

INCIDENT MANAGEMENT

Major/Priority (PCM) Incident Process

TABLE OF CONTENTS

1	SCOPE	3
2	INCIDENT MANGEMENT, MAJOR/PRIORITY (PCM) PROCESS ROLES AND RESPONSIBILITIES	4
2.1	PCM INCIDENTS OPEN INCIDENTS	4
2.2	PCM INCIDENTS RESOLVED INCIDENTS	4
3	INCIDENT MANGEMENT, MAJOR/PRIORITY (PCM) RULES	5
4	MAJOR/PRIORITY (PCM) PROCEDURE	6
5	PRIORITY MATRIX	8
6	MAJOR/PRIORITY (PCM) HANDLING GUIDE	9
7	REFERENCES	12
8	LEGISLATION	12
9	STATUS DEFINITIONS AND ACRONYMS:	12
10	DOCUMENT MANAGEMENT	15

1 SCOPE

- a) This process explains the activities involved in reporting, logging and resolution of incidents that are logged as a Critical/High/Medium Priority.
- b) The following process narrative defines how Major/Priority (PCM) incidents are detected and handled till closure.
- c) It identifies the stakeholders and defines the roles and responsibility of the role-players involved.
- d) Major outages should be managed in conjunction with Problem management process.
- e) Major/Priority (PCM) incidents should be resolved within the agreed SLA/OLA.

2 Incident Management, Major/Priority (PCM) process Roles and Responsibilities	
Roles	Responsibilities
Incident Management	<p>2.1 PCM INCIDENTS OPEN INCIDENTS</p> <ul style="list-style-type: none"> Managing and following up on all open Critical/High/Medium Priority Incidents regularly Escalate and ensure that support teams are aware of the incidents and update them accordingly. Check the Major/Priority (PCM) handling guide for frequency on escalations and targeted audience. User reported incidents are to be facilitated by regularly keeping in touch with the users to understand the impact/progress and communicate to the support teams including the SLM's. All correspondence done between users and support teams should reflect as the work log on the incident. Once user reported incidents are resolved, users are to be contacted to confirm closure. Work info entry confirming the resolution by user should be stated on the incident prior to/after support team has updated incident to status "Resolved No further action Required". <p>2.2 PCM INCIDENTS RESOLVED INCIDENTS</p> <ul style="list-style-type: none"> All resolved incidents are to be checked for proper resolution statements prior to auto closure rule taking effect. Any improper resolution statements are to be escalated to the Manager of the support team to have the team member correct the statements. Any resolutions referring to related Incidents, known Errors, Problem records or Change records are to be checked if the referred records are related. If not, please relate.

3 Incident Management, Major/Priority (PCM) Business Rules

Triggers	<ul style="list-style-type: none"> • Daily Major/Priority (PCM) reports run at 07h00, 08h00 and 14h45 • Predefined Remedy searches run by IM Co-Ordinator throughout the day. • Major/Priority Incident Occurs • Service Thresholds Exceeded
Inputs	<ul style="list-style-type: none"> • Major/Priority (PCM) Report automatically produced and placed on the SARS portal every day at 07h00, 08h00 and 14h45 <ul style="list-style-type: none"> ○ Publish shed on the Report Management link on the SARS Portal ○ Operational Reports ○ Remedy Reports ○ <Sort by date> ○ Remedy Open and Resolved Incidents 2017-06-21 07H00.pdf ○ Remedy Open and Resolved Incidents 2017-06-21 08H00.pdf ○ Remedy Open and Resolved Incidents 2017-06-21 14H45.pdf • Incident Records • SLAs
Outputs	<ul style="list-style-type: none"> • Reduction of Major/Priority (PCM) Incidents • Information/reports sent to Management on any major outages. • Customer Communication, Information sent to users of any Major/Priority (PCM) Incidents impacting the SARS environment. • Technician Communication
General Comments	<ul style="list-style-type: none"> • The purpose of this procedure is to ensure that all Major/Priority (PCM) Incidents are attended to as quickly as possible and normal service operations are restored to minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

4 Major/Priority (PCM) Procedure

Step	Responsible Role	Action
	Tier 1 (Incident Management) Tier 2 (Service Desk/Support Team /Monitoring Team)	<p>Incident Detection:</p> <p>This process involves the detecting and managing of Critical, High, Medium priority incidents.</p> <ul style="list-style-type: none"> The incident is: <ul style="list-style-type: none"> An auto generated incident (Critical, High, Medium) Critical, High, Medium Incidents recorded by Tier 2 (Service Desk). Tier 1 (Incident Management), Analyse the incident and the priority. Tier 1 (Incident Management), Verify if incident is with correct Tier 2 (Support group). Tier 1 (Incident Management), If impact is high, raise priority to medium, high or critical, then follow the crisis management process. Tier 1 (Incident Management), Verify and ensure that incident has been received and acknowledged by Tier 2 (Support group).
	Tier 1 (Incident Management) Tier 2 (Support Team)	<p>Communicate Incident:</p> <p>This process involves communicating to the nominated representatives (i.e., SLM/SLC, SD, Support Group, IM, and User) to create awareness that the incident has been logged and on the progress of the incident.</p> <ul style="list-style-type: none"> Tier 1 (Incident Management) or Tier 2 (Service Desk) communicate to the stakeholders (SLM/SLC/Incident Management and Service Desk) that a major/priority incident has been logged Tier 1 (Incident Management), Obtain feedback on the progress of incident from the Tier 2 (Support group) and send updates to the nominated representatives. Tier 1 (Incident Management), Communicate to the stakeholders (SLM/SLC/USER and Service Desk) the progress of the incident. Note that all updates should be captured as work info entry and recorded on the incident record.

4 Major/Priority (PCM) Procedure

Step	Responsible Role	Action
	Problem Management	<ul style="list-style-type: none"> If further communication is required, Problem Management will convene the crisis meeting with the various key members of the team participating on the incident. The incident will remain open until it is decided otherwise by Problem Management. If further communication is not required, then the support team can resume the standard IM process.
	Problem Management	<ul style="list-style-type: none"> Convene a Crisis Meeting with all impacted stakeholders. Appoint a Crisis Manager Documents actions and reconvene checkpoint meetings to track progress of resolution activities. Keeps Incident Management updated at all times. Schedules and facilitates the RCA once the incident has been resolved and the crisis has been called down.
	Support Team	<ul style="list-style-type: none"> Continue to probe the incident to resolution in accordance to action defined in the checkpoint meetings with Problem Management
	Tier 1 (Incident Management) Tier 2 (Support Team)	<p>Ascertain resolution success:</p> <p>This process involves determining if the resolution was successful in resolving the reported issue.</p> <ul style="list-style-type: none"> Tier 1 (Incident Management) to determine if the implemented resolution/workaround had resolved the incident by confirming with the stakeholders. If solution provided is only a temporary workaround, then update incident to "Resolved" and escalate the incident to Problem Management. If the initial reported issue persists, then escalate to the Tier 2 (Support team). Inform Problem Management about the persistent incident.
	Tier 1 (Incident Management)	<p>Incident Closure:</p> <p>This process involves closing of resolved incidents "No Further Action Required".</p> <ul style="list-style-type: none"> Verify that Incident status is on "Resolved No Further Action Required" Verify if the resolution detail is a concise summary of what was done to resolve the reported incident

4 Major/Priority (PCM) Procedure

Step	Responsible Role	Action
		<p>(should match the incident description).</p> <ul style="list-style-type: none"> • Ensure that all required Incident information is complete. • Resolved incident with status reason other than “No Further Action Required” should not be closed. • All verifications and corrections on incident should be completed within 5 days after being resolved. • Incident is closed by remedy after 5 days.

5 Priority Matrix

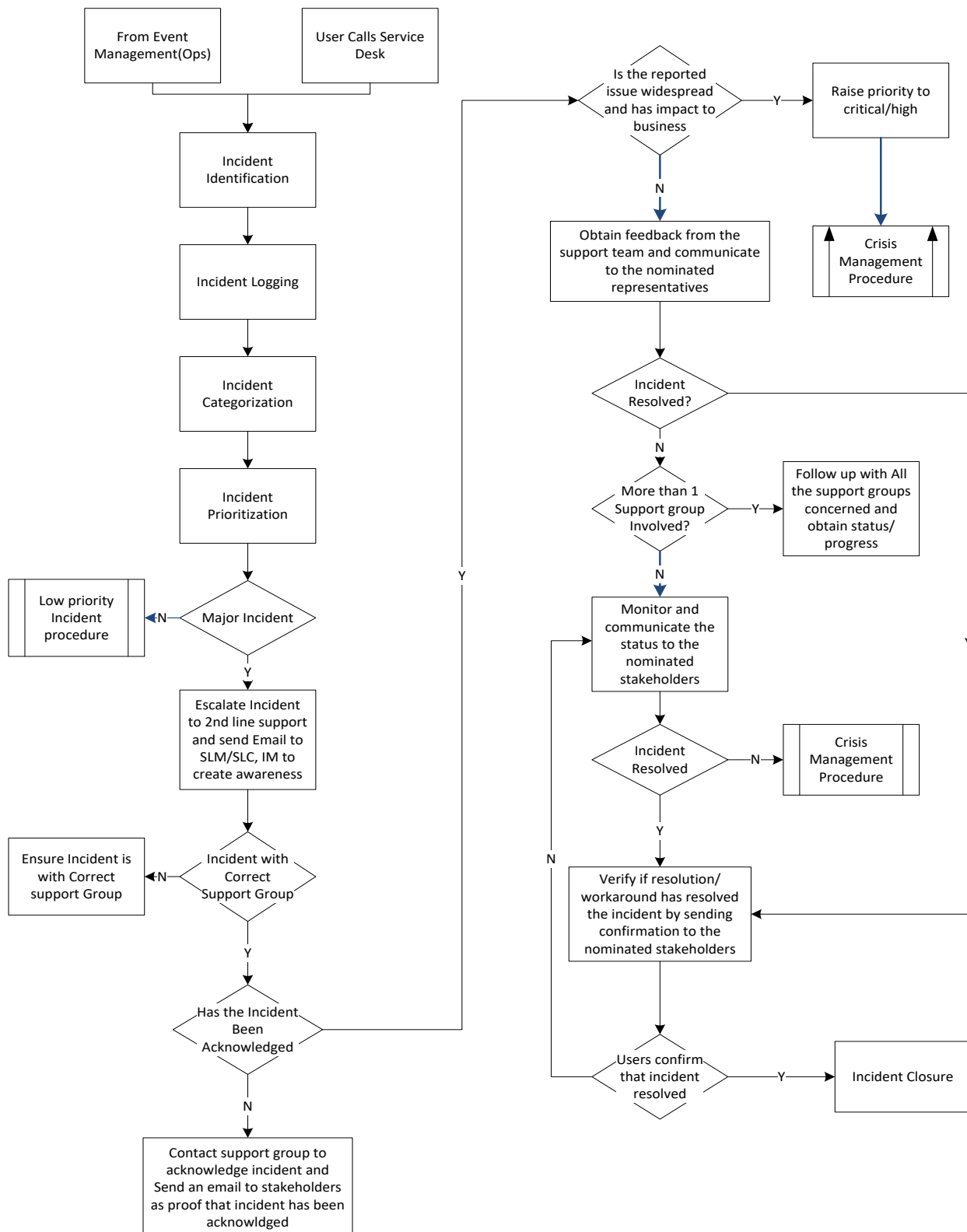
Priority 1 (Critical)	Definition	Major Business Impact: Countrywide outage with no workaround resulting in complete loss of core business systems to customer.	All users affected
	Example	<ul style="list-style-type: none"> • Production system component failure resulting in loss of system availability. • Critical network component (core router or switch supporting enterprise services) not functioning. <p>DNS connectivity and/or component failure resulting in a loss of access to Internet (i.e., firewall, Internet connection, proxy, etc.).</p>	
Priority 2 (High)	Definition	Significant Business Impact: Outage with no workaround resulting in significant loss or degraded system services to customer; however, operations can continue in a restricted mode.	TC sites and > 100 users
	Example	<ul style="list-style-type: none"> • Production system components unavailable impacting batch and online schedules 	

		<ul style="list-style-type: none"> Failure or system degradation in any of the following areas: cluster controller, hub, router, servers, data switch, server application, data-link failure with an alternate route, video services, voice mail system <p>Significantly degraded response from critical applications and databases.</p>	
Priority 3 (Medium)	Definition	Batch/on-line/hardware problems resulting in minimal impact to system and system availability.	The whole office affected and 10 – 100 users affected
	Example	<ul style="list-style-type: none"> Batch job/on-line transaction not requiring immediate contact. Telephone switch unavailable. Inter- and intra-site communication links not functioning. Critical applications and databases (i.e., Service Manager) not functioning 	
Priority 4 (Low)	Definition	<p>Single points of failure resulting in impact to:</p> <ul style="list-style-type: none"> Single customers Single devices <p>Non-critical peripherals.</p>	< 10 users affected
	Example	<ul style="list-style-type: none"> Personal computer (PC), workstation, and terminal Printer, plotter, scanner Telephone End-user software (e.g., LAN access, password resets, etc.) <p>Network services warnings.</p>	

6 Major/Priority (PCM) handling guide

Severity	Response	Resolution	Communication
Critical/High	Initial response within <u>15 minutes</u> from Support Group	<ul style="list-style-type: none"> Continuous effort to resolve by facilitating the resolution process. Facilitation includes initiating meetings, contacting the relevant people etc. Service restored as per agreed OLA/SLA 	<ul style="list-style-type: none"> Immediate notification to the Service Owners (Business and IT), Nominated Representatives and SLM. <u>Update every 30min.</u>
Medium	Initial response within <u>15 minutes</u> from Support Group	<ul style="list-style-type: none"> Regular follow ups on status of resolution effort. Updated incident record with related RFC's where applicable. Service restored as per agreed OLA/SLA 	<ul style="list-style-type: none"> Immediate notification to the Service Owners (Business and IT), Nominated Representatives and SLM. <u>Update hourly.</u>

Critical/High/Medium Priority Incident Process



7 REFERENCES

- There no references to this document.

8 LEGISLATION

- There no legislation referencing to this document.

9 STATUS DEFINITIONS AND ACRONYMS:

Status	Status Reason	Definition
Assigned	N/A	New logged incident
In progress	N/A	Incident acknowledged and being attended to.
Pending	Awaiting Approval	A change has been logged but not approved yet
	Change Implementation	Incident is related to a Change. CRQ must be related
	Client Action Required	Awaiting further information / feedback from client in order to proceed.
	Client Hold	Incident on hold. Awaiting user availability, user testing etc.
	Monitoring Incident	Incident has been resolved. Incident stays open in case incident reoccurs.
	Future Enhancement	Investigating possible future change that may or may not be implemented
	Third Party Action Required	Awaiting 3rd party to attend. e.g., Internal SARS support teams
	Third Party Vendor Action Required	Awaiting external vendor to attend. e.g., Omega, IBM, HP
Resolved	Automated Resolution Reported	No fault found
	Temporary Corrective Action	When service on the reported device/ issue, has been temporarily restored and user is operational.
	CMDB Update Required	CMDB has to be updated before incident closure.
	No Further Action Required	Service Restored. No additional work required.
	Resolution Detail Correction	Insufficient resolution detail provided by internal SARS support or external vendor
Closed	Automated Resolution Reported	No fault found
Cancelled	Budget Constraint	Job exceeds budget threshold
	Cancelled as per User request	User no longer requires the service and request that the incident/request to be cancelled. Name, date and time of confirming with user to be entered on resolution field.
	Duplicate	Incidents of similar nature that are deemed to be duplicates of

		already existing open incidents. Duplicate incidents must be related.
	Incomplete documentation	
	Insufficient documentation	
	Insufficient Signatures	
	Insufficient user information	
	User unavailable	

SARS	South African Revenue Service
Business Owner	The person responsible for the business area in which the application or system is to be and /or enhanced.
Client	Any person or enterprise conducting business with SARS IT
IT users	All users if IT Services as provided by the IT division
DIST	Digital Information Services and Technology
IM	Incident Management
Incident	Service interruption that requires quick restoration.
ITIL	Information Technology Infrastructure Library is a set of best-practices for IT service management (ITSM) that focuses on aligning IT services with the needs of the business.
ITSM	Information Technology Service Management
KEDB	Known Error Database - workarounds to assist resolving incidents
SDB	Solutions database contains solutions to assist in resolving incidents.
Problem	Underlying root cause
RFC	Request For Change
CI	Configuration Item: Any component that is uniquely identifiable that needs to be managed indirectly in order to deliver an IT Service.
SD	Service Desk
PCM	Daily Operational meeting to discuss all Major/Priority incidents and Changes within the SARS environment
Priority, Impact & Urgency Matrix	Service Interruption declared by the Service Support Manager and or Resolution Manager
Critical or High Priority	Determines the impact severity of an outage reported.
Critical Incidents	Country Service Interruption declared by the Service Support Manager and or Resolution Manager.
Critical Incident Manager	Incident Management Regional Coordinator / TL assigned to run with that Incident
Crisis	Country wide service interruption with severe impact.
SOP	Standard Operating Procedure
ICT	Information and Communications Technology
IT Service Management Tool	Technology solutions used for the support of Information Technology Service Management.
Remedy	IT Service Management System used in SARS for logging of all IT requests, incidents, changes, etc.
Root Cause Analysis (RCA)	Problem Management sub-process that identifies the underlying root cause of a problem.
SLM	Service Level Management
SMTSAP	Strategy Modernisation and Technology Standard and Procedure
TPDSAP	Technology Process Division Standard and Procedure
RC	Root Cause
ROLE (RACI) Responsible Accountable Consulted Informed	This role conducts the actual work or owns the problem. This role approves the completed work and is held fully accountable for it. This role may be consulted during the process. This role is to be informed of the progress and or results.

10 DOCUMENT MANAGEMENT

Designation	Name / Division
Business Owner:	
Process Owner:	
SOP Owner:	
Author:	
Detail of change from previous revision:	
Document Approval	
Document Name	TECH-SIO-01-SOP ICT Incident Management Process
Revision Number	