Author:

Written/Revised by: (Name, Position)	Signature:	Date:
Alfred Kilamile, Infrastructure Support Analyst		12/2/2024

Approval cycle:

Reviewed by: (Name, Position)	Signature:	Date:
Martin Ringia		12/02/2024

Authorized by: (Name, Position)	Signature:	Date:
Paul Kasanga (IBA Head) IBA Head		12/02/2024

Document Change Control

Date	Version	Updated by	Change details
01/05/2015	1.0	Catherine Shayo	Initial template
26/05/2015	1.1	Japhet Massawe	Draft for Initial Review
22/06/2015	1.2	Catherine Shayo	General update and formatting
17/07/2015	1.3	Japhet Massawe	Final edit and formatting
31/01/2020	1.4	Mwema Mwamasimbi	General update and formatting
23/08/2022	1.5	Elias Ntulu	Formatting
04/02/2024	.16	Martin Ringia	Updates

Purpose

The primary goal of the Incident Management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

Objectives

i. Provide a consistent process to track incidents that ensures:
ii. Incidents are properly logged
iii. Incidents are properly routed
iv. Incident status is accurately reported
v. Queue of unresolved incidents is visible and reported
vi. Incidents are properly prioritized and handled in the appropriate sequence
vii. Resolution provided meets the requirements of the SLA for the user

Definitions

The table below lists some definitions of key terms within the incident management process.

	Definition
Incident	An unplanned interruption to an IBA service or a reduction in the quality of an IBA service. Failure of a configuration item that has not yet impacted a service is also an incident
Event	A change of state which has significance for the management of a Configuration item or IBA Service. The term "event" is also used to mean an alert or notification created by any IBA Service, configuration item or monitoring tool.
Incident Record	A record containing details of an Incident. Each incident record documents the Lifecycle of a single incident.
Task Record	One or more child records linked to the incident. Used to allocate work to additional teams or Collaborate in the resolution of the incident.

Incident Management guidelines

i. All Incident Records must be raised and managed within the strategic service management OS Ticket.

ii. All Incidents must be assigned a priority rating which is calculated based on the impact and urgency of the incident by a member of ICT.

iii. Incident records must be raised for any issue identified within any of the in-scope ICT environments (i.e. Production, DR, UAT and Development).

iv. If the Incident was caused by change it must be linked to the relevant change record – note if no change record can be found, this must be escalated to Service Delivery TL as a potential breach of the change process to be tabled on CAB for disciplinary action.

v. Any incident that is determined to be a major incident (impact 2 or above), must be raised as a major incident immediately via team lead appointed in case of their absence.

vi. All incidents must be documented (within the OS Ticket) with full details of all actions taken and any additional information received to ensure that there is a full audit trail.

vii. All Incidents must have the root cause documented within Incident record (identified during the Incident lifecycle)

viii. Incident records must have an appropriate status (Open, Closed, Resolved & In progress) set at the point the incident is reported.

Roles and responsibilities

Role	Responsibility
Requestor	Person rising the call-Note; Call maybe raised on behalf of affected person-e.g., CEO Issues maybe logged directly via service desk portal (OS Ticket) or by walking or by sending email to helpdesk@ccbrt.org also my followup the concern via helpdesk number 100

Incident Owner	Group owning the incident - first " touchpoint" group. This is either the support function that has raised the record or the Technical Support Team that a customer has assigned their record to (this is not applicable to a major incident). Logs the Incident in the Helpdesk system (currently OS Ticket). Assesses the nature & impact of the issue. Sets the priority rating based on impact and urgency. Resolves the issue immediately (if possible). Status changed to "In progress" and feedback provided if cannot be resolved immediately. Document the resolution/mitigation that has been taken for solving the incidence.
Incident Assignee	Individual within the Incident Assignment Group that is working on the incident. Additional Assignees allocated to tasks. Gathers facts and investigates incident Generates tasks to other groups if cross-team assistance is required Identifies solution / workaround and updates incident record Implements solution / workaround and verifies outcome with customer Updates knowledge article if required. Initiates problem management process if root cause is unknown.
MIM (major incident management)	Person responsible for owning the major incident at a point in time. Note - this role is occupied by someone in the technical team that is leading Single point of control & coordination for all incident recovery activities Primary interface to the incident management process Responsible for the production and implementation of an agreed recovery plan Ensures that accountable executive and key stakeholders are kept informed Authorizes all agreed actions/changes and monitor results

	Controls information flow across the recovery teams
Incident MIM manager	Makes initial evaluation of business impact with incident/service owner to identify impact level Confirms incident qualifies as a major incident Escalates/de-escalates if incident is at the wrong level Ensures with the incident owner that the correct resources are allocated Monitors recovery plan until service is restored Ensures major incident communications are sent within defined timelines Closes incident bridges and stand down resources Ensures process link to problem management
MIM technical support	Ensure that appropriate resources are engaged in service recovery activities Implement changes authorized by the incident owner. Provide updates and recommendations to the incident owner Verify technical recovery outcomes & organize testing / live proving as required. Undertake parallel lines of investigation / recovery as directed by the incident owner. Perform internal escalations to senior management as required.

MIM Accountable Executive	Accountable person in event of major incident management - derived from business Service owners. Focused on the recovery of business service and coordinating the business recovery stream Provides on-going confirmation to incident owner on service recovery plan and incident severity level. Confirms business communication & timeline plan with service owner Accepts accountability for all actions proposed by incident owner Ensures incident owner has sufficient resources and technical authorities to recover service quickly Confirms and reviews on a regular basis that the recovery plan meets business requirements and priorities. Maintains regular communication with the business on the incident and service recovery plan

Incident Priority Classifications

The classification of incident records is based on the urgency of the underlying issue set against the impact that the incident has on the user/customer base.

Priority = (urgency (criticality) + impact level)/2

Notes:

i. Urgency is defined by the criticality of service – the more important the service, the higher the urgency to resolve the Incident. Criticality is tier based

ii. Impact is defined at the number of users affected ranging from extensive/widespread to local /single user. This is allocated by the Service Desk agent when logging the incident.

iii. The priority is then derived basing urgency (criticality) and impact divided by 2 as illustrated above

NB – where necessary, the priority of an incident record may be overridden in order to meet business.

Priority Matrix

S/N	User impact	Criticality 1	Criticality 2	Criticality 3	Criticality 4	Criticality 5
1	Extensive/widespread	P1	P1	P1	P3	P3
2	Significant/large	P1	P2	P3	P3	P4
3	Moderate/limited	P2	P3	P3	P4	P4
4	Minor/localized/single user	P3	P3	P4	P4	P4

ICT Incident Managemetn Responsibilities

MIM Technical Support	Ensure that appropriate resources are engaged in service recovery activities Implement changes authorized by the incident owner. Provide updates and recommendations to the incident owner Verify technical recovery outcomes & organize testing / live proving as required. Undertake parallel lines of investigation / recovery as directed by the incident owner. Perform internal escalations to senior management as required.
MIM Accountable Executive	Accountable person in event of major incident management - derived from business Service owners. Focused on the recovery of business service and coordinating the business recovery stream Provides on-going confirmation to incident owner on service recovery plan and incident severity level. Confirms business communication & timeline plan with service owner Accepts accountability for all actions proposed by incident owner

Priority Matrix

S/N	User impact	Criticality 1	Criticality 2	Criticality 3	Criticality 4	Criticality 5
1	Extensive/widespread	P1	P1	P1	P3	P3
2	Significant/large	P1	P2	P3	P3	P4
3	Moderate/limited	P2	P3	P3	P4	P4
4	Minor/localized/single user	P3	P3	P4	P4	P4

ICT Incident Managemetn Responsibilities

MIM Technical Support	Ensure that appropriate resources are engaged in service recovery activities Implement changes authorized by the incident owner. Provide updates and recommendations to the incident owner Verify technical recovery outcomes & organize testing / live proving as required. Undertake parallel lines of investigation / recovery as directed by the incident owner. Perform internal escalations to senior management as required.
MIM Accountable Executive	Accountable person in event of major incident management - derived from business Service owners. Focused on the recovery of business service and coordinating the business recovery stream Provides on-going confirmation to incident owner on service recovery plan and incident severity level. Confirms business communication & timeline plan with service owner Accepts accountability for all actions proposed by incident owner

	Ensures incident owner has sufficient resources and technical authorities to recover service quickly Confirms and reviews on a regular basis that the recovery plan meets business requirements and priorities. Maintains regular communication with the business on the incident and service recovery plan

Incident Support Flow

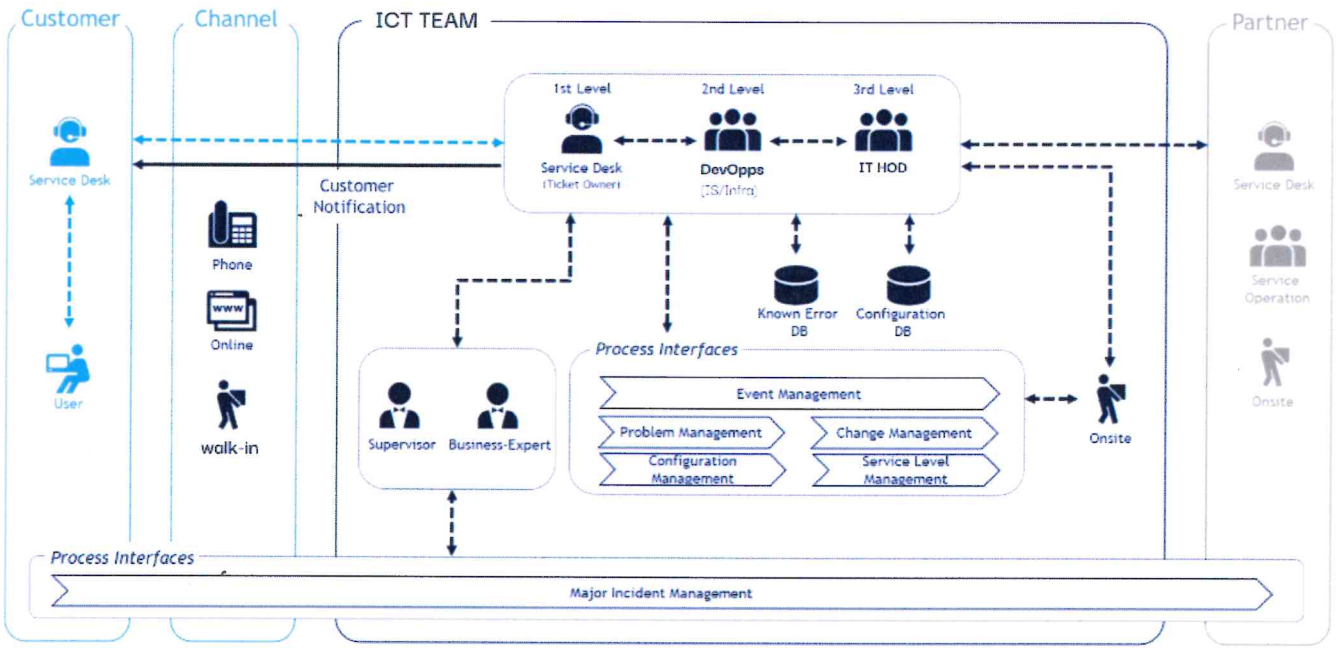

Figure1: Incident Support flow

Incident management lifecycle

This section outlines the key steps in the process and who is responsible for them.

Phase	Activity	Responsible
Incident Detection	Incidents are detected through either: a call contacting the Service Desk; a caller logging an issue via OS Ticket; or a support technician	caller
	Identifying an issue	Support Technician
	Raise a new incident record to document the issue (manually or automated) Identify and validate callers' details (if required) Assess the nature of the issue Resolve immediately via reference to knowledge	Incident owner
Incident Logging, classification Prioritization	Ensure incident classification is correct	Caller
	Establish priority based on impact and urgency	
	Establish priority based on impact and Urgency Ensure incident has been assigned to the correct support Group	Support technician
	Perform incident matching against previous incident, I problem or known error	Incident owner

	Map related change record to incident if it is caused by change	
Incident investigation and diagnosis	Set service status to degraded if there is service interruption	caller
	Initiate major incident management process if required	Support technician
	Gather facts and investigate incident	Incident owner
	Assigns tasks to other teams if collaboration is required	Incident assignee
	Identify solution or work around and update incident record	Incident assignee

Incident resolution and recovery	Implement solution or work a round (raise change if required)	Technical support
	Verify service recovery with end user	Support technician
	Initiate problem management process if root cause analysis is required	Incident assignee
	Restore service status to on-line Issue communications and update incident record to be "resolved"	
Incident closure	Incident record will be closed by the incident assignee from Service	Support technician
	Management toolset (OS Ticket)	Incident assignee

Table VI Incident Management lifecycle

Incident Escalation

The reason for Incidence Escalation is to allow ICT Department Team to identify, track, monitor and manage situations that require increased awareness and swift action.

ICT Department has Hierarchical Escalation. 1st level Support (Support Team) is unable to resolve the issue so it is escalated to 2nd level Support (Infrastructure Team). In case they are also not able to solve the issue they are escalating it to 3rd level Support (Business Application Team).

Escalation Management Process

The process could consist of the following activities:

i. Initiate an Escalation based on meeting specific escalation criteria.
ii. Assign an Escalation Leader (e.g., Team Leader) for the escalation.
iii. Log the Escalation and link the Escalation record to related Incident.
iv. A Hierarchical Escalation (as per Incident Management process) is initiated.
v. Escalation Team works to resolve the problem. At each stage, records are updated and management contacts and team are informed of the progress and escalation plan reviewed and adjusted as required
vi. Once resolved to the Customer's satisfaction the situation is monitored for an agreed period.
vii. The Escalation team remains on standby and available in case the problem recurs during the monitoring period
viii. Once the monitoring period is successfully completed, the escalation is closed by the Escalation Leader, after seeking agreement with the Client.