# ICT SERVICE DESK POLICY


**APPROVED BY:**

**MR M NAKO**

**MUNICIPAL MANAGER**

**DATE:** 21/06/2023

**APPROVED BY:**

**CLLR S JANDA**

**EXECUTIVE MAYOR**

**DATE:** 21/06/2023

## 1. POLICY BACKGROUND

The main objectives of the service desk is to restore service as quickly as possible (incident management) and to fulfil service requests efficiently and effectively (request fulfilment).

## 2. POLICY PURPOSE

To make sure that the service provided by ICT to users is efficient and effective and issues are recorded and processed.

## 3. DEFINITIONS

| | |
|---|---|
| **BCM** | Business continuity management |
| **BIA** | Business impact analysis |
| **BRM** | Business relationship management |
| **CI** | Configuration item |
| **CMS** | Configuration management system |
| **COBIT** | Control Objectives for Information and related Technology |
| **CRM** | Customer relationship management |
| **CSF** | Critical success factor |
| **CSI** | Continual service improvement |
| **DIKW** | Data-to-Information-to-Knowledge-to-Wisdom |
| **ISM** | Information security management |
| **ISMS** | Information security management system |
| **ISO** | International Organization for Standardization |
| **ITSCM** | IT service continuity management |
| **ITSM** | IT service management |
| **itSMF** | IT Service Management Forum |

**Alert** -A notification that a threshold has been reached, something has changed or a failure has occurred.
**Capabilities** -The ability of an organisation, person, process, application, configuration item or IT service to carry out an activity. Capabilities are intangible assets of an organisation.
**Configuration item** -A configuration item (CI) is any component that needs to be managed in order to deliver an IT service. Information about each CI is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by service asset and configuration management. CIs are under the control of change management. CIs typically include IT services, hardware, software, buildings, people and formal documentation such as process documentation and SLAs.

**Configuration management database** -A configuration management database (CMDB) stores configuration records containing attributes of CIs and their relationships. A CMS may include one or more CMDBs.
**Configuration management system** -A configuration management system (CMS) is a set of tools, data and information that is used to support service asset and configuration management. The CMS is part of an overall service knowledge management system and includes tools for collecting, storing, managing, updating, analysing and presenting data about all configuration items and their relationships. The CMS may also include information about incidents, problems, known errors, changes and releases. The CMS is maintained by service asset and configuration management and is used by all IT service management processes.
**Configuration model** -A configuration model is a model of the services, assets and the infrastructure that includes relationships between CIs, enabling other processes to access valuable information (e.g. assessing the impact of incidents, problems and proposed changes; planning and designing new or changed services and their release and deployment; optimising asset utilisation and costs).
**Customer** -Someone who buys goods or services. The customer of an IT service provider is the person or group who defines and agrees the service level targets. The term is also sometimes used informally to mean user.
**Definitive media library** -A definitive media library (DML) is one or more locations in which the definitive and approved versions of all software CIs are securely stored. The DML may also contain associated CIs such as licences and documentation. The DML is a single logical storage area even if there are multiple locations. All software in the DML is under the control of service asset and configuration management and is recorded in the configuration management system. Only software from the DML is acceptable for use in a release.
**Deployment** -Deployment is the activity responsible for the movement of new or changed hardware, software, documentation, process etc. to the live environment.
**Event** -An event is a change of state that has significance for the management of an IT service or other configuration item. The term is also used to mean an alert or notification created by any IT service, configuration item or monitoring tool. Events typically require IT operations personnel to take actions, and often lead to incidents being logged.
**Event management** -The process responsible for managing events throughout their lifecycle. Event management is one of the main activities of IT operations.
**Function** -A team or group of people and the tools they use to carry out one or more processes or activities (e.g. the service desk or IT operations).
**Incident** -An incident is an unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet impacted service is also an incident.
**Key performance indicator** -A key performance indicator (KPI) is a metric that is used to help manage an IT service, process, plan, project or other activity. Key performance indicators are used to measure the achievement of critical success factors. Many metrics may be measured, but only the most important of these are defined as key performance indicators and used to actively manage and report on the process, IT service or activity. They should be selected to ensure that efficiency, effectiveness and cost effectiveness are all managed.
**Known error** -A problem that has a documented root cause and a workaround. Known errors are created and managed throughout their lifecycle by problem management. Known errors may also be identified by development or suppliers.
**Metric** -Something that is measured and reported to help manage a process,

IT service or activity.

**Operational level agreement** -An operational level agreement (OLA) is an agreement between an IT service provider and another part of the same organisation. An OLA supports the IT service provider's delivery of IT services to the customers. The OLA defines the goods or services to be provided and the responsibilities of both parties.

**Problem** -A problem is the cause of one or more incidents.

**Process** -A process is a structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. A process may include any of the roles, responsibilities, tools and management controls required to reliably deliver the outputs. A process may define policies, standards, guidelines, activities and work instructions if they are needed.

**Release** -A release is one or more changes to an IT service that are built, tested and deployed together. A single release may include changes to hardware, software, documentation, processes and other components.

**Resource** -A generic term that includes IT infrastructure, people, money or anything else that might help to deliver an IT service. Resources are considered to be assets of an organisation.

**Risk** -Risk is defined as a possible event that could cause harm or loss, or affect the ability to achieve objectives. Risk can also be defined as the uncertainty of outcome. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred.

**Role** -A set of responsibilities, activities and authorities granted to a person or team. A role is defined in a process or function. One person or team may have multiple roles (e.g. the roles of configuration manager and change manager may be carried out by a single person).

**Service** -A service is a means of delivering value to customers by facilitating outcomes that customers want to achieve without the ownership of specific costs and risks.

**Service design package** -(Service design) document(s) defining all aspects of an IT service and their requirements through each stage of its lifecycle. A service design package is produced for each new IT service, major change or IT service retirement.

**Service improvement plan (SIP)** -A formal plan to implement improvements to a process or IT service.

**Service level agreement** -ITIL defines a service level agreement (SLA) as an agreement between an IT service provider and a customer. The SLA describes the IT service, records service level targets, and specifies the responsibilities for the IT service provider and the customer. A single SLA may cover multiple IT services or multiple customers.

**Service management** -Service management is a set of specialised organisational capabilities for providing value to customers in the form of services.

**Service option** -A service option is a choice of utility and warranty offered to customers by a core service or service package. Service options are sometimes referred to as service level packages.

**Service package** -A service package is two or more services that have been combined to offer a solution to a specific type of customer need or to underpin specific business outcomes. A service package can consist of a combination of core services, enabling services and enhancing services. A service package provides a specific level of utility and warranty.

**Service request** -A service request is a request from a user for information, for advice, for a standard change or for access to an IT service.

**Standard change** -A standard change is a pre-approved change that is low risk, relatively common and follows a procedure or work instruction.
**Strategic asset** -Strategic assets are assets that provide the basis for core competence, distinctive performance, durable advantage, and qualifications to participate in business opportunities. IT organisations can use the guidance provided by ITIL to transform their service management capabilities into strategic assets.
**Supplier** -A third party responsible for supplying goods or services that are required to deliver IT services.
**User** -A person who uses the IT service on a day-to-day basis. Users are distinct from customers because some customers do not use the IT services directly.
**Utility** -Functionality offered by a product or service to meet a particular need. Utility is often summarised as 'what it does'.
**Vital business function** -A vital business function is that part of a business process that is critical to the success of the business.
**Warranty** -A promise or guarantee that a product or service will meet its agreed requirements

## 4. APPLICATION AND SCOPE

The service desk is a function and not a process. A function is a defined group of people who carry out a process or processes. The service desk typically conducts a number of processes, in particular incident management and request fulfilment.
The service desk is made up of a group of staff trained to deal with service events. Service desk staff will have access to the necessary tools to manage these events. For most IT users within an organisation, the service desk is their only contact with the IT Department. Therefore, the impression made by the service desk in the handling of events will have a large influence on how the IT Department as a whole is viewed within that organisation.
The service desk should be the single point of contact for IT users within an organisation. The size and structure of a service desk will be driven by the size and structure of the organisation it supports. The number and skills of the IT user community and their geographical spread are factors. The service desk is the single point of contact for all IT users wishing to log an incident, report an event, initiate a change request, make a service request or raise a query regarding any of the services that the IT Department provides.

## 5. LEGISLATIVE FRAMEWORK

5.1.1 Constitution Act 108 of 1996
5.1.2 Information Technology Infrastructure Library (ITIL v3) standard

## 6. POLICY PROCEDURE

This policy is applicable to all municipal employees that uses ICT equipment as a tool of trade.

## 6.1 GENERAL POLICY PROVISIONS

### 6.1.1 BASIC CONCEPTS

#### 6.1.1.1 Methods of contacting the service desk

Traditionally, most IT users have contacted their service desk via telephone. However, there are various methods of making contact with a service desk:

- Telephone;
- Web interface;
- Automated alert;
- Email;
- Pager;
- Personal contact.

Mbhashe local municipality recommends the use of email: helpdesk@mbhashemun.gov.za or extension no. 5872 / 5825 if emails are not working in the absence of automated service desk system and in future it should implement service desk system.

#### 6.1.1.2 Single point of contact

It is very important that the service desk is the single point of contact for IT users within an organisation. Without a single point of contact, there is no control and ownership throughout the management of incidents, service requests and queries.

It is the service desk which owns incidents throughout their lifecycle. It does not matter who is working on the incident, the ownership remains with the service desk. The service desk will receive and log incidents or service request details. They will undertake first-line investigation and diagnosis with escalation if incidents or service requests are not resolved.

The existence of the single point of contact can be reinforced by advertising the sole service desk number (ext no. 5872 / 5825) or email address (helpdesk@mbhashemun.gov.za) as widely as possible.

#### 6.1.1.3 Service Desk structures

The service desk must be structured in a number of ways. The structure should be driven by the nature of the business supported. Factors such as user skill profile and geographical location of users will influence the structure.

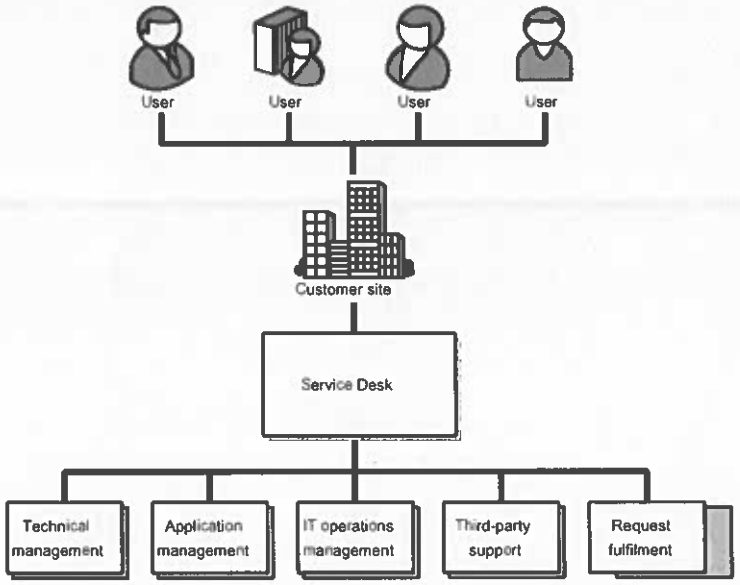
**Structures:**

- **Local service desk**
- **Centralised service desk**
- **Virtualised service desk**
- **Follow the sun**

Mbhashe Local Municipality will have to implement any of the two Service desk structures are defined below.

**Local service desk:** Local service desks (Figure 1) are situated adjacent to the users that they support. Frequently, this means that they are in the same building or on the same site as the people who contact them.

**Figure 1** Local service desk




The advantages of such a structure are visibility of the service desk function and easy communication links. However, there are disadvantages such as the risk of incidents not being prioritised in line with business impact because users are able to physically appear at the service desk and request/demand action. Another potential disadvantage is that service desk staff are not used as efficiently as they would be under other service desk structures because they are 'fixed' in one place supporting local users.

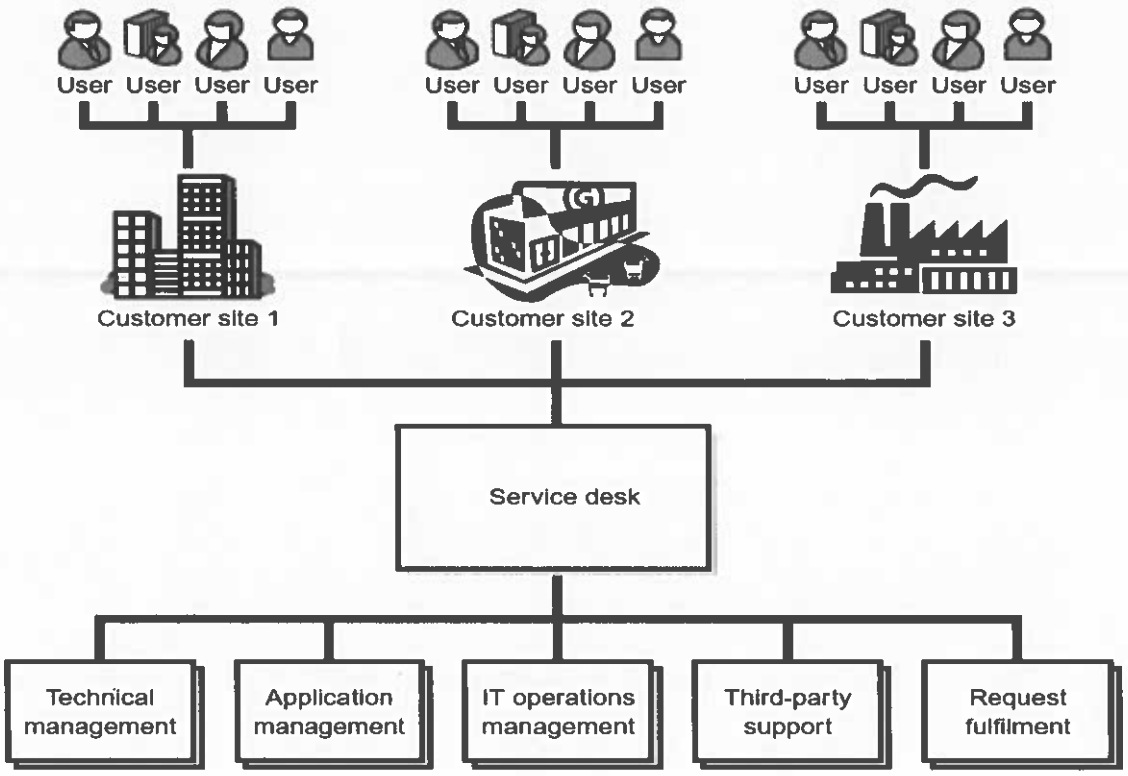
Good reasons for adopting a local service desk structure include time zone restrictions, language issues, the requirement to support a specialist group of users needing specialist support or the requirement to support specific services which again require specialist support. There may even be arguments for having a local service desk adjacent to and available to key users. Such key users may be important functionally, in that they undertake processes critical to the business of the organisation or hierarchically in that are at a senior level.

Seniority should not drive the prioritisation of an incident. Incidents should always be prioritised on the basis of business impact and urgency.

**Centralised service desk:** Implements efficiency and cost-effectiveness for Mbhashe local municipality. By adopting a single telephone number, calls from anywhere in the organisation will be directed to the centralised service desk. It should not matter to the user where their call is dealt with; their only interest ought to

be the way in which the call is handled. Centralised service desk reduce hardware requirements.

**Figure 2** Centralised service desk




**Specialised service desk groups:** Within service desks Mbhashe Local Municipality will put together specialist groups who perhaps look after one particular high profile or complex service. Where this happens, calls can be routed to the specialist group via the telephony with an option of escalating a call to specialised group.

### 6.1.2 KEY ACTIVITIES

The key activity undertaken by the service desk is to manage incidents and events as effectively and as efficiently as possible. In order to facilitate this, service desk staff need to have certain skills. It is the application of these skills, along with the use of an appropriate toolset that allows the service desk to be effective and efficient.

#### 6.1.2.1 Skills required by service desk staff

Staff should be recruited with the skills listed below. Ongoing training is required to ensure that these skills are being translated into an effective service and to ensure that the quality of that service is consistent. Service desk staff should be:

- Customer focused;

- Business aware;
- Service aware;
- Technology aware;
- Articulate.

They should have:

- Good interpersonal skills;
- The ability to translate the user description into an incident narrative.

Training will be needed on:

- The processes used by the service desk;
- Using the tool and relevant technology;
- Problem-solving skills.

### 6.1.3 RELATIONSHIPS WITH OTHER SERVICE MANAGEMENT PROCESSES

The service desk undertakes a number of service management processes, primarily incident management and request fulfilment. There will also be links to many other processes. Service level management provides the targets for incident and request handling. Change management will provide details of forthcoming changes allowing the service desk to plan, train and roster staff accordingly.

### 6.1.4 METRICS

Metrics should be put in place to measure the performance of the service desk. While call volumes are important to indicate required staffing levels, they are not a measure of service desk performance or something that the service desk can necessarily control.

Metrics for Mbhashe Local Municipality:

- The average time to resolve an incident is **2 hours** (where the incident is resolved by the service desk and not subject to functional escalation);
- The percentage of calls resolved during the first call is **80%**;
- The average time to escalate an incident **2 hours** (this will then be compared with the relevant SLA e.g SLA for email solution);
- The average time to resolve escalated calls is **24 hours** (this will depend if a technician do not have to come onsite);
- On site technician, call should be resolved with **48 hours** (this will depend if no part needs to be ordered and replaced);
- Average time to resolve and incident which needs parts to be ordered and replaced should be **7 days**.

## 7. PROCEDURES FOR IMPLEMENTING POLICY

There are number of roles to be fulfilled on a service desk. These include:

- service desk manager;
- service desk supervisor;
- service desk analyst;
- Super user.

The mix of roles will be determined by the size of the municipality being supported and the type of support being provided and Mbhashe local municipality is not forced to have all those roles.

## 8. SERVICE REQUEST

### 8.1 INTRODUCTION AND SCOPE

Request fulfilment is the process that carries out service requests from users. It covers standard change requests, requests for information and complaints. From a service desk point of view, the process of request fulfilment tends to cover all the calls that are not incidents. Password resets and queries about obtaining additional software are some of the higher volume requests.

Requests are usually high in volume, but low risk and low cost. A separate distinct process is in place to avoid confusion with the incident handling that the service desk is also undertaking.

### 8.2 PURPOSE AND OBJECTIVES

The objective of the process is to action the service requests effectively and efficiently. Request fulfilment allows users to obtain information and complete standard changes as quickly as possible.

### 8.3 SERVICE REQUEST

A service request is a request from a user for information, for advice, for a standard change or for access to an IT service.

### 8.4 STANDARD CHANGE

A standard change is a pre-approved change that is low risk, relatively common and follows a procedure or work instruction.

### 8.5 KEY ACTIVITIES

Request fulfilment should be made as simple as possible. Unlike incidents, requests ought to be predictable and planned for. It will depend on the size

and scale of an organisation whether requests are handled through the same logging system as incidents. For organisations with a large number of requests, a separate logging and progressing system may be appropriate.

The key role of request fulfilment is to handle a large number of requests efficiently and to avoid any bureaucratic bottlenecks. Users will be frustrated if a legitimate request or query cannot be efficiently handled and responded to. A holistic view of the situation can be taken by handling all the requests in one place, allowing training needs, communication gaps and requirements for standard changes to be identified.

### 8.6 REQUEST MODELS

Where high volumes of the same or similar requests are expected, a process model can be defined to standardise the activities to be undertaken. Adoption of request models will streamline the process and allow greater volumes to be processed.

Model – same model for service request will be followed but depending on the nature of request.

### 8.7 RELATIONSHIPS WITH OTHER SERVICE MANAGEMENT PROCESSES

#### 8.7.1 Financial management

There needs to be a strong link between financial management and request fulfilment to ensure that volumes, workload and use of resources are fully understood.

#### 8.7.2 Change management

Where the request model relates to a standard change, there will have been the necessary approval from change management which will have taken into account the financial management issues

## 9. INCIDENT MANAGEMENT

### 9.1 PURPOSE

This process is a structured set of activities designed to accomplish a defined objective.

All Incidents are reported through the approved Incident management software. This process focuses on reporting and resolving Incidents reported through the approved Incident management software. These may be incidents where service is being disrupted or incidents where service has not yet been disrupted.

The value of incident management to the business is that resources are allocated to minimising and mitigating the impact of incidents and service unavailability in line with business priorities. Lower levels of incidents and quicker resolution times will enable the services to run as intended.

During the handling of incidents, the service desk may be able to identify improvements in both business and technical processes. The service desk often has a unique position within organisations in that its staff can take a holistic view of how the organisation operates, allowing good practice to be propagated and bad practice to be eradicated.

The main objective of the incident management process is to restore normal service operation as quickly as possible and to minimise the adverse impact on business operations.

## 9.2 SCOPE

The Incident Management process applies to all Mbhashe local municipality employees, contracted vendors who report Incidents through the approved Incident management software. It ensures Incidents are managed in a uniform and predictable manner.

## 9.3 BASIC CONCEPTS

9.3.1 **Incident:** An incident is an unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet impacted service is also an incident.

9.3.2 **Timescales:** Timescales for incident handling and triggers for escalation must be agreed and documented in the SLA. Performance against SLA can then be measured and reported. Tools can be configured to enable automated escalation in accordance with the agreed timescales.

9.3.3 **Incident models:** The adoption of incident models is a method of standardising and automating, if possible, the approach to groups of similar incidents. An incident model is a defined set of steps to be undertaken. Incident model details can be input into the incident handling tool(s).

9.3.4 **Major incidents:** For Mbhashe local municipality, the trigger for 'calling' a major incident is when a certain number of users have been impacted and also the trigger may be the actual or potential financial loss from the loss of service. If the actual or potential financial loss is over a certain amount, the incident becomes major. There may be risk of injury or loss of life if particular services are not available. Again, this may be the trigger for the incident becoming major. Reputational damage to the municipality can be another trigger.

## 9.4 Transition

Incident Management replaces Help Desk tickets. This process includes:

- Recording Incidents
- Assigning, managing, and resolving Incidents
- Communicating Incidents

## 9.5 PROCESS DESCRIPTION

Incident Management cases are created to restore a service as quickly as possible. Incidents may be transitioned to:

- Problems if they are not resolved.
- Changes when appropriate.

**Note:** Change Management or Release Management may generate Incidents.

### 9.5.1 Recording Incidents

***Before you begin:*** To record an Incident in the approved Incident Management software, you must have access to the software. To gain access to Incident Management, submit an eAccess request and select the Incident module.

### 9.5.2 Assigning, Managing, and Resolving Incidents

The sections outlined below provide a high-level overview of the Incident Management process.

9.5.2.1 Incident Identification and Logging.

The Service Desk Analyst receives and logs the incident through an approved method.

9.5.2.2 Incident Categorization and Prioritization.

The Service Desk Analyst assigns impact and urgency to the incident.

9.5.2.3 Initial Diagnosis and Escalation.

The Service Desk Analyst determines whether the incident can be resolved by the Service Desk or whether escalation to Technical Support is required. If the incident priority is critical (major), the Critical (Major) Incident Process is followed.

9.5.2.4 Investigation and Diagnosis.

The Service Desk Analyst or Technical Support assesses the incident, escalates it if necessary, and communicates status to users impacted by the incident.

9.5.2.5 Resolution and Recovery.

The Service Desk Analyst or Technical Support analyzes the incident, applies a resolution, and notifies users of the resolution.

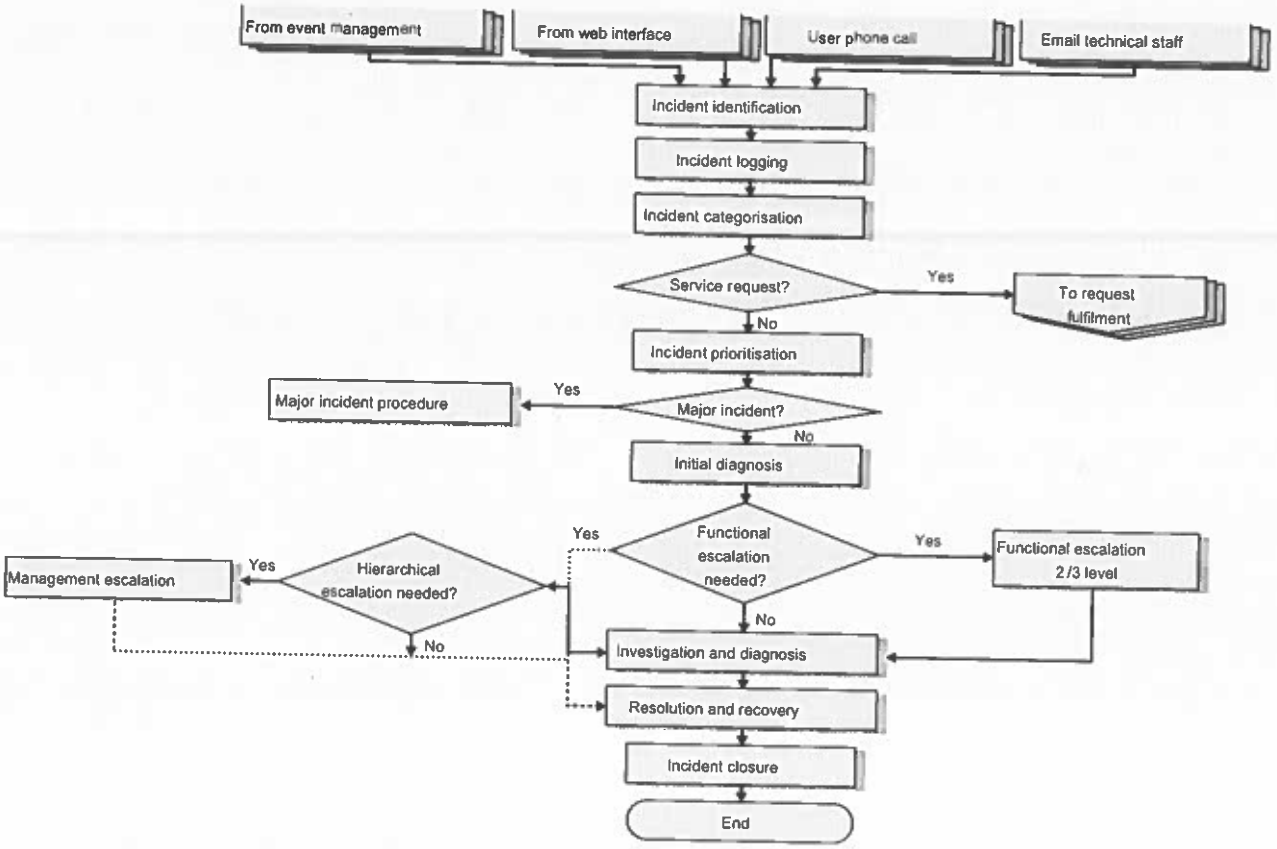
9.5.2.6 Incident Closure.

The Service Desk Analyst or Technical Support confirms the resolution with the originator and completes the incident. The incident is automatically closed after seven days of inactivity.

9.5.2.7 Incident Reopening.

The Service Desk Analyst may reopen an incident up to seven days after incident resolution. Once the incident is closed, it cannot be reopened.

**Figure 3** Incident Management process flow




## 9.6 Communicating Incidents

The Incident Management software provides a notification of the status of the Incident.

## 9.7 Critical (Major) Incident Process

A critical (major) incident has significant impact or urgency for the business and demands a response beyond the routine incident management process. An incident can be declared critical (major) only for applications in Tier 1 (business critical production services) and Tier 2 (high level support services). One of the following must be true:

- The selected Product CI is down or not responding, affecting multiple users and locations with no workaround.
- The impact of the incident is national or regional, or the incident has the potential for a significant loss of revenue.

- **Incident categorisation:** A suitable categorisation code will be allocated. For example, this may be hardware or software with sub-codes for lower level categorisation. Accurate categorisation is important because it will allow useful metrics to be gathered highlighting areas of the infrastructure where incidents are occurring.
- **Incident prioritisation:** The priority of an incident is based on the impact and the urgency. Impact is the 'pain' to the business. Impact may relate to the number of users impacted, the potential financial loss to the organisation, the risk of breach of regulatory or legislative rules or, for some services, the risk of loss of life. Urgency relates to how quickly the business requires the incident to be resolved.

**Table 1** A simplistic incident priority coding system

| | | **Impact** | | |
|---|---|---|---|---|
| | | *High* | *Medium* | *Low* |
| **Urgency** | *High* | Priority 1 | Priority 2 | Priority 3 |
| | *Medium* | Priority 2 | Priority 3 | Priority 4 |
| | *Low* | Priority 3 | Priority 4 | Priority 5 |

The process is as follows:

- **Initial diagnosis:** If the incident has been raised by a call to the service desk, then it will be the service desk which conducts the initial diagnosis, usually while the user is still on the telephone. The availability of diagnostic scripts will help as will the ability to match against problems and known errors. The CMDB may also be consulted at this stage.
- **Incident escalation:** Escalation may be functional or hierarchical.
- Functional escalation occurs when the service desk is not able to resolve the incident or where the incident has not been resolved within the target resolution time. The service desk will involve second-level support, which has more specific technical knowledge. Further functional escalation may occur through the lifecycle of the incident to third-level support, which may be part of the organisation or third parties such as suppliers. It is important to remember that the ownership of an incident always remains with the service desk regardless of which other support areas are working on a resolution.
- Hierarchical escalation raises the profile of a specific incident within the IT organisation and also within business areas. More senior IT staff are able to provide focus and resources, but ownership of the incident will be retained by the service desk. Organisations will have triggers that indicate when hierarchical escalation is required. This may be for all 'Priority 1' incidents or when incidents of a certain priority have not been resolved with a target timescale. The triggers for escalation will be recorded in the relevant

SLA and ought to be highlighted by the support tool in use. The service desk will keep the user informed of all functional or hierarchical escalations that occur during the lifecycle of an incident and at the same time the incident record will be updated.

- **Investigation and diagnosis:** In this phase of the incident lifecycle, work is undertaken by the service desk or support areas to understand what has to be done in order to restore service. This is often the most time-consuming part of the process although it can be speeded up using diagnostic scripts and by reference to other incidents and problems as well as known error databases.

- **Resolution and recovery:** The investigation and diagnosis phase will arrive at a resolution. This needs to be applied and then testing needs to take place to ensure that the incident has been resolved and service restored. There may be a time lag between a fix being applied and the service running normally again (e.g. there may be a backlog of processing to catch up on). On other occasions, it may not be possible to ascertain whether the fix has worked for a period of time (e.g. if the original issue was with a month-end process). Regardless of where the resolution has been put in place or who was involved, the incident should be passed back to the service desk for closure.

- **Incident closure:** Only the service desk should close incidents. It needs the user's agreement that the incident has been resolved. All incident documentation will have to be completed prior to closure and a closure category allocated to allow meaningful metrics to be produced. User satisfaction surveys ought to be conducted for an agreed (in the SLA) percentage of incidents. These user satisfaction surveys can be undertaken via telephone, email or web interface.

## 9.8 RELATIONSHIPS WITH OTHER SERVICE MANAGEMENT PROCESSES

Incident management is closely linked to problem management with one or more incidents being caused by a problem. There is also a strong link with change management. Changes are often implemented to resolve an incident or a number of incidents and, unfortunately, changes that do not do exactly what they were intended to do may cause incidents. Service asset and configuration management provides the information needed to manage incidents. Service level management will provide the target resolution times together with escalation criteria.

## 9.9 METRICS

Useful incident metrics include:

- The percentage of incidents resolved within SLA;
- The average cost of an incident;
- The average cost of a major incident;
- The percentage of incidents that are major.

On their own, these metrics do not necessarily give a measure of effectiveness or efficiency, but they are important in understanding the scale of the issues being raised.

## 9.10 ROLES AND RESPONSIBILITIES

Defined roles and responsibilities are key elements to the effective execution of the incident management process. Roles reflect a functional group of logical responsibilities for a given process. Responsibilities reflect the assignment of a set of duties to be implemented to complete an Incident request. Users may be assigned one or more roles.

### 9.10.1 Crisis Team

- Comprises members of the following: Network infrastructure, Application Support Teams, IT Service Providers, Service Desk.
- Troubleshoots the incident and provides timely updates to the incident ticket.
- Verifies service restoration; resolves and documents the resolution.

### 9.10.2 Critical (Major) Incident Manager

- Serves as a subject matter expert for the current critical (major) incident designated during the Crisis Bridge call.
- Manages the life cycle of the critical (major) incident and provides status updates.

### 9.10.3 Critical (Major) Incident Validation Team

- Includes members of System Application and Network infrastructure.
- Validates all non-telecom critical (major) incidents by verifying they meet the criteria for a critical (major) incident.

### 9.10.4 Critical (Major) Incident Validator

- Reviews the critical (major) incident and verifies it meets the criteria for a critical (major) incident.

### 9.10.5 End User

- Requests support when necessary and provides the required information to help resolve the requests. The incidents are submitted by filling out the Request form or by contacting the Service Desk by email or telephone.
- Confirms the solution that the service provider organization provides for incident requests and reopens them when solutions are not acceptable.

### 9.10.6 Process (Incident) Manager

- Assumes day-to-day operational responsibility of the Incident Management Process.
- Oversee production of management information, including KPIs and reports.
- Monitors process efficiency and effectiveness; ensures adherence to the process.
- Oversees development and maintenance of the Incident Management tool.
- Develops, manages, and maintains processes and procedures; participates in review and audit processes.

9.10.7 **Process Owner**

- Has overall responsibility of the Incident Management Process.

9.10.8 **Service Desk Analyst (Level 1 Support)**

- Verifies end user profiles.
- Obtains required information from users when they request support and enters that information in the Incident Management tool.
- Uses the knowledge base to troubleshoot the incident and determine priority.
- Logs and assigns the incident.
- Engages the Incident Manager to validate priority (as necessary).
- Resolves incidents.

9.10.9 **Service Desk Management Team**

- Ensures incident requests assigned to the group are resolved within the completion target dictated by the Service Level Agreements; follows up on SLA escalations.
- Escalates service outages to the appropriate support group when resolution does not occur within the period stated by the SLA.

9.10.10 **Service Manager**

- Determines whether resolution can be achieved within the Incident Management process or if Change Management is required.

9.10.11 **Service Owner**

- Owns the impacted service and is a primary stakeholder in all underlying IT processes that enable or support this service.

9.10.12 **Technical Support (Tier 2 and Tier 3)**

- Resolves incidents and updates Incident Records with relevant information and status changes.
- Escalates incidents to technical teams as required.
- Enters change requests for incidents that may be resolved only through the implementation of a change.

## 10. PROBLEM MANAGEMENT

### 10.1 Purpose

The purpose of the Problem Management Process is to capture the problems, identify the root causes of problems, provide quick resolution, to prevent problems and resulting incidents from occurring, to stop repeat incidents happening, and to minimize their impact on business operations.

Problem management, like most processes, has reactive and proactive aspects. From a reactive perspective, the purpose of the process is to manage the lifecycle of

problems from identification to elimination by determining the root cause and then applying the necessary change(s) to prevent recurrence. From a proactive perspective, the purpose of the process is to prevent future incidents wherever possible or reduce the impact of those incidents that can't be prevented.

### 10.2 Scope

The Problem Management Process includes all activities associated with the logging, acknowledgment, and classification of all problems including those in non-production environments, as well as problem response and tracking activities. Additionally, reporting tools are utilized to identify recurring problems. Such problems are communicated to the municipality for development of a long-term solution.

### 10.3 Problem models

A problem model is a similar idea to that of an incident model. Problem models provide a standardised approach to tackling problems.

### 10.4 Difference between reactive and proactive

There are two parts of problem management. Reactive problem management responds to incidents and problems that occur. The proactive side of problem management is concerned with preventing incidents and problems occurring. Proactive problem management is often triggered by continual service improvement.

Problem management should ensure that resources are involved in longer-term problem prevention as well as the here and now reactive response to problems and incidents. It is often difficult to release resources to the proactive side, especially when the reactive demands are high, but it is proactive problem prevention that allows organisations to become more mature in their service management.

### 10.5 PROCESS DESCRIPTION

The Problem Management Process aims at resolving and eliminating problems permanently from the Mbhashe local municipality technology environment in order to provide a more stable environment and reduce the impact on business and user productivity.

The Problem Management Process is composed of the following processes:

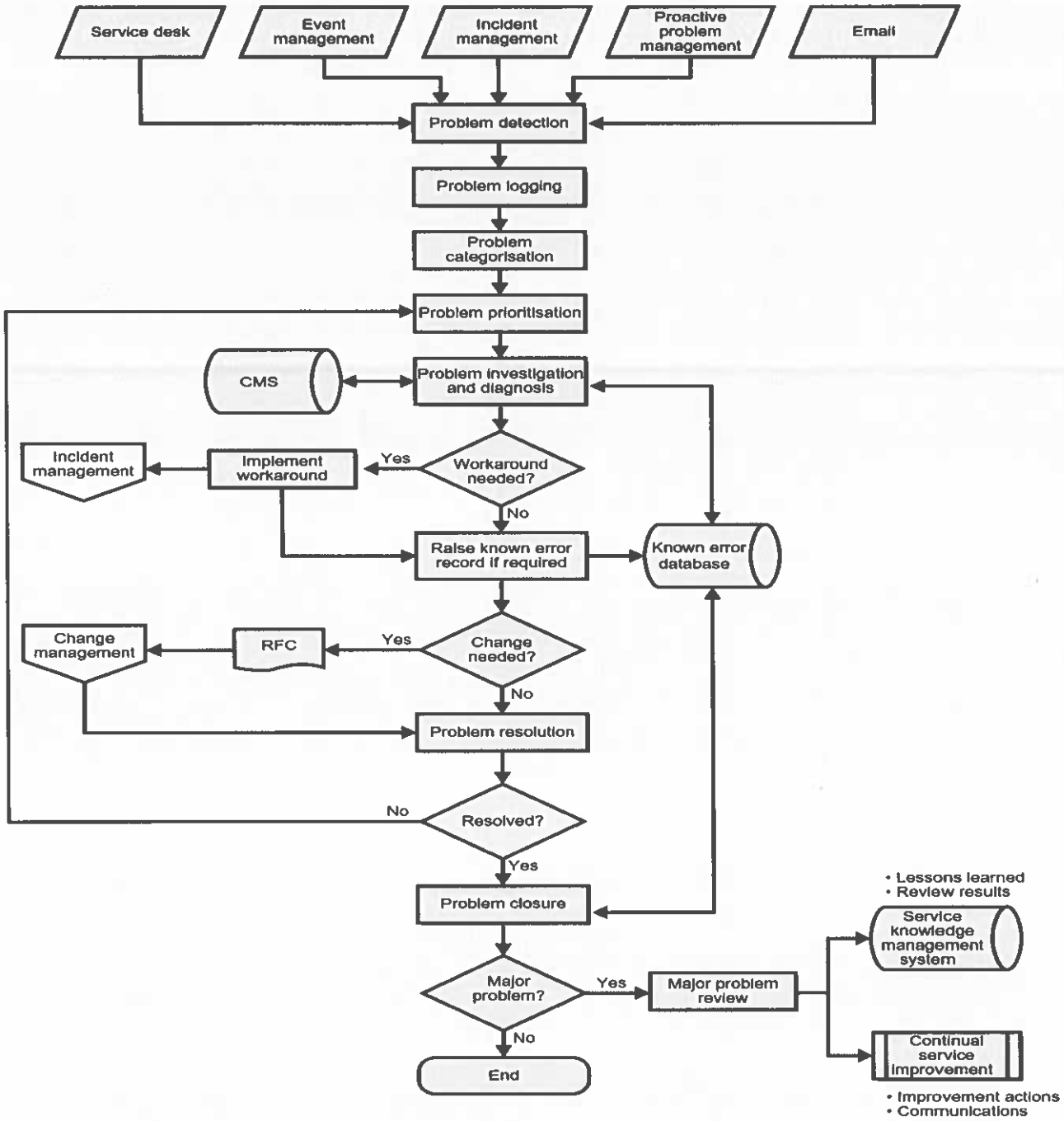
- **Problem Identification / Log:** This process detects and logs problems reported by the user; determines the impact, urgency, and priority of logged problems; identifies the reason(s) for the problem; compares problems to known errors; and correlates with other problems and alerts the support groups as necessary.

**Table 2** A simplistic problem priority coding system

| | | Impact | | |
|---|---|---|---|---|
| | | *High* | *Medium* | *Low* |
| **Urgency** | *High* | Priority 1 | Priority 2 | Priority 3 |
| | *Medium* | Priority 2 | Priority 3 | Priority 4 |
| | *Low* | Priority 3 | Priority 4 | Priority 5 |

- **Troubleshoot:** This process assesses the problem and all data associated with it in order to identify appropriate responses and actions, and to formulate a resolution.
- **Escalation:** If resolution to the problem is not found via the troubleshooting path, this process includes escalating the problem to identify potential problem resolution or workarounds.
- **Link Change Record and Problem:** This process ensures related problem cases are referenced in the Change Request (CR) and the CR is referenced in the problem case.
- **Resolve Problem:** This process includes taking the necessary actions to resolve the problem and restore service using an existing solution/workaround or escalating as necessary. Activities also include determining resolution approach, providing resolution information to the user, validating service recovery, communicating closure to the user, and setting the problem to "Resolve" status.
- **Close Problem:** In this step, the problem is set to "Resolve" status and then the system automatically closes the parent problem records and all related records five days after the "Resolve" status has been set.
- **Problem Analysis:** This process is focused on diagnosing problems to identify the root cause of the problem.
- **Provide Resolution Recommendation:** Provide business owner (customer) with recommendations (short- and long-term if applicable) to resolve problem based upon root cause analysis.
- **Coordinate with Application Support:** This process ensures that resolutions are communicated back to the Help Desk.
- **Update Knowledge Management:** This process ensures that resolutions are documented in the Knowledge Management database.

**Figure 4** Problem management process flow




## 10.6 PROCESS INPUT/OUTPUT

### Inputs

- User Call
- Logged Problem

### Outputs

- Change Request (CR)

## 10.7 ROLES AND RESPONSIBILITIES

10.7.1 **Problem Manager:** Responsible for the quality and integrity of the Problem Management process. He or she is the interface to the other process managers. The Problem Manager is also the focal point for escalation.

10.7.2 **Help Desk Agent:** Oversees the handling of the problem, bringing in analysts and specialists as needed to handle the problem. The Help Desk Agent is responsible for seeing that analysts and specialists bring the problem to a close.

**10.7.3 Problem Analyst (Tier 2 Support):** A subject-matter expert who uses technical knowledge and subject-matter expertise to discover incident trends, identify problems, and determine the root cause of problems. Responsibilities include determining what is required to solve problems and initiating appropriate actions.

## 10.8 PROACTIVE PROBLEM MANAGEMENT

It is clearly better for Mbhashe local municipality to prevent incidents occurring rather than waiting for them to occur and then committing resource to fixing them, often repetitively over time. This is the basic principle of quality assurance, as opposed to quality control, and it is not only better for Mbhashe local municipality and its users but also more efficient for IT. Problem management is therefore one of the most important processes in helping reduce the amount of time IT staff spend particularly for second and third line teams whose primary role is project-related improvement work and for whom reacting to incidents is an unwanted interruption.

In operating proactively, problem management often works closely with both the availability management process and continual service improvement since each of these aspects has similar objectives, namely to protect the IT environment from disruption and improve services wherever it is cost-effective to do so.

Proactive activities include analysing trends associated with historic incidents to identify and eliminate underlying infrastructure or application weaknesses. Proactive work may be initiated from a service improvement plan that has been created perhaps in response to poor performance or simply from a wish to improve performance, for instance in a competitive situation to gain an advantage over another service provider.

## 10.9 RELATIONSHIPS WITH OTHER SERVICE MANAGEMENT PROCESSES

There are very close connections between problem management and incident management. Also, problem management needs to work closely with the service transition processes of change management, configuration management and release and deployment management.

Information about problems and known errors will come from processes such as availability management, capacity management and IT service continuity management. The proactive side of problem management has close relationships with both continual service improvement and availability management. Financial management and service level management provide some of the cost and service guidelines to which problem management adheres.

### 10.10 METRICS

Metrics should be put in place to measure the effectiveness and the efficiency of the problem management process. Metrics should include:

- the percentage of problems resolved within the timescales set out in the SLA is **80%;**
- the average cost of resolving a problem depends if there are any financial implication to resolve a problem.
- the percentage of major problems where major problem reviews have been carried out is **80%** (where the problem is resolved by the service desk and not subject to functional escalation);
- the percentage of actions from completed major problem reviews that have been completed is **80%** (where the problem is resolved by the service desk and not subject to functional escalation);
- the number of known errors identified.

The actual number of problems identified during a period is useful to give an indication of the scale of issues and the resources required, but on its own it is not a measure of the effectiveness or efficiency of the process.

## 11. IMPLEMENTATION

2023/2024

## 12. REVIEWAL

Annually