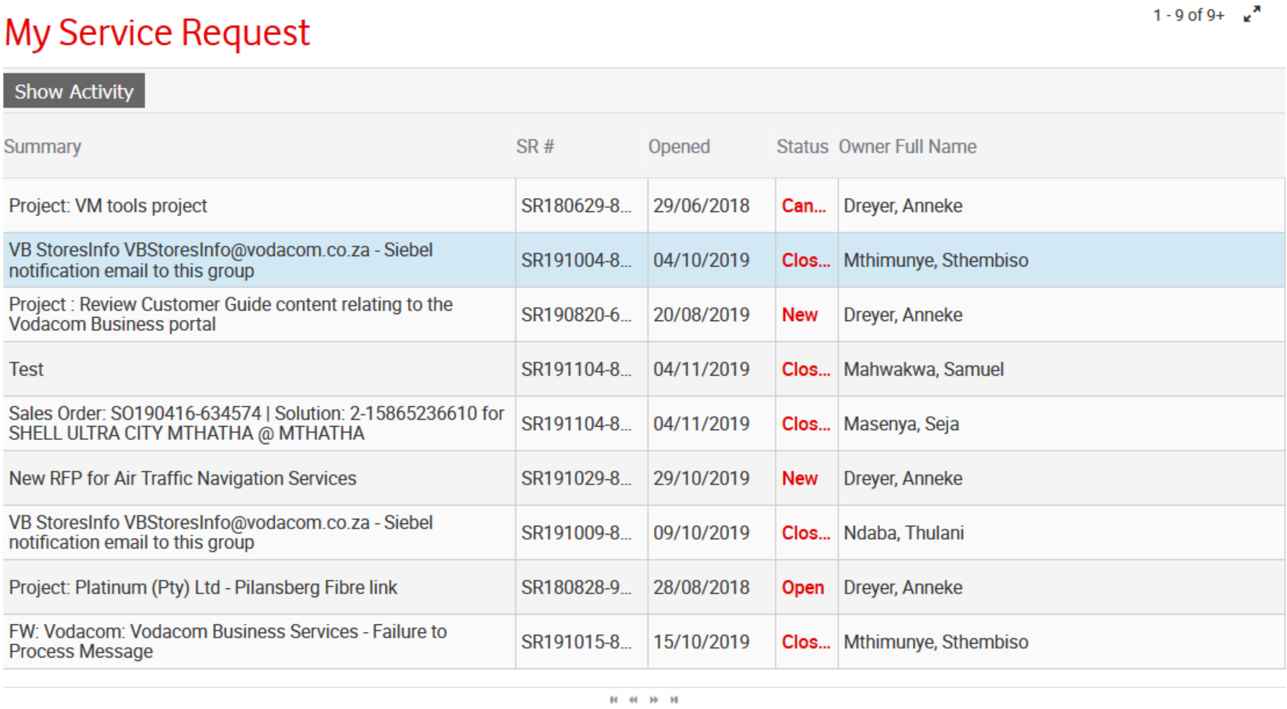
Please enter the One Time PIN you received

Your One Time PIN has been sent to: ********9000

You can also send the One Time PIN to the email address: ann**********@vco********.co.za

PIN:

Successful login will allow access to the relevant incidents



My Service Request

Summary	SR #	Opened	Status	Owner Full Name
Project: VM tools project	SR180629-8...	29/06/2018	Can...	Dreyer, Anneke
VB StoresInfo VBStoresInfo@vodacom.co.za - Siebel notification email to this group	SR191004-8...	04/10/2019	Clos...	Mthimunye, Sthembiso
Project : Review Customer Guide content relating to the Vodacom Business portal	SR190820-6...	20/08/2019	New	Dreyer, Anneke
Test	SR191104-8...	04/11/2019	Clos...	Mahwakwa, Samuel
Sales Order: SO190416-634574 | Solution: 2-15865236610 for SHELL ULTRA CITY MTHATHA @ MTHATHA	SR191104-8...	04/11/2019	Clos...	Masenya, Seja
New RFP for Air Traffic Navigation Services	SR191029-8...	29/10/2019	New	Dreyer, Anneke
VB StoresInfo VBStoresInfo@vodacom.co.za - Siebel notification email to this group	SR191009-8...	09/10/2019	Clos...	Ndaba, Thulani
Project: Platinum (Pty) Ltd - Pilansberg Fibre link	SR180828-9...	28/08/2018	Open	Dreyer, Anneke
FW: Vodacom: Vodacom Business Services - Failure to Process Message	SR191015-8...	15/10/2019	Clos...	Mthimunye, Sthembiso

10. Customer Contact Management

a. It is the responsibility of the customer to:

   i. Provide Vodacom Business with the details of users that are authorised to order or request in-scope services and their level of authority.

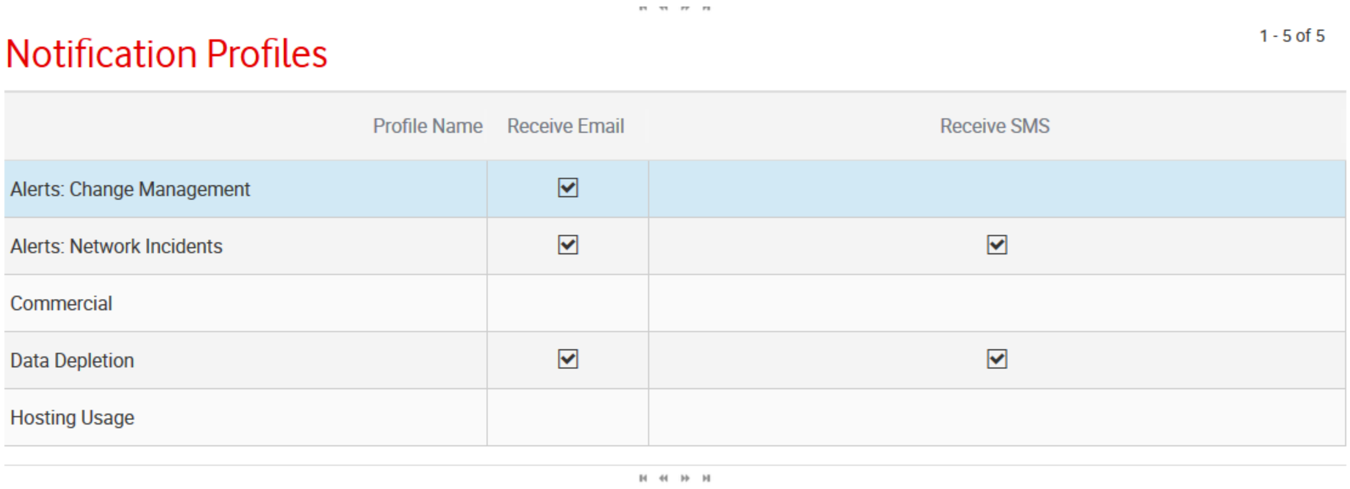
   ii. Ensure that the list of authorised users is maintained.

   iii. Customers can maintain the list of authorised users on the Vodacom Business self-service portal, (www.vodacombusiness.co.za/business/main/login).

b. The Customer Service Desks or nominated party shall be the first point of contact (Level 1) as the Nominated and Authorized Users regarding incidents. This includes events that cause or may cause an interruption or reduction of service, as well as for problems and service requests.

c. The customer can also use the Vodacom Business Self Service Portal to indicate whether it would be preferable to receive automated incident notifications. The customer will have the option to select whether it is preferable to receive SMS or email notifications. Furthermore, a choice is available to receive these notifications during Business Hours, Extended Hours or 24/7/365.

Below the related incidents in "My Service Request" area, you will find your "Notifications Profiles"

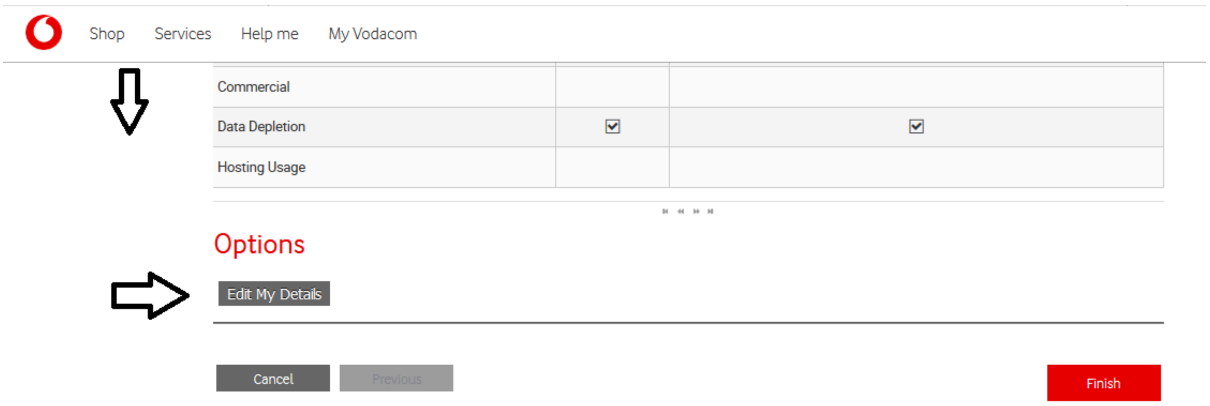


Notification Profiles

1 - 5 of 5

Profile Name	Receive Email	Receive SMS
Alerts: Change Management	☑	
Alerts: Network Incidents	☑	☑
Commercial		
Data Depletion	☑	☑
Hosting Usage		

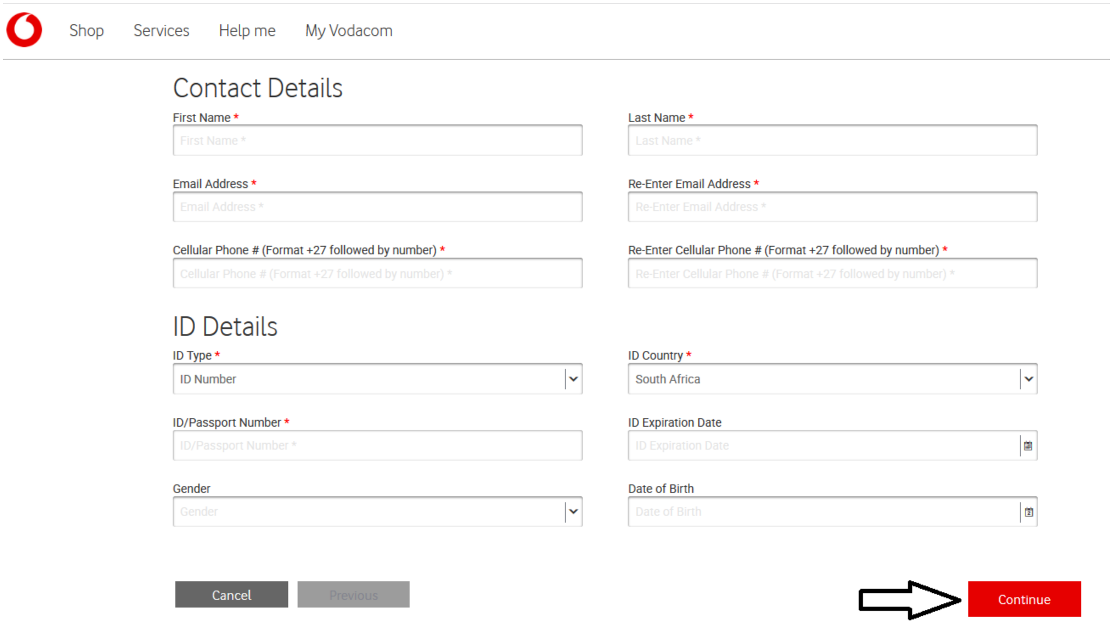
Scrolling down for the option "Edit My Details"



Commercial		
Data Depletion	☑	☑
Hosting Usage		

Options

Contact Details can be updated for existing registered contacts.
After updates were done, click continue to submit the changes made.



Contact Details

First Name *
First Name *

Last Name *
Last Name *

Email Address *
Email Address *

Re-Enter Email Address *
Re-Enter Email Address *

Cellular Phone # (Format +27 followed by number) *
Cellular Phone # (Format +27 followed by number) *

Re-Enter Cellular Phone # (Format +27 followed by number) *
Re-Enter Cellular Phone # (Format +27 followed by number) *

ID Details

ID Type *
ID Number

ID Country *
South Africa

ID/Passport Number *
ID/Passport Number *

ID Expiration Date
ID Expiration Date

Gender
Gender

Date of Birth
Date of Birth

11. Customer Site Specific Incident Notifications

These email notifications are sent by the CSOC Service Desk.

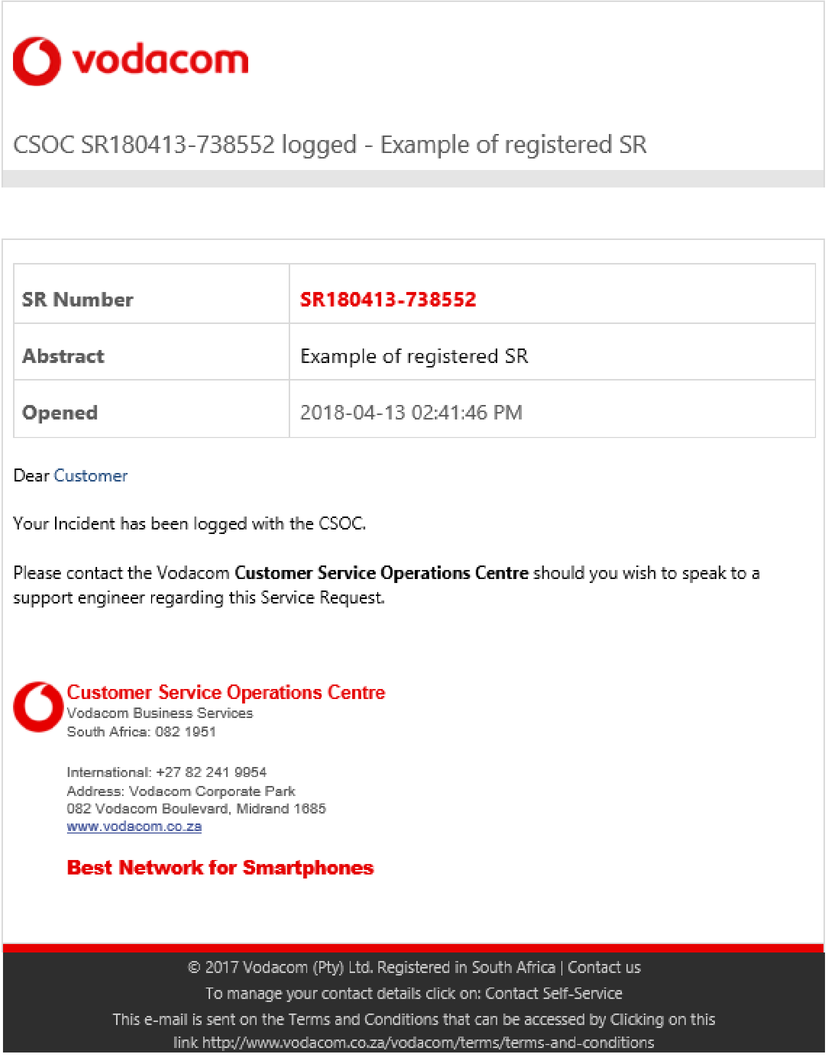
For proactive incident alerting the CSOC technical officer acknowledges the alarm presented on our monitoring systems and logs into the affected device to validate the alarm. If the alarm is valid the CSOC technical officer will open a Service Request on Siebel for the customer. If the customer has elected to receive automated notifications, Siebel will automatically send a notification to the nominated technical contacts.

The CSOC will endeavour to open valid tickets and inform customers within 20 minutes of the alarm being presented.

An example of the notification email is included below. Individual site impacting incident notifications are sent by the CSOC Service Desk and will have the subject line **"Vodacom Proactive SR # XXXXXXX has been raised"**.

This notification is to simply inform the customer that the CSOC is investigating a fault that was picked up and the CSOC TO (Technical Officer) will keep the customer updated. The customer can contact the CSOC If you require further information.

Example of email:



vodacom

CSOC SR180413-738552 logged - Example of registered SR

SR Number	**SR180413-738552**
Abstract	Example of registered SR
Opened	2018-04-13 02:41:46 PM

Dear Customer

Your Incident has been logged with the CSOC.

Please contact the Vodacom **Customer Service Operations Centre** should you wish to speak to a support engineer regarding this Service Request.

Customer Service Operations Centre
Vodacom Business Services
South Africa: 082 1951

International: +27 82 241 9954
Address: Vodacom Corporate Park
082 Vodacom Boulevard, Midrand 1685
www.vodacom.co.za

Best Network for Smartphones

© 2017 Vodacom (Pty) Ltd. Registered in South Africa | Contact us
To manage your contact details click on: Contact Self-Service
This e-mail is sent on the Terms and Conditions that can be accessed by Clicking on this link http://www.vodacom.co.za/vodacom/terms/terms-and-conditions

Appendix 1: Acronyms

Acronym	Definition
CAB	Change Advisory Board
CI	Configuration Items
CSOC	Customer Service Operations Centre
EHOD	Executive Head of Department
IM	Incident Management
MTTR	Mean Time to Repair
MTTr	Mean Time To respond
NDA	Non-disclosure Agreement
RCA	Root Cause Analysis
RFC	Request for change
RFO	Reason for Outage
SRF	Service Request Form
SRM	Service Request Management
TC	Technical Consultant/Contact
TO	Technical Officer
VSB	Vodacom Security Baseline
VB	Vodacom Business
QOS	Quality of service

Appendix 2: Incident Logging Template

Vodacom Business Technology Solutions

Customer Service Operations Centre

☎ 21951 | Incident Management and Logging Template - Fixed Managed Services | ✉ 0821951@vodacom.co.za

NB: The more information we have the better we can serve your needs. Please use the below template and share as much information as possible.
The fields marked with an * are important and compulsory and needs to be typed, no handwritten documents please

General Information related to incident	
* Date and Time of incident	
* Customer or Account name	
* Solution ID & Product name	
Circuit: Number | ID | Mac Address	
* Incident location name	
* Physical Address at location of incident	
* Technical Contact person at location	
* Technical Contact person contact number – prefer mobile number	
* Technical Contact person eMail address	
* Operating Hours at location of incident	
* Problem Statement – what do you experience or what are the symptoms?	
* Do you experience loadshedding or power related outages in your area at this stage?	
Access | MPLS | SD-WAN | Business Connect | Hosting | Security | VoIP | incidents	
* Equipment details - Make and Model numbers. Was equipment rebooted?	
* Router light status? A photo speaks a thousand words, if at all possible it will assist if you can attach a photo and send to us	
* Accedian and POE devices - powered on and light status? A photo speaks a thousand words, if at all possible it will assist if you can attach a photo and send to us	
Cabling checked and confirmed secure? A photo speaks a thousand words, if at all possible it will assist if you can attach a photo and send to us	
Corporate APN incidents	
* Corporate APN Name	
* Description of the problem experienced with the APN? A photo speaks a thousand words, if at all possible it will assist if you can attach a photo and send to us	
Location of person who experiences the problem if other than above information	
* SIM number(s) or MSISDN number(s)	
Does the situation affect a single or multiple users?	
Do you use a Radius Server, and if so who manages the Radius Server?	
Type of device used and model number? Is it a Phone, Modem, Router, MiFi Device, Other? Is there an error message, if so, what is the error message?	
Please give us an indication of the Operating System (OS) installed on your devices as well as the Connectivity Software?	
Mobile coverage incidents related to APN connectivity or Access Medium failover for MPLS | SD-WAN | Business Connect	
* Location information of perceived coverage related incident - Physical address or GPS co-ordinates	
Do you have, or do you know if Vodacom have installed a cell extender or booster at your premises? If so, can you give us some additional information?	
* Is the problem experienced more indoors or outdoors?	
GSM medium used, LTE or 3G? Have you confirmed the device is not locked on LTE or 3G only?	
Please give us an indication of the Operating System (OS) installed on your devices as well as the Connectivity Software?	
* Type of device used? Phone, Modem, Router, MiFi Device, Other? Is there an error message, if so, what is the error message?	
* Short description of your perceived coverage related incident	

Appendix 3: RFC Template

Area of Work	Vodacom Business
Requestor Name/Company	
Requestor Contact No	
Site	
Configuration Item **(Service/device affected)**	
Short Description	
Reason for Change	
Required Start	YYYYMMDD AT 20H00
Required Finish	YYYYMMDD AT 21H00
Classification	New, Add, Remove, Move, Amend, Retire
Change Type	Standard/Emergency
Business Risk	Low/Medium/High
Priority	Low, Medium, High (Urgent)
Service Affecting	Yes / No
Notes, Comments	

Appendix 4: Frequently Asked Questions

	Frequently Asked Questions
1	**What types of devices are monitored?**
	• Routers (CE/PE/P) • Switches • Hosting Servers
2	**What is monitored on the device?**
	On Routers and Switches we monitor: • CPU • Memory Usage • Buffer Utilization • Saturation • Availability For Managed Hosted Environments we monitor hardware components of the hosted servers.
3	**How often is a monitored device checked/polled?**
	• The SMARTS discovery device will ping CE (Customer Edge) nodes, PE (Provider Edge) nodes, and hosting servers every 20 seconds to test for availability • When a ping fails the SNMP polling frequency is increased until the link or device returns to a normal state • SMARTS will poll (using SNMP protocol) CE nodes, PE and P nodes, and other nodes or servers every 4 minutes • PE and P nodes forward syslogs to Netcool on all router activity • IPSLA tests are performed at a 5-minute interval, the tests are initiated from a shadow router connected to the PE and will generate an alarm when a latency breach is detected. • Alarms are forwarded to Netcool • The alarm is verified by a CSOC Engineer and if valid a ticket is opened on the SRM System and the customer is notified accordingly
4	**What is the process that is followed once an alarm is detected?**
	The CSOC Engineer acknowledges the alarm presented on Netcool and logs into the affected device to validate the alarm. If the alarm is valid the CSOC Engineer will open a Service Request on the SRM System against the affected customer. The CSOC Engineer will then inform the nominated customer technical contact, telephonically or through email. The CSOC will endeavour to open valid tickets and inform customers within 15 minutes of the alarm being presented on Netcool.
5	**Why aren't Customers informed as soon as Netcool picks up the alarm?**
	Netcool which monitors our environment currently sends SMS's and emails to internal resources for alarm investigation when an outage occurs to ensure that the alarm generated is a valid one. This is currently an internal system that alerts the relevant technical resources to ensure that action can be taken for the specific generated alarm and to verify if it is valid. As it stands Vodacom Business does not have any immediate plans to enable SMS/email alerts at the monitoring level, as in some cases the monitoring tools generate false positives and this will result in SPAM and an incorrect service perception to our customers and be of little value. Thus, the CSOC Engineers will notify customers telephonically only once the alarm has been validated, acknowledged and a ticket has been opened on the SRM System.
6	**How does Vodacom Business Services know what service is affected by the alarm raised?**
	The node name is clearly presented as part of the alarm. Alarms will also be enriched with customer, service and site information.
7	**When is an alarm cleared or cancelled?**
	When it is resolved i.e. An event will clear when an interface or router is up again.
8	**Who can log a call?**
	For security reasons, only authorised company contacts will be allowed to log a call. Remember to keep your contact details up-to-date on the Vodacom Business self-service portal (www.vodacombusiness.co.za/business/main/login). If you have any questions, feel free to contact your Service or Account Manager.