MKHAMBATHINI MUNICIPALITY

BUSINESS CONTINUITY PLAN (BCP)

TABLE OF CONTENTS

1. PURPOSE

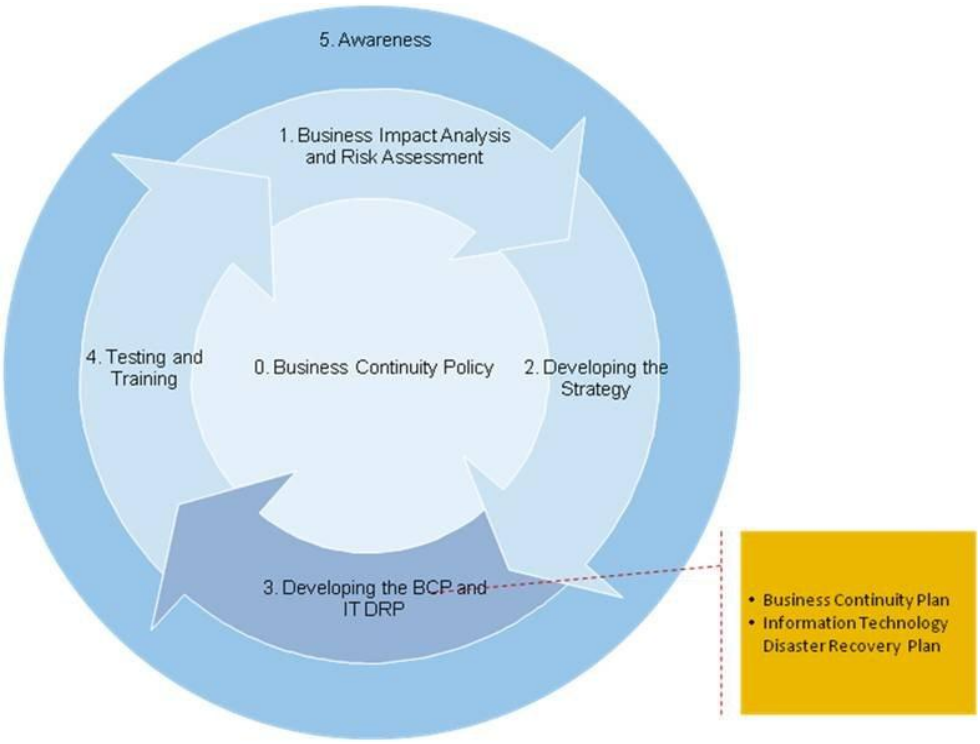
Business Continuity Planning is a proactive planning process that ensures critical services are delivered during a disruption. The main purpose of this document is to ensure that municipality's critical operations are identified and continually available. Secondly, the purpose of this document is to make a recommendation on an implementation strategy that will satisfy both the Council and Auditors.

2. INTRODUCTION

This document is the Business Continuity Plan (BCP) for Mkhambathini Local Municipality located at No. 18 Old Main Road, Camperdown, 3720. This plan is specifically designed to guide through a recovery effort of specifically identified critical organization functions and systems. One of the key tasks for management is to plan for the future and to create an optimal environment for business sustainability and growth. In line with this, management is compelled to consider and plan for the many risks that threaten normal business activities and ultimately, even the existence of the business itself. The majority of the business operations of Mkhambathini Municipality are highly dependent on the availability of ICT infrastructure and services. There is therefore a great risk to operations should a disaster strike despite the protection of insurance policies on those assets. Although assets can be later or even immediately replaced, the information on them cannot be replaced should the recovery plan not be in place.

Disasters may manifest themselves in many different ways from natural occurrences such as earthquakes or floods, or man-made such as sabotage and arson. Disasters can also be as simple as a power failure that can present a significant risk to business continuity, hence the need for continuity planning to be in place. Management depends on ICT assets including the availability of line-of-business applications and the information contained in those assets to make decisions. Management must also determine for how long the business can survive should these assets become unavailable due to natural or man-made disasters, as well as consider the implications of a possible unavailability.

The ICT Section endeavors to adhere to the ITIL best practice guidelines for IT Service Continuity Management (ITSCM). According to ITIL, the Business Continuity Management emphasis is based on the Lifecycle below:



BCP life cycle above:

3. BUSINESS IMPACT ANALYSIS

The main purpose is to determine the exact requirements of the organization and to gather all the required information to define a cost effective and efficient recovery strategy that can be implemented in a phased approach.

3.1 Disaster impact criticalities

For the purposes of the exercise mentioned above the following criticalities were defined:

Table 1 - Defined Criticalities

Criticality	Description
1 – Critical (C)	**Very serious/disastrous impact:** Inability to conduct business or perform business functions
2 – High (H)	**Serious impact:** Partial or very little ability to conduct business or perform business functions
3 – Medium (M)	**Manageable impact:** Impaired ability to conduct business or perform business functions
4 – Low (L)	**Limited to minimal impact:** Disruption with limited impact on ability to conduct business or performance of business functions

The purpose of defining the criticalities above is to provide a measure for rating the impact of a loss of a specific system or environment on the ability to conduct business or perform the required business functions to remain profitable and to effectively and efficiently service clients or communities.

Table 2 - Critical System List

#	System	Description	Hosted at?	Client Department
1	Pastel	Financial System	Mkhambathini	All
2	Municipal Billing	Billing System	Mkhambathini Offices	Revenue & Cashier
3	Sage 300	Human Resource & Payroll System	Mkhambathini	Finance & HR
4	File Server	Primary Domain Controller-provides authentication	Mkhambathini	All
5	Exchange Server	Electronic Mail Collaboration suite	Mkhambathini Offices	All
6	PABX	Telephone System	Mkhambathini Offices	All
7	Website	Organizational content published and internet mails	DMICT-Durban	All
8	Internet	Access to internet including remote access	Ion Consulting-Durban	All
9	Inter-gis	Property and valuation system	Mkhambathini	Revenue & PA' to Technical

From an organizational perspective these business processes can be mapped to a set of critical application systems. These applications can therefore be seen as enablers in the process of conducting business. The systems listed in Table 2 above are identified to be the critical systems for Mkhambathini Municipality. This table identifies the 9 critical business systems with an indication of where they are hosted and by which department(s) it is accessed.

3.2 System Loss Impact

From the above, the business processes were mapped onto critical application systems to assess the impact on business in the event of these application systems becoming unavailable or inoperable.

Some business processes and the associated application systems are more critical than others and the effect of an outage in the one instance is therefore more pronounced than in the other. It is important to determine the criticality or business impact in the case of loss of each of the identified critical systems. This will also impact on the strategy required as part of the ITSCM Process. It must be noted that as time progresses after the loss of a specific critical system the impact on the business starts to escalate. Table 4 below gives an indication of the identified criticalities for the listed critical systems as identified above:

Table 3 - System Loss Impact

#	System	Time lapsed after a disaster has occurred: Immediate	0-6 Hours	0-12 Hours	12-24 Hours	24-48 Hours	5 Days	1 Week	2 Weeks	1 Month
1	Pastel	C	C	C	C	C	C	C	C	C
2	File Server- PDC	C	C	C	C	C	C	C	C	C
3	Sage 300	C	C	C	C	C	C	C	C	C
4	Exchange	C	C	C	C	C	C	C	C	C
5	Municipal Billing	C	C	C	C	C	C	C	C	C
6	PABX	L	M	H	C	C	C	C	C	C
7	Internet	L	L	M	H	C	C	C	C	C
8	Website	L	L	M	H	C	C	C	C	C
9	GIS	L	L	M	M	H	C	C	C	C

From the table above it can be seen that Pastel, File server, Exchange, Municipal Municipality and sage 300 systems have been identified as being the most critical followed by GIS, Website and PABX systems.

3.3 System Recovery Time Target

The loss of a critical system has an immediate impact on the Municipality's ability to conduct its business and deliver services. This impact can range from Low to Critical and escalates as time progresses. As the critical state of the system and the impact on the ability to conduct business increases, so does the urgency in restoring the system to an operable state.

The System Recovery Time Target is an indication of the maximum amount of time a system can be inoperable before significant impact on business is experienced. It is therefore also an indication of the time frame within which a system must be restored to avert serious business losses. This is a further criterion for determining the required ITSCM strategy to be implemented.

Table 4 below gives an indication of the System Recovery Time Target for the identified critical systems.

Table 4 - System Recovery Time Target

#	System	System Recovery Time Target								
		Immediate	0-6 Hours	0-12 Hours	12-24 Hours	24-48 Hours	5 Days	1 Week	2 Weeks	1 Month
1	Pastel	✓								
2	File Server- PDC	✓								
3	Sage 300	✓								
4	Exchange	✓								
5	Municipal Billing	✓								
6	PABX				✓					
7	Internet				✓					
8	Website				✓					
9	GIS					✓				

4. STRATEGY DEVELOPMENT

As business processes are mapped to critical application systems these application systems can be mapped to critical ICT infrastructure. Provision must be made for the recovery infrastructure at a Remote Disaster Recovery Site in the event of a disaster.

Mkhambathini Local Municipality must ensure that an IT Disaster Recovery Site is built to ensure business continuity, and that it is up to date, meaning there must be network infrastructure, replication of data takes place, stable fibre link is established between the main office where servers are hosted and the disaster recovery site where backup servers shall be hosted. This would ensure that the municipality is always prepared for any type of disaster that might occur and that there shall be continuity in business operations.

4.1 Natural, Internal and External Threats

The list below gives an indication of the potential threats to the environment (Natural and Man-made):

- Fire;
- Explosion;
- Earthquake;
- Storms;
- Wind;
- Water;
- Floods;
- Aircraft, aerial devices or articles dropped from it;
- Riot & Strike;
- Malicious damage;
- Sprinkler leakage;
- Theft;
- Burglary;
- Arson;
- Sabotage;
- Terrorism;
- Major equipment breakdown;
- Major loss or damage to equipment; and
- Environmental impairment.

4.2 Disaster Scenarios

Taking cognisance of the afore-mentioned threats to the environment, various potential disaster scenarios specific to Mkhambathini Local Municipality were identified.

Scenario 1 – Loss of a server infrastructure in data center (server room)

In this scenario the server infrastructure in Mkhambathini offices Data Centre is rendered inoperable due to a disaster event confined to that area.

The potential threats to the environment in this scenario are as follows:

- Fire;
- Explosion;
- Water (leakage from air-conditioning units etc.);
- Malicious damage;
- Theft;
- Burglary;
- Arson;
- Sabotage;
- Terrorism;
- Major equipment breakdown;
- Major loss of or damage to equipment; and
- Environmental impairment (power, air-conditioning etc.).

Scenario 2 – Loss of the entire Data Centre

In this scenario the Mkhambathini Local Municipality is lost in totality. All equipment in the data centre is rendered inoperable.

The potential threats to the environment in this scenario are as follows:

- Fire;
- Explosion;
- Water (leakage from air-conditioning units etc.);
- Malicious damage;
- Theft;
- Burglary;
- Arson;
- Sabotage;
- Terrorism;

- Major equipment breakdown;
- Major loss of or damage to equipment; and
- Environmental impairment (power, air-conditioning etc.).

Scenario 3 – Loss of the PABX (Telephone System)

In this scenario the PABX Telephone System hosted at Mkhambathini Municipality offices is rendered totally inoperable. This scenario excludes normal breakage and lightning damage for which emergency spares will be supplied by the PABX supplier.

The potential threats to the environment in this scenario are as follows:

- Fire;
- Explosion;
- Malicious damage;
- Theft;
- Burglary;
- Arson;
- Sabotage;
- Terrorism.

Scenario 4 – Loss of Mkhambathini Local Municipality Offices

This is the worst case scenario in which the entire Mkhambathini municipality is lost or rendered inaccessible in totality.

The potential threats to the environment in this scenario are as follows:

- Fire;
- Explosion;
- Earthquake;
- Storms;
- Wind;
- Aircraft;
- Riot & Strike;
- Malicious damage;
- Theft;
- Burglary;
- Arson;
- Sabotage;
- Terrorism;

- Major equipment breakdown;
- Major loss or damage to equipment.

4.3 Business Continuity (ITSCM Strategy)

Taking cognisance of all the above information, the following must be provided for to ensure effective, efficient and timeous recovery in the disaster scenarios as defined above:

- **Alternate Recovery Facility**

It is proposed that the municipality build an alternate recovery facility. Provision must be made for the required *power supply*, *redundancy* in terms of *battery backup and generators, air-conditioning* and *fire detection* and *suppression systems*. Hosting space for 4 racks must be provided for.

Cognisance must also be taken of the office recovery seats that must be provided for at alternate sites for users to access the systems recovered at the recovery facility.

- ***Server Infrastructure***

In addition to the recovery facility, provision must be made for the entire required server infrastructure. Since technology keeps changing the exact numbers and technology will most likely be different at the time of implementation.

- ***Network Infrastructure***

  - *Scenario 1 – Loss of server infrastructure in data centre*

    It is proposed that the municipality implements redundant fibre connections between Mkhambathini offices and Disaster Recovery Site.

A second similar network infrastructure to that of Mkhambathini Local Municipality must be implemented in the Disaster Recovery Site one building including the secondary core and distribution switches. Implementation of these devices will allow for interconnecting the devices in both sites in a mesh method, therefore building full redundancy for ICT Service Continuity purposes.

- *Scenario 2 – Loss of the entire Data Centre*

  It is proposed that a fibre link between Mkhambathini offices and Disaster Recovery site be installed to allow for connectivity between the two sites in scenario where users must operate utilising the servers and systems hosted at the DR site. The municipality must ensure that not only the primary fibre link is installed, but also the redundancy link must be in place. Servers must be configured for instant replication of data.

- *Scenario 3 – Loss of the PABX (Telephone System)*

  Ideally, in order to ensure full business continuity, the municipality must have two PABX Systems, the primary system at Mkhambathini municipal offices and a secondary one in Disaster Recovery site. This will ensure the municipality is able to continue its operations in an event where the main PABX System is inoperable. It is therefore proposed that a redundant PABX be implemented at a different location that is Disaster Recovery site. This will be a classic situation of the implementation of Risk Mitigating Measures as defined by the ITL ITSCM Process. At the implementation of the secondary PABX, the procedure will have to be drawn on how the switch between the two systems will take place in case of a disaster.

- *Scenario 4 – Loss of Mkhambathini municipality offices*

  Provision will have to be made for office recovery seats at alternate client sites. Inclusive in the provisioning will be the required telephony infrastructure. Departments will decide where and for how many individuals provision will be made and will therefore also be responsible for the provision on the required telephone infrastructure.

  The fibre backbone between Mkhambathini municipal offices and the Disaster Recovery site needs to be enhanced considerably and must also cater for redundancy.

  It is further proposed that benchmarking be done with other municipalities that have successfully implemented DRP and BCP, and also source the skills of a professional consultant to test and certify the Disaster Recovery and Continuity Plan.

4.4 Advantages of providing own recovery infrastructure and facilities

Third party recovery facilities share infrastructure amongst multiple clients. This is what affords them the economies of scale but by implication every piece of equipment can be *"sold"* to at least 5 clients. In disaster situations this equipment is allocated to clients on a first come first serve basis and no guarantees exists for equipment being available. In addition to the above most of these providers charge a monthly fee for infrastructure to be available for a limited period of time, e.g. up to 1 month. If the client requires recovery equipment for longer periods a charge per day is given for every day over and above the contracted minimum period. Prolonged periods at the recovery facility can therefore

become very expensive. Clients are also limited to the number of days available for testing in the environments.

Owning and managing your own recovery infrastructure eliminates all of the above. The infrastructure is dedicated and always available at no additional cost. Testing can be done anytime, again at no additional cost. In a situation where there is a very high speed network implemented, and the recovery facility is part of the main network, options like replication to a live recovery site become available; this would have been an extremely expensive option should a third party recovery facility be utilized.

4.5 Disadvantages of providing own recovery infrastructure and facilities

The following disadvantages can be noted:

- Provision for the required facility and infrastructure is a once-off capital expenditure;
- Mkhambathini Local Municipality must ensure that the infrastructure stays in pace with the production environment;
- Mkhambathini Local Municipality must ensure that the recovery infrastructure does not get utilized for production requirements but is reserved for recovery needs;
- The recovery facility and infrastructure must be maintained to ensure that it remains adequate and serviceable at all times.

4.6 Replication / Clustering Services for BCP

The best route to recovery from a disaster is to use a replication or clustering technology or virtualization. This service ensures that the recovery system is current up to the last successful transaction and therefore recovery from backup would not be required. This however does not make backups obsolete in any way.

- Mkhambathini Local Municipality is in the process of implementing virtualization technology.
- The servers will be equipped with a 8Gbps single port fibre HBA(host bus adapter) card, providing high-speed access to the virtual hard drives hosted on the SAN.
- Each card will connect directly to the SAN providing simple and high performance fibre channel connectivity to the IMB servers.
- On the networking side of the architecture, each server will be equipped with 4 gigabit network interfaces (NIC) connecting to the following networks:
- LAN Networks 2x Gigabit Ethernet- providing connectivity to LAN
- Live Migration networks- provides migration of virtual servers between physical hosts- Bonded Interfaces
- NAS is also implemented to auto backup all data on the SAN.

5. OPERATIONAL MANAGEMET

The primary focus of this stage is the regular testing and continuous improvement of the Business Continuity Plan developed as part of the implementation stage. The BCP implemented is also frequently reviewed to ensure the recoverability at all times. The tests are also used to train additional technical staff members to ensure that capable recovery personnel are available. Training covers the various levels in the organization from technical recovery teams to the business members of the executive and coordinating structure.

As part of the education & awareness process, presentations and information sessions can be conducted to inform and sensitize the business community at all levels of the organization about all the facets of the implemented recovery plans, processes and procedures. Staff members are sensitized to the implications and requirements of the

Business Continuity Planning process and to entrench these as part of their daily working routine.

5.1 Service Summary

The infrastructure required for implementing ITSCM/ DR comprises the alternate hosting facility with entire required ICT infrastructure (Server & Network). Cognisance must be taken of the required software licenses (operating system, utility and application software).

5.2 Proposed Implementation Approach

Taking cognisance of the extensive capital expenditure required for the establishment of ITSCM/ DR for the environment, the following phased implementation approach is to be followed:

Phase 1:

- Draw up a plan for the recovery facility and have it approved.
- Provide the bill of quantities for the building.
- Build the recovery facility or recovery site
- The Recovery site must be fire proof, must be air conditioned, must have fire detection & suppression system and floor must be raised.
- Acquire the required Server infrastructure & virtualization technology be implemented.
- Be configured for alerts and replication of data
- Acquire and implement the required fibre network infrastructure between data center at the main office and the Recovery site building.

Phase 2:

- Setup the required redundant PABX Infrastructure as Risk Mitigating Measure to cater for Disaster Scenario 3 as detailed above.
- Update the BCP to cater for this scenario.

5.3 Pricing Estimates

Cost of equipment will vary from time to time as the technology develops. The pricing will be provided as and when required. It will be noted that the costs of recovery and resumption of business will be far higher if the municipality does not start early, that is at the approval of this policy to invest in the recovery site and disaster recovery centre for ICT.

- The Recovery Facility or site shall be estimated at R600 000.
- The Server Infrastructure for the site with Access control shall be estimated at R1 700 000.00
- UPS system estimated at R300 000.00
- PABX system estimated at R300 000

6. Business Continuity Plan Review

The BCP shall be reviewed annually or as and when required.

7. Custodian of the BCP

Corporate Services Department shall be the custodian of the Business Continuity Plan