

**TECHNOLOGY AND SOLUTIONS
DELIVERY**

INTERNAL

STANDARD OPERATING PROCEDURE

MANAGE ICT INCIDENTS

TABLE OF CONTENTS

1	SCOPE	3
2	PROCEDURE	3
2.1	Interpretation of process models	3
2.2	Manage ICT Incidents	4
2.3	Manually administer ICT incidents	8
3	MEASURES	9
4	REFERENCES	9
4.1	Legislation	9
4.2	Cross References	9
4.3	Quality Records	9
5	DEFINITIONS AND ACRONYMS	10
6	DOCUMENT MANAGEMENT	10

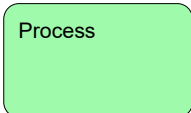
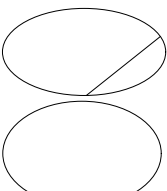
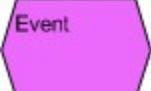
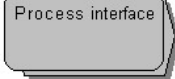



1 SCOPE

- a) The objective of this document is to outline the process followed to manage Information and Communication Technology (ICT) incidents.
- b) The procedures contained in this document apply to all the South African Revenue Service (SARS) staff, contractors / vendors and / or stakeholders.
- c) This procedure will be managed by the **Technology and Solutions Delivery (T&SD)** Incident Management using an Information Technology Service Management (ITSM) System.
- d) This document establishes an Incident Management (IM) process. Adoption and Implementation of these procedures will ensure timely recovery of services provided by **T&SD**.

2 PROCEDURE

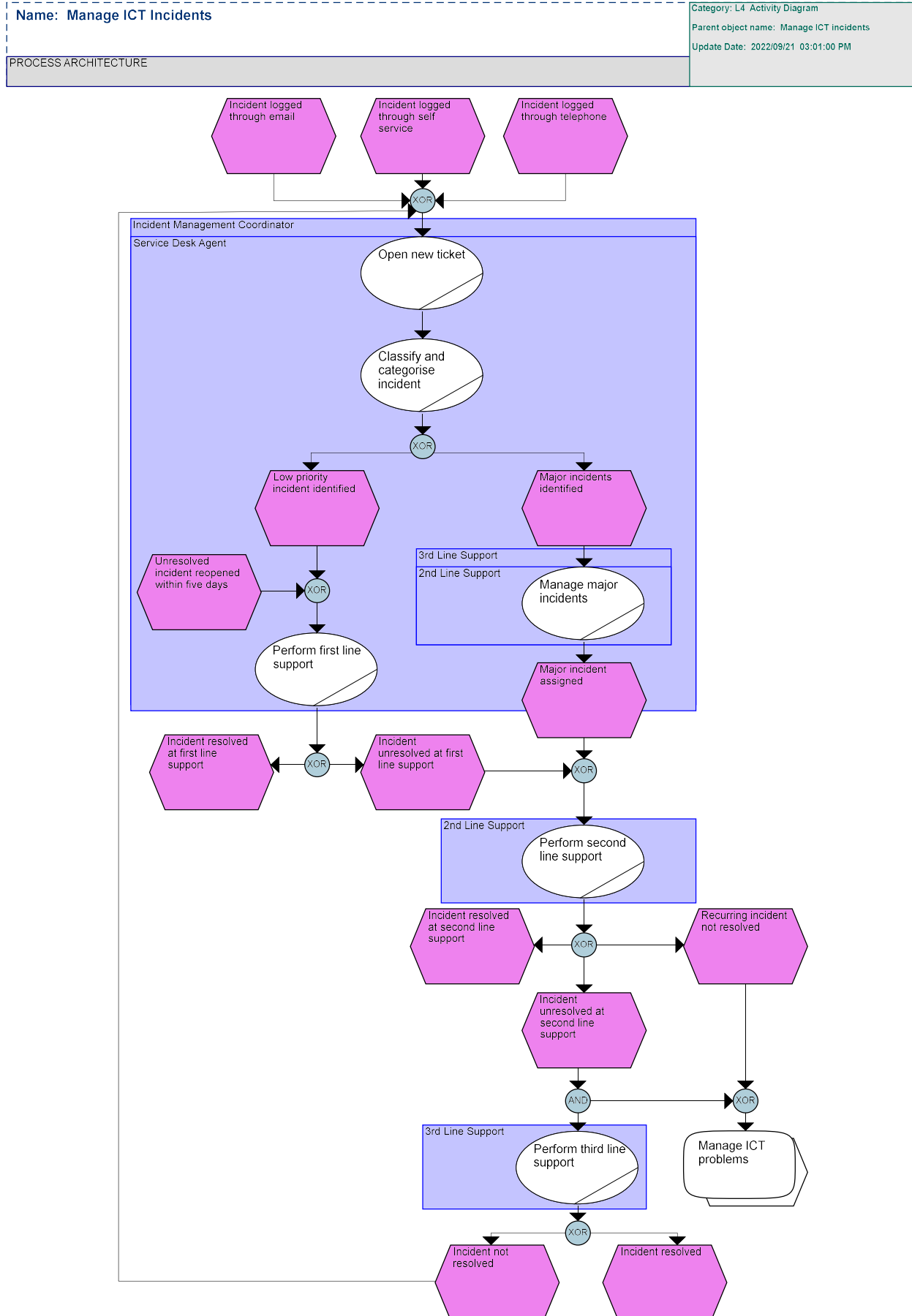
2.1 Interpretation of process models

- a) The modelling methodology is based on a hierarchical set of process models with several levels of decomposition (drill-down) defining the processes on lower levels. The following objects are utilised in the models:

Object Name	Object	Purpose
Process		A process is an action that is performed manually.
Use case		A use case is a group of tasks that are performed manually or systematically. A business use case is a combination of tasks, which consist of manual and system tasks. A system use case is a combination of tasks that are only performed by an application/program.
Event		Defining the start and end conditions in a process flow. Events trigger functions and are the results of functions.
Process interface		Indicates an interface with an associated process.
AND rule		All results must occur.
XOR rule (exclusive OR)		Either result can occur. Any of the results, however, cannot occur at the same time.
OR rule		Either or all results can occur.

- b) **Note:** The functional descriptions have to be read with reference to the process flow diagrams. Each description relates to a function defined in the process flow diagram.

2.2 Manage ICT Incidents



PROCEDURE STEP	ROLE
<p>a) Open a new ticket.</p> <p>i) For a new incident:</p> <p>A) Open a new ticket;</p> <p>B) Verify and update the Requestor's information (contact numbers, office / building name and floor);</p> <p>C) Request a clear, concise description of the incident;</p> <p>D) Request a clear / understandable description of the query and all mandatory information required in the notes must be completed;</p> <p>E) Request for supporting documents, if necessary;</p> <p>F) Verify the asset / configuration item (CI) affected or impacted;</p> <p>G) If all the required information is complete, continue with the process "Classify the incident"; or</p> <p>H) If the information is incomplete, acquire additional incident data.</p> <p>ii) Existing closed incident re-opened after five (5) working days:</p> <p>A) The closed incident will open a new related incident and assign it to IM for Quality Assurance (QA), before being sent back to the Support Group that initially resolved the incident.</p> <p>iii) All incidents are recorded as incident tickets in the IT Service Management Tool (through Self Service or IT Service Desk).</p> <p>iv) Continue with the process "Classify and categorise the incident".</p>	<p>Incident Management Coordinator(R)</p> <p>IT Service Desk (R)</p>
<p>b) Classify and categorise the incident.</p> <p>i) Classify and categorize request or restoration. If it is a request it will follow RF process, and if it is a restoration, it will follow the IM process according to the following:</p> <p>A) User Site Information;</p> <p>B) CI information from Configuration Management;</p> <p>C) Priority Matrix / Impact / Urgency Table; and</p> <p>D) Service and Service Type.</p> <p>ii) If the priority of the incident is major, then continue with the process "Manage major incidents"; or</p> <p>iii) If the priority of the incident is low, then continue with the process "Perform first line support".</p>	<p>Incident Management Coordinator(R)</p> <p>IT Service Desk (R)</p>
<p>c) Manage Major Incidents</p> <p>i) Assign the incident to the relevant Assigned Groups (second line Support) and / or Vendors.</p> <p>ii) Communicate the incident information to the nominated representatives for awareness.</p> <p>A) IT Service Desk:</p> <p>I) Once the critical or major incident has been logged, send a communication email to the nominated representatives to create awareness that the incident has been logged and on the progress of the incident.</p> <p>II) Determine the scope and impact of the incident, validate that it meets the definition for a critical incident.</p> <p>B) Incident Management (IM):</p> <p>I) Liaise with Change and Release Management to determine any changes to the environment; and</p> <p>II) Once second line support is done with the investigations and is unable to continue, log a problem investigation.</p> <p>C) Problem Management:</p> <p>I) Convene a Crisis Meeting with all impacted stakeholders;</p> <p>II) Appoint a Crisis Manager;</p> <p>III) Document actions and reconvene checkpoint meetings to track progress of resolution activities;</p> <p>IV) Keep the IM team updated at all times; and</p>	<p>Incident Management Coordinator(R)</p> <p>IT Service Desk (R)</p> <p>Second Line Support (R)</p> <p>Third Line Support (R)</p>

PROCEDURE STEP	ROLE
<p>V) Schedule a Root Cause Analysis (RCA) once the incident has been resolved and the crisis has been called down.</p> <p>iii) Obtain feedback of the resolution progress from the second line support group(s);</p> <p>iv) Manage incident escalations; and</p> <p>v) Record the progress of the incident until it is resolved.</p>	
<p>d) Perform first line support.</p> <p>i) Check for existing Incident tickets.</p> <p>ii) Check to see if there are any changes / releases that may resolve the incident.</p> <p>iii) Check for Wiki's, Known Errors and Solutions from the Problem Management console.</p> <p>iv) Request for Additional information, if required (screen prints, documents, error messages, etc.) and pend the incident for three (3) working days while awaiting further information (if not received within the specified time the ticket will be cancelled and a new ticket has to be logged when the information is available).</p> <p>v) If the priority level of the incident is Low:</p> <p>A) Perform first line support and capture the information in 'work info';</p> <p>B) Relate incident to the SDB before resolving, if there is no solution create a solution.</p> <p>C) If the incident is resolved at first line, the incident status will be updated to "Resolved" and a clear resolution entered with what was done to resolve the ticket and actions taken to prevent re-occurrence. The status reason will be 'No Further Action Required' and it will automatically close after five (5) working days.</p> <p>D) If the incident could not be resolved at first line support, before re-assigning, add a meaningful work info, then re-assign the incident to the relevant Assigned Groups (Second line Support) and / or Vendors.</p>	IT Service Desk Agent (R)
<p>e) Perform second line support.</p> <p>i. If the incident is resolved at second line support, the incident status will be updated to "Resolved", and a clear resolution added with what was done to resolve the ticket, and actions taken to prevent re-occurrence. The status reason will be 'No Further Action Required' and it will automatically close after five (5) working days;</p> <p>ii. If the incident is resolved at the Vendor, proceed to follow the Vendor resolution process; or</p> <p>iii. If the incident could not be resolved at second line support, assign the incident to the Assigned groups (third line support) and add a Work Info / log of steps taken in order to attempt the resolution of the ticket to date.</p>	Second Line Support (R)
<p>f) Perform third line support.</p> <p>i. If the incident is resolved at third line support, the incident status will be updated to "Resolved"; a clear resolution will be added with what was done to resolve the ticket and actions taken to prevent re-occurrence. The status reason will be 'No Further Action Required' and it will automatically close after five (5) working days;</p> <p>ii. If the incident is resolved at the Vendor, proceed to follow the Vendor resolution process; and</p> <p>iii. If the incident could not be resolved at third line support, a problem investigation ticket should be logged following the Problem</p>	Third Line Support (R)

PROCEDURE STEP	ROLE
Investigation process. And add the Work Info of steps taken in order to attempt the resolution of the ticket to date.	

2.3 Manually administer ICT incidents

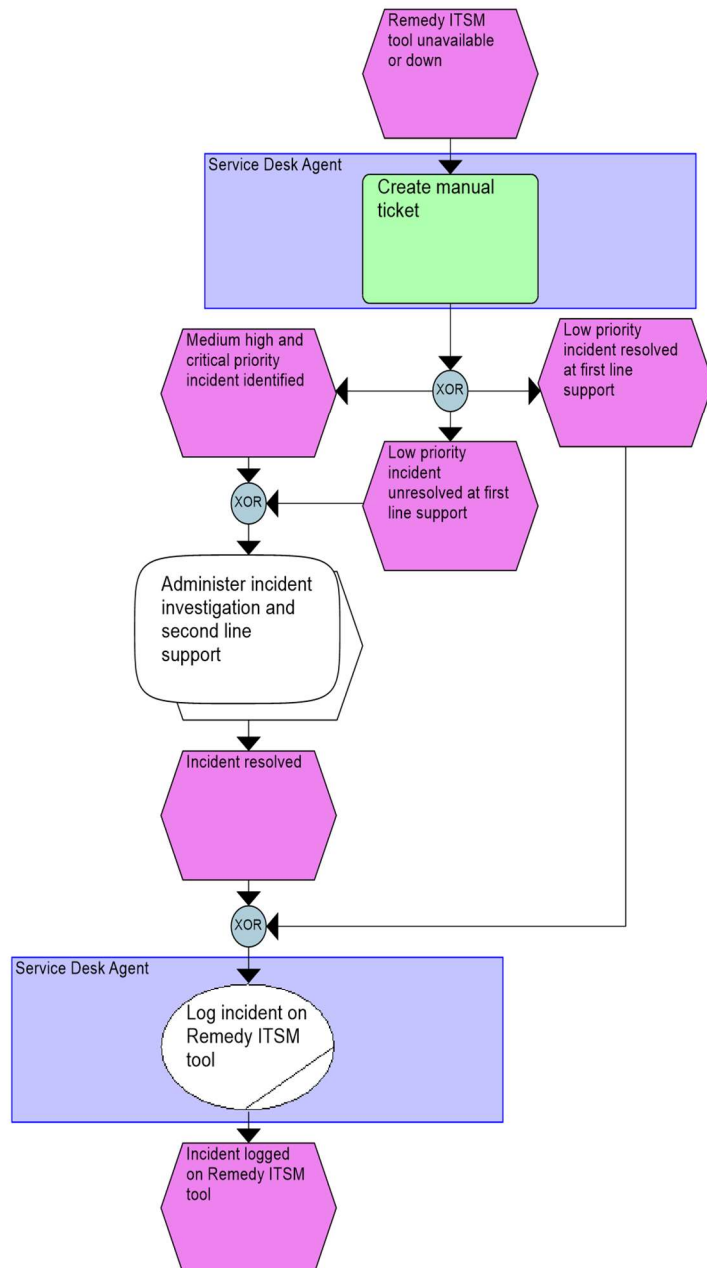
Name: RM_Manually administer ICT incidents

Category: L4 Activity Diagram

Parent object name: Administer ICT incidents manually

ENTERPRISE ARCHITECTURE (EA)

Update Date: 2018/06/07 11:42:17 AM



PROCEDURE STEP	ROLE
a) Create manual ticket. <ul style="list-style-type: none"> i) Capture the user's information and the incident information on a manual ticket logging form; ii) Provide the reference number: prefix of the agent's surname and four (4) digits e.g. BEUK 0001; iii) Validate the impact, urgency and priority level of the incident: <ul style="list-style-type: none"> A) If the priority level of the incident is Low: <ul style="list-style-type: none"> I) Perform first line support while the user is on the line, recording all the information on a manual Word document; and II) Mail the manual ticket logging form to the responsible Support Team (second line support) / Third Party Vendor and Incident Management. B) If the priority level of the incident is medium, high, or critical: <ul style="list-style-type: none"> I) Mail the manual ticket logging form to the responsible Support Team (second line support) / Third Party Vendor and Incident Management; and II) Continue with the process "Administer incident investigation and second line support". iv) Mail IT Service Desk and Incident Management mail groups to archive the forms. 	IT Service Desk Agent (R)
b) Log the incident on the ITSM tool. <ul style="list-style-type: none"> i) When services are restored, the IT Service Desk Agents will retrieve the forms from the mail group, log and attach all emails on the Work Info on the ITSM tool. 	IT Service Desk Agent (R)

3 MEASURES

e) None.

4 REFERENCES

4.1 Legislation

TYPE OF REFERENCE	REFERENCE
Legislation and Rules administered by SARS:	South African Revenue Service Act, No. 34 of 1997
Other Legislation:	None.
International Instruments:	None.

4.2 Cross References

DOCUMENT #	DOCUMENT TITLE
SS-TECH-06	ICT Quality Assurance Management - Internal Policy
SS-TECH-08	ICT Change Management - Internal Policy
SS-TECH-08-S01	ICT Change Management - Internal SOP
SS-TECH-09	ICT Problem Management – Internal Policy
SS-TECH-10	Incident Management – Internal Policy

4.3 Quality Records

a) None.

5 DEFINITIONS AND ACRONYMS

Asset Configuration Item (CI)	The SARS Barcode (CI) of any item required when logging a ticket.
Classify	Providing information regarding business and user impact in order to restore services as quickly as possible.
T&SD	Technology and Solutions Delivery.
ICT	Information and Communication Technology.
IM	Incident Management.
ITSM	Information Technology Service Management.
Nominated Representatives	Service Level Management (SLM) / Service Level Coordinator (SLC), IT Help Desk, Support Group, IM, and Users.
Priority, Impact & Urgency Matrix	Service Interruption declared by the Service Support Manager and or Resolution Manager.
Problem	Underlying root cause.
QA	Quality Assurance.
RCA	Root Cause Analysis - Problem Management sub-process that identifies the underlying root cause of a problem.
Requestor	Customer that is requesting a service.
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.
SARS	South African Revenue Service.
SLC	Service Level Coordinator.
SLM	Service Level Management.
SOP	Standard Operating Procedure.
Supporting Documentation	Any documents that relates to the service, including error messages, mandatory request forms etc.
Ticket	A request for a service logged on the ITSM Tool.

6 DOCUMENT MANAGEMENT

Business Owner	Ares Head: IT Services, Operations and Support
Document Owner	Head: Business Design and Engineering
Author	Operational Specialist: Business Design and Engineering: Policies and Procedures
Detail of change from previous revision	Amendments are highlighted in red.
Template number and revision	GC-TM-15 – Rev 7