PORTFOLIO COMMITTEE :

MANAGEMENT SERVICES

Chairperson :

Cllr R de Coning

Committee Members :

Ald M Sapepa, Cllrs J Kloppers-Lourens,
M Opperman & N Nqinata

PORTEFEULJEKOMITEE :

BESTUURSDIENSTE

Voorsitter :

Rdl R de Coning

Komiteelede :

Rdh M Sapepa, Rdle J Kloppers-Lourens,
M Opperman & N Nqinata

MANAGEMENT SERVICES PORTFOLIO COMMITTEE

BESTUURSDIENSTE PORTEFEULJEKOMITEE

20 JUNE 2017

I N D E X

AGENDA of the
Portfolio Committee : Management Services
20 June 2017
(Also the agenda for the Mayoral Committee Meeting : 28 June 2017)

1.
BUSINESS CONTINUITY FRAMEWORK

2/B
A Riddles **(028) 313 5044** **Corporate Head Office**
29 May 2017

1. Executive Summary

To obtain Council's approval for the Business Continuity Framework, that has been reviewed by the Risk Management Committee.

2. Service Delivery and Budget Implementation Plan - IGNITE

Directorate: Management Services
Risk Management Unit

3. Compliance with Strategic Priority

The provision and maintenance of municipal services.

4. Delegated Authority

None

5. Legal Requirements

Constitution of the Republic of South Africa

6. Background/Discussion

The purpose of a business continuity plan is to prepare the Municipality in the event of extended service outages caused by factors beyond our control (e.g. natural disasters, man-made events) and to restore services to the widest extent possible in a minimum time frame.

All Municipal departments are expected to implement preventive measures whenever possible to minimise operational failure and to recover as rapidly as possible when a failure occurs.

Instead of focusing on resuming a business after critical operations have ceased, or recovering after a disaster, a business continuity plan endeavours to ensure that critical operations continue to be available.

This framework must further be developed by the managers themselves to ensure its relevance to their departments and its eventual use in developing their department specific business continuity plans.
An explanatory report on the differences between business continuity and disaster management is circulated with the framework.

7. Financial Implications

This is only a framework and not the continuity plans itself, thus there are no financial implications yet.

The financial implications of the continuity plans will be determined during the development of the plans and should then be budgeted for by the departments and Council.

8. Staff Implications

None

9. Comments from other Departments, Divisions and Administrations

This framework was created with the input of the managers of departments responsible for the delivery of critical services and departments who must assist with the business continuity of the critical service departments.

In addition to the two scheduled workshops with managers, continuous participation took place with the risk management role players to formulate the draft business continuity framework for the perusal of the Risk Management Committee. The Risk Management Committee's considerations were taken into account in the final draft of the business continuity framework presented to Council.

10. Annexures

Annexure A: Business Continuity Framework
Annexure B: Relationship between Business Continuity and Disaster Management

RECOMMENDATION TO THE COUNCIL:

1. that the Business Continuity Framework **be approved**; and

2. that the Relationship between Business Continuity and Disaster Management **be noted**.

AGENDA of the
Portfolio Committee : Management Services
20 June 2017
(Also the agenda for the Mayoral Committee Meeting : 28 June 2017)

RESPONSIBLE OFFICIAL : **A RIDDLES**

TARGET DATE FOR IMPLEMENTATION : **1 JULY 2017**

AGENDA of the
Portfolio Committee : Management Services
20 June 2017
(Also the agenda for the Mayoral Committee Meeting : 28 June 2017)

1.
BUSINESS CONTINUITY FRAMEWORK

2/B
A Riddles **(028) 313 5044** **Corporate Head Office**
29 May 2017

THIS MATTER SERVED BEFORE THE JOINT PORTFOLIO COMMITTEE ON 20 JUNE 2017, WHICH COMMITTEE RECOMMENDED AS FOLLOWS:

RECOMMENDATION TO THE COUNCIL:

1. that the Business Continuity Framework **be approved**; and

2. that the Relationship between Business Continuity and Disaster Management **be noted**.

RESPONSIBLE OFFICIAL : **A RIDDLES**

TARGET DATE FOR IMPLEMENTATION : **1 JULY 2017**

Annexure A
1/25

OVERSTRAND MUNICIPALITY

Munisipaliteit • U-Masipala • Municipality
OVERSTRAND

BUSINESS CONTINUITY FRAMEWORK

2/25

1. Business Continuity Plan Committee

1.1. Introduction

A Business Continuity Plan (BCP) requires a governance structure in the form of a committee that will ensure senior management commitments and define senior management roles and responsibilities.

The BCP committee is responsible for the oversight, initiation, planning, approval, testing and audit of the BCP. It also implements the BCP, coordinates activities, approves the Business Impact Analysis (BIA) survey, oversees the creation of continuity plans and reviews the results of quality assurance activities.

1.2. Responsibilities

A BCP Committee must:

- approve the governance structure;
- clarify their roles, and those of participants in the program;
- oversee the creation of a list of appropriate committees, working groups and teams to develop and execute the plan;
- provide strategic direction and communicate essential messages;
- approve the results of the BIA;
- review the critical services that have been identified;
- approve the continuity plans and arrangement;
- monitor quality assurance activities;
- resolve conflicting interests and priorities; and
- meet every 6 months to review the business continuity plan.

1.3. Composition

The BCP Committee is comprised of the following members:

- Executive sponsor – Director: Management Services

The executive sponsor has overall responsibility for the BCP committee; elicits senior management's support and direction; and ensures that adequate funding is available for the BCP program.

The executive sponsor is also a co-chair of the BCP Committee.

- BCP Administrator – Risk Management Unit

The BCP Administrator secures senior management's support; estimates funding requirements; develops BCP policy; coordinates and oversees the BIA process; ensures effective participant input; coordinates and oversees the development of plans and arrangements for business continuity; establishes working groups and teams and defines their responsibilities; coordinates appropriate training; and provides for regular review, testing and audit of the BCP.

The BCP Administrator is also a co-chair of the BCP Committee.

- Operational Command Coordinator – Chief: Fire, Rescue & Disaster Management

The Operational Command Coordinator is responsible for the coordination of disaster management emergency services, such as fire and rescue, disaster management and relocation.

- Security Officer – Chief: Traffic & Law Enforcement

The Security Officer works with the BCP Administrator to ensure that all aspects of the BCP meet the security requirements of the Municipality.

- Chief Information Officer (CIO) – ICT Business Analyst

The CIO cooperates closely with the BCP Administrator and IT specialists to plan for effective and harmonised continuity.

- Communication Officer – Head of department: Communication

The Communication Officer formalises communication structures, handles internal and external communication and ensure everyone is aware of the communication policy.

- Business unit representatives (Risk Champions)

Business unit representatives (Risk Champions) provide input and assist in performing and analysing the results of the business impact analysis.

2. Business Impact Analysis (BIA)

2.1. Introduction

The purpose of the BIA is to identify the Municipality's mandate and critical services; rank the order of priority of services for continuous delivery or rapid recovery; and identify internal and external impacts of disruptions.

2.2. Steps for a BIA

2.2.1. Identify the critical services of the Municipality

This step determines what services must be delivered. Information can be obtained from the IDP of the Municipality and legal requirements for delivering specific services.

Based on basic service delivery needs of the community, legal requirements and the support functions required to deliver the services and meet the legal requirements, the following critical services have been identified:

➢ Technical and Community Services
- Water supply
  - extraction / sourcing
  - treatment
  - distribution
- Electricity supply
  - purchase of electricity
  - distribution of electricity

- electrical support services
- Sewerage removal
- removal
- treatment
- Solid waste removal
- collection
- processing
- disposal
- Roads & storm water maintenance
- repair of roads
- maintenance of roads
- maintenance of sidewalks
- repair of storm water systems
- maintenance of storm water systems
- Support services
- Finance
- payroll
- asset management
- insurance
- supply chain management
- revenue management
- budgeting
- accounting
- Information and Communication Technology (ICT)
- computers
- screens and projectors
- network infrastructure
- telephones
- internet capability
- software
- servers
- server room
- ICT support services
- Human Resources (HR)
- employee administration
- recruitment and appointment
- occupational health and safety
- labour relations
- Legal
- legal representation
- legal advice
- municipal court
- Administrative services
- Support buildings & structures
- offices
- workshops
- work sites
- archives
- inventory stores
- parking lots
- Communication
- public relations

- media relations
- Advice on statements and answers prepared by municipal officials or political office bearers.

➢ Oversight and Strategic Services

• Top Management
- Municipal Manager
- Directors

• Council
- Ward Councillors
- Proportional Councillors
- Portfolio Committees
- Speaker

• Mayoral Committee
- Mayor
- Deputy Mayor
- other Mayoral Committee members

• Internal Audit
• Joint Audit and Performance Audit Committee (JAPAC)

2.2.2. Identify risks to business continuity

Risks are identified in the BIA. Mitigating risk is an ongoing process and must be performed even when the BCP is not activated.

For example, if a municipality requires electricity for service delivery, the risk of a short term power outage can be mitigated by installing stand-by generators.

Another example would be a municipality that relies on internal and external telecommunications to function effectively. Communications failures can be minimised by using alternate communications networks or installing redundant systems.

The risks to business continuity are the following:

Ranking	Risk
1	Lack of communication mediums (internet, email, telephone, cell phone)
2	Lack of electricity
3	Downtimes at water treatment plants.
4	Downtimes at sewerage treatment plants.
5	Cyber attacks
6	Security of infrastructure
7	Loss of key personnel
8	Disruptions in supply chain management
9	Social conflict
10	Fires
11	Floods
12	Strong winds
13	Tsunami
14	Compromised employee health and safety

2.2.3. Prioritise critical services

Once the critical services are identified, they must be prioritised based on minimum acceptable delivery levels and the maximum period of time the service can be down before severe damage to the Municipality results.

To determine the ranking of critical services, information is required to determine impact of a disruption to service delivery, loss of revenue, additional expenses and intangible losses.

3. Business Continuity Plan Quality Assurance

3.1. Review

Review of the BCP should assess the plan's accuracy, relevance and effectiveness. The review should also uncover which aspects of the BCP needs improvement.

The BCP must be reviewed on the following occasions:

- Scheduled review

The BCP must be reviewed at least 365 days after the last review or changes.

- Changes in risks

The risks identified during the BIA changes. The disruptions covered in the BCP are based on the risks identified in the BIA.

- Changes in critical services

The critical services identified during the BIA changes. Recovery operations in the BCP only exist for the critical services identified in the BIA.

- Changes in personnel or contact details

The BCP must be updated to include up to date personnel and contact details.

- Changes to the Municipality's organisational structure or operations

Changes to the Municipality's structure (e.g. directorates and departments) or operations (e.g. replacement of people with machinery) can make the BCP outdated and inadequate for business continuity purposes.

- After exercises and tests

The results of business continuity exercises and tests must be incorporated into the BCP if applicable.

3.2. Assurance

Continuous evaluation of the BCP is essential to maintain its effectiveness.

The Risk Management Unit should play an oversight role, as it is strategically located to challenge the reliability and realism of the business continuity plans, among other things.

Internal Audit Services should provide assurance on the accuracy and reliability of the information contained in the components of the business continuity framework.

Assurance concerns all aspects of the framework; it tests processes to ensure that information is complete, accurate and valid. Assurance can be provided by either Internal Audit Services, Risk Management Unit or/and external assurance providers.

4. Business Continuity Plan

4.1. Introduction

The purpose of this business continuity plan (BCP) is to prepare the Municipality in the event of extended service outages caused by factors beyond our control (e.g. natural disasters, man-made events) and to restore services to the widest extent possible in a minimum time frame. All municipal departments are expected to implement preventive measures whenever possible to minimise operational failure and to recover as rapidly as possible when a failure occurs.

The BCP identifies vulnerabilities and recommends necessary measures to prevent extended service outages. It is a plan that encompasses all municipal systems, departments and operation facilities.

Apocalyptic disasters such as a nuclear war are beyond the scope of this plan.

4.2. Business Continuity Plan Objectives

- Serves as a guide for the Municipal recovery teams.
- References and points to the location of any information/plans that reside outside this document.
- Provides procedures and resources needed to assist in recovery.
- Identifies vendors and customers that must be notified in the event of a disaster.
- Assists in avoiding confusion experienced during a crisis by documenting, testing and reviewing recovery procedures.
- Identifies alternate sources for supplies, resources and locations.
- Documents storage, safeguarding and retrieval procedures for vital records.
- Key people (Team Leaders or Alternates) will be available following a disaster.
- This document and all vital records are stored in a secure offsite location to survive a disaster and be accessible immediately following the disaster.
- Each support organisation will have its own plan consisting of unique recovery procedures, critical resource information and procedures.

4.3. Mitigating Risks

Risks are identified in the business impact analysis (BIA). Mitigating risk is an ongoing process and should be performed even when the BCP is not activated.

For example, if the Municipality requires electricity for ICT, the risk of a short term power outage can be mitigated by installing stand-by generators.

Risk	Cause of risk	Critical Services Impacted	Reason for mitigation	Mitigation strategy	Mitigating actions
Lack of communication mediums (internet, email, telephone, cell phone)	▪ Lack of available bandwidth. ▪ Congestion of airwaves used for wireless bandwidth. ▪ Malfunctioning communication equipment. ▪ Wind ▪ Failure of network infrastructure. ▪ Lack of electricity supply. ▪ Lack of cellular coverage. ▪ GroupWise malfunctioning.	All municipal services.	Ensure service delivery.	Treatment	▪ Electricity generators. ▪ UPS for servers. ▪ Upgrading of hardware to increase bandwidth capacity. ▪ Replacement of faulty telephones. ▪ Shift from public airwaves to restricted airwaves for less congestion. ▪ Replacement of faulty modems and routers. ▪ Switch between cellular service providers. ▪ ICT support staff available to restore GroupWise functionality.
Lack of electricity.	▪ Inability of Eskom to meet demand. ▪ Fires that destroy power lines. ▪ Technical faults in the electrical wiring or switchboards of buildings. ▪ Ageing infrastructure ▪ Theft of and damage to electricity infrastructure.	▪ Electricity supply ▪ Water supply ▪ Sewerage removal ▪ Support services ▪ Administrative services ▪ Oversight and strategic services	▪ Ensure delivery of electricity when Eskom reduces supply. ▪ Ensure service delivery during blackouts.	Treatment	▪ Fixed electricity generators ▪ Mobile electricity generators ▪ UPSs ▪ Repair and replacement of ageing electricity infrastructure. ▪ Repair and replacement of stolen / damaged electricity infrastructure. ▪ Load shedding
Downtimes at water treatment plants.	▪ Ageing infrastructure. ▪ Lack of electricity. ▪ Veld fires	Water supply	Ensure continuous supply of clean water.	Treatment	▪ Repairs and replacement of ageing water infrastructure. ▪ Applications for infrastructure grants to upgrade water treatment plants. ▪ Electricity generators at critical water treatment plants.

Risk	Cause of risk	Critical Services Impacted	Reason for mitigation	Mitigation strategy	Mitigating actions
Downtimes at sewerage treatment plants.	▪ Ageing infrastructure. ▪ Lack of electricity. ▪ Veld fires.	Sewerage removal	▪ Prevent untreated sewerage from entering the environment and water resources. ▪ Compliance with legislation. ▪ Protect reputation of Overstrand Municipality. ▪ Disease control	Treatment	▪ Repairs and replacement of ageing sewerage infrastructure. ▪ Applications for infrastructure grants to upgrade sewerage treatment plants. ▪ Electricity generators at critical sewerage treatment plants.
Cyber attacks	▪ Poor cyber security awareness among municipal employees. ▪ Continuous evolvement and creation of new malicious code. ▪ Inadequate network and/or internet security. ▪ Poor access controls.	All municipal services.	▪ Prevent theft from bank accounts. ▪ Prevent fraudulent transactions from being recorded in or deleted from the accounting records. ▪ Protect confidential data and information. ▪ Protect the network from malware infection. ▪ Ensure continuous uptime of ICT capabilities. ▪ Protect software components of infrastructure.	Treatment	▪ Symantec cyber security software. ▪ ICT security measures part of ICT policies. ▪ Internet usage directives. ▪ Backup of data. ▪ ICT control room door always locked and uses a fingerprint lock system. ▪ Server room located in locked ICT control room, with its own locked door.
Security of infrastructure	▪ Vandalism ▪ Theft ▪ Unauthorised access	All municipal services can be impacted. Specific service impact depends on the infrastructure compromised.	Ensure service delivery.	Treatment	▪ Fingerprint access controls ▪ Security guards ▪ Use of municipal law enforcement to safeguard infrastructure. ▪ Fences and gates. ▪ Alarms ▪ Repairs and replacement of stolen / vandalised infrastructure.

Risk	Cause of risk	Critical Services Impacted	Reason for mitigation	Mitigation strategy	Mitigating actions
Loss of key personnel	▪ Shortage of qualified and skilled personnel. ▪ Small recruitment pool. ▪ Lack of funds to compete with private sector remuneration. ▪ No personnel available to take over from key personnel. ▪ Inadequate system of delegations in place. ▪ Key personnel go on leave. ▪ Social environment prevents key personnel from going to work. (E.g. protests, family matters, etc.) ▪ Key personnel unable to work due to drug and alcohol use.	All municipal services can be impacted. Specific service impact depends on the key personnel lost.	Ensure service delivery.	Treatment	▪ Scarce skills policy, including higher remuneration for the retention of personnel with scarce skills. ▪ Succession Planning and Career Pathing policy in place. ▪ Approved delegates of key personnel available. ▪ Directors on permanent employment contracts to ensure stability and retention. ▪ Substance abuse policy in place, which includes the assistance of employees addicted to drugs or alcohol.

14

11/25

Risk	Cause of risk	Critical Services Impacted	Reason for mitigation	Mitigation strategy	Mitigating actions
Disruptions in supply chain management	▪ Procurement legislation. ▪ Changes to procurement regulations by National Treasury. ▪ Lack of knowledge of procurement procedures among municipal employees. ▪ Lack of cooperation from municipal departments with the SCM department. ▪ Legal challenges by unsuccessful bidders. ▪ Non-performance by suppliers. ▪ Shortage of SCM personnel.	All municipal services.	Maintain a timely and effective supply chain.	Treatment	▪ SCM department divided into 3 main sections, each specialising in certain aspects of SCM. ▪ SCM policy available on the intranet for municipal employees. ▪ Emails sent to municipal employees to clarify and explain certain procurement procedures. ▪ 3 different bid committees to minimise the risk of bias decisions or errors, reducing the likelihood of unsuccessful bidders challenging the awards in court. ▪ Use of interns in SCM department. ▪ Supplier performance monitoring system in place. ▪ Training of SCM officials when regulations change.
Social conflict	▪ Inadequate policing ▪ Inadequate prosecution and sentencing. ▪ Politics ▪ Migration	All municipal services.	Protect municipal property and personnel required for service delivery.	Treatment	▪ Use of municipal law enforcement to police areas prone to social conflict. ▪ Cooperation with SAPS. ▪ Ward Committee system in place to enable communities to voice their grievances and influence municipal decision-making. ▪ Zero tolerance approach to damage to municipal property or attacks on municipal employees.

Risk	Cause of risk	Critical Services Impacted	Reason for mitigation	Mitigation strategy	Mitigating actions
Fires	▪ Lightning ▪ Concentrated reflection of sunlight onto dry surfaces. ▪ Arson ▪ Negligence	All municipal services can be impacted. Specific service impact depends on whether the fire impedes delivery of the service or damaged / destroyed the infrastructure/assets required to deliver the service.	Ensure service delivery is not affected by fires or can resume within the maximum allowable downtime.	Treatment Transfer	▪ Fire safety training ▪ Fire extinguishers ▪ Reliable and fast communication line with ODM Fire Department. ▪ Veld Fire Plan ▪ Fire and waterproof safes ▪ Safe storage of flammable materials. ▪ Use of fire retardant materials where possible. ▪ Insurance against fire damage. ▪ Real-time access to information from an efficient and timely fire forecasting and early warning system.
Floods	▪ Heavy rain ▪ Inadequate maintenance of storm water system. ▪ Burst water pipes.	All municipal services can be impacted. Specific service impact depends on whether the water impedes delivery of the service or damaged / destroyed the infrastructure/assets required to deliver the service.	Ensure service delivery is not affected by flooding or can resume within the maximum allowable downtime.	Treatment Transfer	▪ Waterproof safes ▪ Electric equipment stored on top of elevated platforms (e.g. desks). ▪ Critical equipment stored on 2nd floors of buildings. ▪ Maintenance of storm water systems. ▪ Replacement of deteriorating water pipes. ▪ Installation of water management systems that can identify leaks. ▪ Flood barriers ▪ Insurance against water and flood damage. ▪ Real-time access to information from an efficient and timely flood forecasting and early warning system.

Risk	Cause of risk	Critical Services Impacted	Reason for mitigation	Mitigation strategy	Mitigating actions
Tsunami	Earthquakes	All municipal services.	Ensure service delivery.	Treatment Transfer	▪ Establish a backup location high enough to avoid destruction by a tsunami. ▪ Construct critical infrastructure as high and far away from the coast as possible. ▪ Real-time access to information from an efficient and timely tsunami forecasting and early warning system. ▪ Insurance against tsunami damage. ▪ Scenario budgeting to plan the financial survivability of the Municipality when income from property rates significantly decline due to the destruction of high value properties along the coast.
Compromised employee health and safety.	▪ Viruses and bacteria. ▪ Unsafe work environments. ▪ Non-compliance with Occupational Health and Safety Act	All municipal services. Specific service impact depends on the employees affected by illness or injury.	Ensure service delivery.	Treatment	▪ Occupational Health and Safety function. ▪ Sister employed to help employees with health problems and injuries. ▪ OHS officers appointed from among municipal employees who are responsible for the occupational health and safety of certain departments or a building. ▪ Cleaners employed. ▪ 80 days sick leave, to encourage sick employees to stay away from work while they are sick. ▪ Medical aid contributions.

4.4. Event Response

Each risk event stemming from the risks identified in the BIA is addressed in the continuity plans contained in the BCP, in terms of the disruptions it causes to the Municipality's service delivery and business operations.

One risk event can be the cause of another risk event, for example a fire can destroy power lines, resulting in a lack of electricity supply.

Many risk events can also have the same impact, for example a flood, fire, protest action and vandalism can all result in damage to or destruction of assets.

Due to the abovementioned interrelatedness of risk events and risk event impacts, most of the continuity plans are designed for responses to a specific disruption impact, for example destruction of water pumps, and not for responses to the impacts of a specific risk event, for example water pumps destroyed by fire.

Cyber attacks and a tsunami are the only events covered on a risk event basis, due to the complexity of responses to cyber attacks and a tsunami's "black swan" status.

4.4.1. Lack of communication mediums

The continuity plans covers the loss of internet, GroupWise, telephone and cellular services.

The ICT department has the responsibility to ensure the internet, email and telephone services are available.

Other forms of communication, including cell phones, radios and satellite phones, are the responsibility of each department.

The lack of communication mediums are covered in the continuity plans as a universal risk event for all critical services and separately for ICT, where the ICT department's role and responsibilities regarding communication mediums are addressed.

4.4.2. Lack of electricity

A lack of electricity supply can either be caused by a lack of supply from Eskom, technical faults or external events affecting the distribution network.

See the continuity plans for responses to a lack of electricity supply.

4.4.3. Downtimes at water treatment plants

The main contributing factor to downtimes at water treatment plants is the ageing infrastructure. The response is adequate maintenance and replacement, which is an ongoing process and not covered by the BCP.

Natural and man-made events that cause downtimes are covered by the continuity plans.

4.4.4. Downtimes at water treatment plants

The main contributing factor to downtimes at water treatment plants is the ageing infrastructure. The response is adequate maintenance and replacement, which is an ongoing process and not covered by the BCP.

Natural and man-made events that cause downtimes are covered by the continuity plans.

4.4.5. Cyber attacks

It is the ICT department's responsibility to implement preventative measures and recover systems after a cyber attack occurs.

Other departments have the responsibility to ensure their use of ICT does not compromise the security of ICT systems.

Due to the complexity of the responses required to address cyber attacks, it is dealt with individually in the BCP.

4.4.6. Security of infrastructure

Security of infrastructure refers to unauthorised access, theft, vandalism and sabotage of municipal infrastructure. The resulting damage to or loss of infrastructure is covered by the continuity plans.

Detailed security plans for the protection of municipal infrastructure fall outside the scope of a BCP. It is the responsibility of municipal law enforcement and departmental managers to develop and implement security measures to ensure the security of infrastructure.

The South African Police Service (SAPS) has the responsibility to enforce the law, consisting of apprehending criminals and crime prevention, which should include the protection of municipal infrastructure from known criminals and planned attacks.

4.4.7. Loss of key personnel

Key personnel refer to personnel who if lost, will immediately or within a short time result in a critical service not being delivered.

Each critical service has its own key personnel and is covered in the continuity plans.

4.4.8. Disruptions in supply chain management

Disruptions in supply chain management refer to any delay in receiving, ordering of wrong quality and/or quantity and delivery of the wrong quality and/or quantity by suppliers of goods and/or services required by the Municipality to deliver critical services.

The main responsibility to ensure a disruption free supply chain lies with the supply chain management department. Other departments have the responsibility to ensure they relay their requirements for goods and/or services accurately and keep to the deadlines for submissions to prevent any delays.

Disruptions in supply chain management are covered as a universal risk event in the continuity plans.

4.4.9. Social conflict

Social conflict refers to a variety of violent and other illegal behaviour that impact on the Municipality's delivery of critical services.

This includes violent protests, gangsterism, vandalism and sabotage.

Social conflict can result in the damage or destruction of municipal assets, for example the stoning of municipal vehicles, or it can prevent critical services from being delivered, for example municipal employees are not allowed to enter certain areas or key personnel are unable to get to work. These disruptions are covered in the continuity plans.

Detailed plans for the prevention of and reaction to social conflict fall outside the scope of this BCP. It is the responsibility of the SAPS and municipal law enforcement to create plans to address social conflict.

4.4.10. Fires

Each department has the responsibility for basic fire prevention and firefighting measures, like fire extinguishers and not storing flammable materials near ignition sources.

The basic fire prevention and firefighting measures will be assessed by the Occupational Health and Safety inspector and/or an inspector from the Fire Department.

Detailed and complex fire prevention and firefighting plans and measures are the responsibility of the Fire Department and Disaster Management, which will form part of their fire plans and are beyond the scope of the BCP.

Evacuation plans are the responsibility of each department's/building's safety officer. Evacuation plans should already be displayed and known by every municipal official, thus it will not be included in the BCP.

In the continuity plans, the disruptions caused by fires are dealt with as part of general groupings of disruptions (e.g. damage to / destruction of infrastructure) and individually (e.g. inaccessible roads due to fires).

4.4.11. Floods

Detailed and complex flood mitigation plans are the responsibility of Disaster Management and beyond the scope of the BCP.

In the continuity plans, the disruptions caused by floods are dealt with as part of general groupings of disruptions (e.g. damage to / destruction of infrastructure) and individually (e.g. flooding of sewerage system).

4.4.12. Tsunami

A tsunami is a "black swan" event, highly unlikely to occur, but it will have catastrophic consequences. A tsunami will impact all critical services at once and besides the direct impacts, will also have material indirect impacts on the Municipality's ability to deliver critical services, for example the decline in income from property rates due to the destruction of high wealth property along the coast.

Due to the catastrophic, wide-reaching and all-inclusive impact of a tsunami, it is dealt with individually in the BCP.

4.4.13. Compromised employee health and safety

Compromised employee health and safety risks consist of anything that can cause harm or illness to municipal employees.

Harm can result from an unsafe work environment or inadequate protection gear. Illness can be caused by viruses and bacteria, contracted at the workplace or elsewhere.

Detailed plans for a safe and healthy work environment are the responsibility of managers and the Occupational Health and Safety officer and beyond the scope of the BCP.

In terms of business continuity, injured and sick employees can result in a loss of key personnel, which is covered in the continuity plans.

Unsafe work environments can result in a shutdown of the premises.

4.5. Business Continuity Teams

Proper response to a disruption for the Municipality requires teams to lead and support business continuity operations. Team members should be selected from trained and experienced personnel who are knowledgeable about their responsibilities.

The duties and responsibilities for each team must be defined, including the team members and authority structure, the specific team tasks, members' roles and responsibilities, creation of contact lists and identifying alternate members.

The business continuity teams consist of the following:

1) Management Emergency Team

2) Response & Recovery Co-ordinator

3) Business Continuity Teams

- Technical / Community Services Team

- Water
- Electricity
- Sewerage
- Solid Waste
- Roads
- Storm Water Systems

- Finance Team

- Information and Communication Technology Team

- Communication Team

- Occupational Health and Safety Team

- Disaster Management Team

- Fire & Rescue
- Disaster Management
- Traffic
- Law Enforcement

4.5.1. Management Emergency Team (MET)

The MET is responsible for overall coordination of the business continuity effort, determining whether the BCP should be activated and communications with senior management.

The MET's other responsibilities include:

- Evaluate which BCP actions should be invoked and activate the corresponding teams.
- Evaluate and assess damage assessment findings.
- Set restoration priority based on the damage assessment reports.
- Provide senior management with ongoing status information.
- Act as a communication channel to teams and major stakeholders.
- Work with suppliers and business continuity teams to develop a rebuild/repair schedule.

4.5.2. Response & Recovery Co-ordinator

The Response & Recovery Co-ordinator is responsible for the overall coordination of the recovery effort, establishment of the command centre and communications with the MET.

The Response & Recovery Co-ordinator's other responsibilities include:

- Notify the business continuity teams.
- Gather damage assessment information and report it to MET.
- Determine recovery needs.
- Establish command centre and related operations.
- Notify all Team Leaders and advise them to activate their plan(s) if applicable, based upon the disruption situation.
- If the BCP is not activated, take appropriate action to return to normal operation using regular staff.
- Determine whether suppliers or other teams are needed to assist with detailed damage assessments.
- Prepare post-disruption debriefing report.

4.5.3. Technical / Community Services Team

The Technical / Community Services Team is responsible for the response and recovery of services delivered to the community. The services are interdependent on one another to a certain extent and therefore a combined team will be best suited to restore the services as soon as possible.

The responsibilities of the Technical / Community Services team include the following:

1) Water

- Repair / Reconstruction of water infrastructure;
- Monitor water levels of reservoirs and coordinate refilling of reservoirs that are empty or nearly empty;
- Dispatch and coordinate water tankers to residents who are or will be without water for more than 24 hours;
- Ensure maintenance of water infrastructure;
- Ensure the fleet of water service vehicles are maintained;
- Review the controls in place to protect water infrastructure against vandalism and theft and ensure improvements are implemented where necessary;
- Ensure a fast and effective reporting mechanism for burst or leaking water pipes exist;
- Monitor water levels of dams and boreholes supplying Overstrand Municipality;
- Identify possible borehole sites for establishing boreholes during a water crisis;
- Identify key personnel in the water department and ensure continuity plans address key personnel adequately;
- Inform the Communication team about the timeframes for the restoration of water supply and the timetables of water tankers.

2) Electricity

- Repair / Reconstruction of electricity infrastructure;
- Review the controls in place to protect electricity infrastructure against vandalism and theft and ensure improvements are implemented where necessary;
- Ensure maintenance of electricity infrastructure;
- Ensure maintenance of electricity generators;
- Maintain a 7 day fuel supply for electricity generators;
- Procure electricity generators for infrastructure identified in the BCP;
- Dispatch and coordinate mobile electricity generators to infrastructure;
- Explore possible alternative electricity suppliers and self-generation;
- Inform the Communication Team about the timeframes for the restoration of electricity supply.

3) Sewerage

- Repair / Reconstruction of sewerage infrastructure;
- Ensure maintenance of sewerage infrastructure;
- Review the controls in place to protect sewerage infrastructure against vandalism and theft and ensure improvements are implemented where necessary;
- Monitoring of sewerage levels;
- Dispatch and coordinate sewerage tankers to drain areas that will spill;
- Clean-up of sewerage spills;
- Ensure a fast and effective reporting mechanism for burst or leaking sewerage pipes exist.

4) Solid Waste

- Ensure maintenance of fleet;
- Identify alternative routes and collection spots when usual routes are inaccessible;
- Create new collection schedules to suit the circumstances;
- Inform the Communication Team about alternative collection spots and adjusted collection schedules.

5) Roads

- Repair / Reconstruction of roads;
- Ensure maintenance of roads;
- Ensure an effective reporting mechanism for damaged roads exist;
- Monitor bitumen supply to proactively manage possible shortages.

6) Storm Water

- Repair / Reconstruction of storm water systems;
- Ensure maintenance of storm water systems;
- Ensure a fast and effective reporting mechanism for blocked or damaged storm water systems exist.

4.5.4. Finance Team

The Finance Team is responsible for recovery of the finance function and supporting business continuity.

The Finance Team's responsibilities regarding recovery of the finance function include:

- Ensure municipal employees are paid no later than 2 days after their payment date stipulated in their employment contracts;
- Ensure suppliers are paid no later than 2 days after the due date;
- Liaise with SARS if taxes and/or levies will not be paid over on time and arrange for extension of the payment date;
- Implement controls to prevent fraudulent transactions during downtime;
- Recovery of financial data and information in cooperation with the ICT Team;
- Ensure financial transactions are recorded in an appropriate and standardised system while the mSCOA portal is inaccessible.

The Finance Team's responsibilities regarding business continuity of the Municipality include:

- Help departments and directorates establish the necessary emergency procurement procedures in advance;
- Handle requests for emergency procurement;
- Perform cost-benefit analysis and probability calculations to determine which insurable events identified in the BIA should be covered by insurance;
- Continuously monitor the BIA and insurance policy to ensure adequate coverage;
- Calculate the costs mentioned in the BIA.

4.5.5. Information and Communication Technology Team (ICT Team)

The ICT Team is essential to the business continuity and recovery efforts. Their responsibilities' include:

- Backup of all important electronic data;
- Safekeeping of backups;
- Restore data after a disruption;
- Ensure the security of the Municipality's network against cyber intrusions and attacks;
- Restoration of network capabilities;
- Recover email system and functionality;
- Restore telephone functionality;
- Restoration of internet connectivity;
- Equip alternative sites with the necessary ICT infrastructure.

4.5.6. Communication Team

The Communication Team is responsible for communication to the Municipality's stakeholders the effects of the disruption on the Municipality's operations, the current recovery operations in progress, additional planned recovery operations, the estimated time before services are resumed at minimum levels and the estimated time before normal operations are resumed.

The Communication Team's responsibilities include:

- Communicating to employees if there wages/salaries will not be paid on time and the estimated pay date;
- Communicating to suppliers if they will not be paid on time and the estimated pay date;
- Informing the public when service delivery will be resumed;
- Media relations, including handling all media queries, forwarding questions to the appropriate municipal officials, reviewing answers to media questions from municipal officials before sending it, releasing continuous updates on the state and progress of recovery efforts and communicating information from other response and recovery teams to the public.

4.5.7. Occupational Health & Safety Team (OHS Team)

The OHS Team is responsible to oversee the safety of all municipal employees while they are performing municipal work and/or while they are at municipal premises.

The OHS Team's responsibilities for business continuity include:

- Inspect damaged buildings, vehicles and equipment for contraventions of the Occupational Health and Safety Act, Act 85 of 1993 (OHS Act), and unsafe conditions;
- Declare whether repaired buildings, vehicles and equipment are safe and meet the requirements of the OHS Act before municipal personnel move back in;
- Ensure alternative premises fulfil the requirements of the OHS Act;
- Ensure complete medical records are kept of all personnel and that backup copies are made of medical records;

- Assist municipal departments to create safe working environments and fulfil all requirements of the OHS Act.

4.5.8. Disaster Management Team

The Disaster Management Team's role is to prevent disasters from occurring where possible, decrease the likelihood and impact of unpreventable disasters and managing the fallout of disasters to enable the other business continuity teams to focus on returning the Municipality's operations to normal.

The Disaster Management Team's responsibilities for business continuity include:

1) Fire & Rescue

- Extinguish fires on municipal property;
- Evacuate municipal employees from burning or flooded buildings;
- Assist municipal departments to acquire adequate firefighting equipment and reduce fire risks;
- Salvage data, records and equipment from buildings, if it is safe to do so.

2) Disaster Management

- Perform disaster risk assessments on potential disasters, determining its potential impact and likelihood on the Municipality's services;
- Inform the BCP Committee of changes in the risk profile of disasters, to enable them to evaluate whether the business continuity plan addresses all relevant disaster scenarios;
- Assist departments with the creation of mitigation strategies for disasters;
- Ensure disaster relief funds received specifically for components of the business continuity plan, are allocated to the specific components;
- Include business continuity funding requirements in applications for disaster relief funds;
- Warn the MET of approaching fires that could disrupt the operations of the Municipality and advise them on steps to take to prevent or mitigate a disaster;
- Warn the MET of impending or current flooding that could disrupt the operations of the Municipality and advise them on steps to take to prevent or mitigate a disaster;
- Warn the MET of any other known approaching event that can have disastrous consequences and advise them on steps to take to prevent or mitigate a disaster.

3) Traffic

- Regulate traffic to enable municipal service vehicles to get to their destinations to deliver or restore services;
- Regulate traffic to enable municipal officials to get to work at the main sites or at alternative sites;
- Regulate traffic to enable suppliers or couriers to deliver equipment and materials required to restore services.

4) Law Enforcement

- Protect the Top Management Team;
- Assist the SAPS with crowd control;

24/25

- Protect municipal property and municipal officials' property on site;
- Act against people and businesses who dump waste in the storm water system;
- Act against people and businesses who dump waste in the sewerage system;
- Assist municipal departments with acquiring and/or implementing adequate security measures.

4.5.9. General team member responsibilities

- Each team member must designate a team alternate backup.
- All team members must keep an updated calling list of their team members' work, home and cell phone numbers.
- All team members must keep the BCP for reference at home in case the disruption happens after normal work hours.
- All team members must familiarise themselves with the contents of the BCP.

4.6. Alternative Sites

Alternative sites must be identified where municipal services can be delivered from in case the primary sites are unavailable.

4.6.1. Identify the amount of alternative sites

Each function, department, directorate, the whole municipality or a combination of the aforementioned can have an alternative site.

The amount of alternative sites will be determined by cost and practicality considerations.

Functions, departments and directorates whose operations overlap can share an alternative site. Functions or departments that have unique operations can have their own alternative sites.

To keep capital costs to a minimum, one alternative site for the whole municipality can be used.

4.6.2. Location of alternative sites

Alternative sites should be situated in areas where it will not simultaneously be affected by the same disruption as the primary site.

The location must also be accessible by municipal officials during disruptions.

For example, if the primary site is in a low lying area prone to flooding and surrounded by veld that can burn, the alternative site should be on top of a barren hill to prevent floodwater and fires from reaching it, but it must also be accessible by a road that cannot be flooded or surrounded by veld fire.

4.6.3. Requirements of alternative sites

The requirements of alternative sites will differ, depending on the function, department or directorate operating from the alternative site. The assets and materials at the alternative site must enable the function, department, directorate or municipality to resume critical services and start the process to return to normal operations.

The minimum requirements of alternative sites are the following:

- Access control to ensure the physical security of the site and staff.
- Backup electricity supply that can support the operations at the site for a one week period.
- Office furniture and supplies, including:
  - Desks
  - Chairs
  - One week's supply of stationary.
  - One week's supply of printing paper.
  - One week's supply of printing ink.
- Information communication technology infrastructure, including:
  - Power points
  - Network points
  - Wi-Fi
  - Network hub and network infrastructure
  - Landlines (telephone/facsimile)
  - ISDN lines
  - ADSL lines
  - Satellite communications
  - Radios
  - Computers
  - Computer Screens
  - Printers
  - Projectors
- Conference facilities, including conference calls and webcams
- One week's supply of portable water stored on site.
- Ablution facilities
- Sewerage storage for a period of one week.
- Refuse storage capacity for one week's accumulation.
- One week's supply of food stored on site.
- Kitchen
- Lounge/Relaxation area

Annexure B 1/3

OFFICE OF THE DIRECTOR: MANAGEMENT SERVICES
RELEVANT DEPARTMENT: RISK MANAGEMENT
SHARED SERVICES

NAVRAE | ENQUIRIES: Ashwille Riddles

DATE | DATUM: 26 May 2017

TO: OVERSTRAND MUNICIPAL COUNCIL

SUBJECT MATTER: RELATIONSHIP BETWEEN BUSINESS CONTINUITY AND DISASTER MANAGEMENT

1. Introduction

Anticipating the worth and planning how to manage it is the backbone of business continuity. It requires both time and resources that may be difficult to justify in the moment, but much like the value of paying fire insurance premiums, its value is very much appreciated after a fire.

However, municipalities must also recognise that where there is risk, there is also opportunity. Therefore municipalities should also focus on business improvement. Organisational resilience reaches beyond risk management towards a more holistic view of business health and success. In today's dynamic, interconnected world, the ability of a municipality to anticipate, prepare for, respond to and adapt and change – and crucially to prosper from it – is more important than ever.

2. What is the purpose of a business continuity plan?

The purpose of a business continuity plan is to prepare the Municipality in the event of extended service outages caused by factors beyond our control (e.g. natural disasters, man-made events) and to restore services to the widest extent possible in a minimum time frame.

Instead of focusing on resuming a business after critical operations have ceased, or recovering after a disaster, a business continuity plan endeavours to ensure that critical operations continue to be available.

3. What is the purpose of a disaster management plan?

The purpose of the disaster management plan is to establish a disaster management strategy, guiding the disaster managing plans of the various departments and role players.

It outlines procedures for both the pro-active disaster prevention and the reactive disaster response and mitigation phases of Disaster Management.

4. Difference between business continuity operations and disaster management operations

The business continuity plans and teams only focus on the municipality's personnel, systems and infrastructure in the event of a disaster. Business continuity plans also cover disruptions caused by incidents that are not classified as "disasters" in terms of the Disaster Management Act.

The disaster management unit focusses on all people and structures in the Overstrand area. Its response is mostly limited to events classified as a disaster in terms of the Disaster Management Act.

In short, business continuity has a very narrow and more specific focus. The business continuity plan is a detailed document that outlines the recovery of operations that relates to personnel, systems and infrastructure of the Municipality only.

Tel: 028 425 1157 | Cell: 082 739 0365 | E-mail: ariddles@odm.org.za
PO Box 20 | **HERMANUS** 7200
www.overstrand.gov.za

OFFICE OF THE DIRECTOR: MANAGEMENT SERVICES
RELEVANT DEPARTMENT: RISK MANAGEMENT SHARED SERVICES

NAVRAE | ENQUIRIES: Ashwille Riddles

Munisipaliteit • U-Masipala • Municipality
OVERSTRAND

The table below summarises the differences in focus.

Disaster Management	Business Continuity
Disasters	Disruptions
All people in the Overstrand municipal area.	Municipal officials required to deliver critical services.
All property in the Overstrand municipal area.	Municipal property required to deliver critical services.
Compliance with the Disaster Management Act and regulations.	Restore critical services to comply with legal mandates regarding service delivery.
Save lives and property.	Restore critical services.

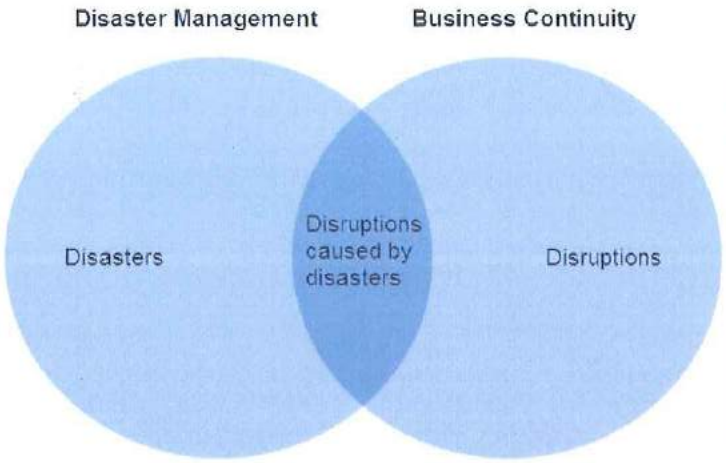
5. Synergies between business continuity and disaster management

The objectives and activities of disaster management and business continuity will sometimes coincide.

For example, during a disaster, the disaster management unit will focus on saving lives and property, which will include municipal officials and municipal property, residents and businesses; the business continuity teams will also focus on saving municipal officials and municipal property required for the delivery of critical services.

The business continuity framework has been developed with the disaster management policy and plan in mind to prevent contradictions between the documents. The business continuity framework supplements or incorporates aspects such as recovery protocols and evacuation procedures pertaining only to the municipality that is also included in the disaster management policy and/or plan.

The disaster management unit has also been included in the disaster management team in the business continuity plan. There functions related to business continuity are closely related to their functions for disaster management in general, for example warning the municipality of forecasted flooding and advising on flood mitigation plans.



Tel: 028 425 1157 | Cell: 082 739 0365 | E-mail: ariddles@odm.org.za
PO Box 20 | **HERMANUS** 7200
www.overstrand.gov.za

OFFICE OF THE DIRECTOR: MANAGEMENT SERVICES
RELEVANT DEPARTMENT: RISK MANAGEMENT SHARED SERVICES

NAVRAE | ENQUIRIES: Ashwille Riddles

Munisipaliteit • U-Masipala • Municipality
OVERSTRAND

6. The need for a business continuity framework

The purpose of a business continuity plan is to restore services to the widest extent possible in a minimum time frame.

The business continuity framework covers only the critical services of the municipality, with specific business continuity plans and governance structures to ensure continuous service delivery or rapid restoration.

7. Closing remarks

The disaster management plan does not include any specific provisions to restore the critical services of the municipality. The disaster management policy, section 10.4 states "*Departments who are responsible for the maintenance of specific infrastructure are responsible for the repair or replacement of such infrastructure after disasters.*" This is exactly what the business continuity plan address, among other things.

In many instances, the disaster management unit will not drive work streams of business continuity teams. As an example, remember the disruptions at the end of March when the power of the server room was switched off. It was contingency plans of ICT and Finance that restored the services within a few days. The disaster management unit was not involved.

Tel: 028 425 1157 | Cell: 082 739 0365 | E-mail: ariddles@odm.org.za
PO Box 20 | **HERMANUS** 7200
www.overstrand.gov.za