BUSINESS CONTINUITY MANAGEMENT POLICY

Title:	Business Continuity Management Policy
Custodian:	Pension Funds Adjudicator
Prepared By:	Risk and Compliance Officer
Date Created:	October 2021
Version No:	3
Reference No.	011
Date Approved:	26 March 2024
Effective Date:	Date of approval by Accounting Authority
Approved By:	Accounting Authority

Document Approval Page

Document owner:

NAME	POSITION	SIGNATURE	DATE
Lutendo Tshifularo	Risk and Compliance Officer		

Document recommended by:

COMMITTEE	Chairperson	SIGNATURE	DATE
Management Committee	Bulelani Makunga Acting Chairperson		
Risk Committee	Prof Tania Ajam Chairperson		

Document Approval:

COMMITTEE	Chairperson	SIGNATURE	DATE
Accounting Authority	Muvhango Lukhaimane Pension Funds Adjudicator		

Mandatory Review period:

To be reviewed every second year or when significant changes occur

Version Control Page

This page should provide a history of previous versions of the policy and changes made:

Version	Date	Author	Status	Comment / changes
3.0	October 2021	Ayanda Twaku	Reviewed	All pages reviewed
4.0	December 2023	Lutendo Tshifularo	Reviewed	Reviewed to align with the changes in the founding legislation.

Table of Contents

Contents

1. INTRODUCTION

The Office of the Pension Funds Adjudicator (OPFA) is committed to protecting and safeguarding its personnel, organisational assets, information, reputation and stakeholder value.

Business Continuity is the strategic and tactical capability of the OPFA to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable level, as defined in the Business Impact Analysis (BIA). Business Continuity Management (BCM) is focused on planning for unexpected events that can affect critical business infrastructure and processes. The Business Continuity Management program is designed to ensure that the long term viability of the OPFA is maintained in the event of an interruption to essential business operations and will provide for the recovery of the critical business processes and supporting information technology systems within a specified timeframe and in terms of the provisions of this policy as outlined hereunder.

2. PURPOSE

The purpose of this policy is to formalise Business Continuity Management programme for the OPFA and to provide guidelines for developing, maintaining and testing Business Continuity Plans (BCPs).

This policy establishes the basic principles and framework necessary to ensure emergency response, recovery, restoration and resumption of the OPFA operations and business activities in the event of business interruption.

3. SCOPE AND APPLICATION

This policy applies to all OPFA permanent employees, contract employees, temporary workers, facilities, services, processes, operations and IT systems.

The OPFA shall be prepared for scenarios including, but not limited to, natural disasters, power outages, systems and telecommunications failures, loss of data or data corruption, loss of premises, equipment, technology, key employees, critical suppliers, chemical and biological hazards, health outbreaks and the OPFA building not being accessible.

4. STATUTORY AND OTHER REQUIREMENTS

The Disaster Management Act (No 57 of 2002)

King IV on Corporate Governance

The Business Continuity Institute Good Practice Guidelines 2018

ISO 22301 (2012) Societal Security- Business Continuity Management Systems

ISO 22313 (2012) Societal Security- Business Continuity Management Systems Guidance

5. RISK MANAGEMENT, EMERGENCY RESPONSE, BUSINESS CONTINUITY RESPONSE AND RECOVERY RESPONSE

There is a close relationship between BCM, risk management and emergency response. This aligns with the comprehensive approach that focuses upon the four pillars of emergency management; prevention, preparedness, response and recovery (see figure 1).

a. Risk management.

Risk management is the practice of dealing with uncertainty and its effect on an organisation. Risk management incorporates a systematic approach to identifying, assessing and responding to risks, and interfaces with the principle of ‘prevention’. BCM can be utilised as a control for business disruption related risks.

b. Emergency response

Emergency response is the initial reaction to an incident or disruption, which aims to protect people and property from immediate harm. This may include the mobilisation of the Incident management team and activation of business continuity management plans.

c. Business continuity response

Business continuity response refers to the actions taken to ensure that the OPFA is able to resume and continue delivering critical business functions in a timely manner following a disruption. Depending upon the nature of the incident, the continuity response may last from hours to weeks. The business continuity response interconnects the period from where normal work practices are suspended to when recovery is affected. As a result, the continuity response bridges the principles of 'response' and 'recovery'.

d. Recovery

Recovery is the process of restoring normal work practices within the organisation. This may include re-establishing suspended activities, clearing of backlogs and repairing damaged infrastructure. Depending upon the nature of the disruption, the recovery response may take weeks to months.

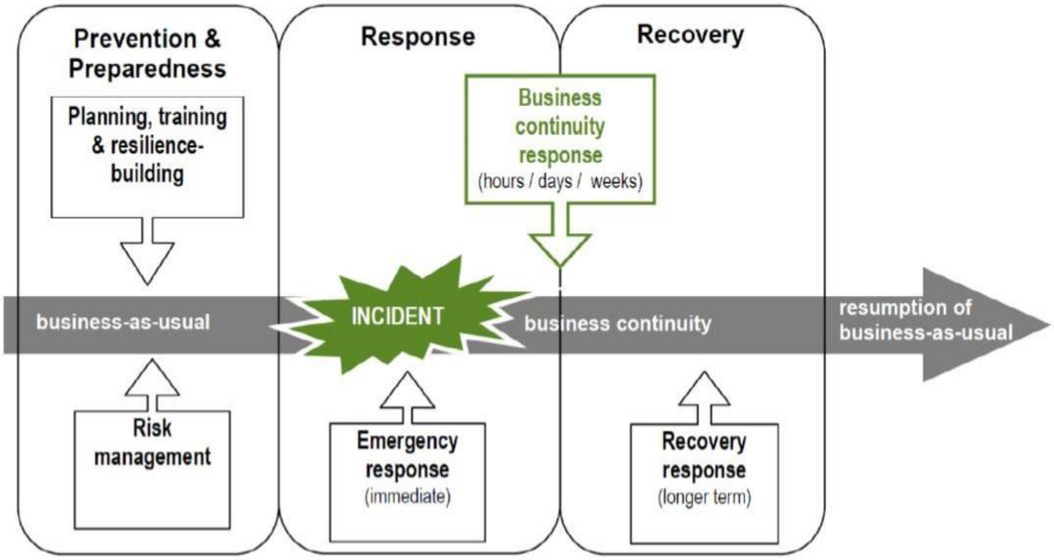
Prevention & Preparedness
Response
Recovery
Planning, training & resilience-building
Business continuity response (hours / days / weeks)
business-as-usual
INCIDENT
business continuity
resumption of business-as-usual
Risk management
Emergency response (immediate)
Recovery response (longer term)

Figure 1

6. ROLES AND RESPONSIBILITIES

6.1 Pension Funds Adjudicator (PFA)

The Pension Funds Adjudicator, as head of the OPFA, is responsible to the Accounting Authority and the stakeholders for the efficient running of the business and therefore, is responsible to ensure the OPFA will recover from a disruptive event.

6.2 IT Senior Manager

The IT Senior Manager shall -

- Ensure regular tests of the Disaster Recovery Plan;
- Ensure the application of the recommendations contained in King IV on sound ICT governance in relation to BCM.

The IT Senior Manager is also responsible for ensuring that:

- The ICT disaster recovery management programme is implemented according to business recovery requirements.
- ICT security risks that could be exploited and lead to business disruptions are addressed in the DR program (DRP).
- All the DRP test issues identified are addressed within reasonable time and implement optimisation of the DRP as per changing business architecture and technology landscape.

6.3 Spokesperson

The Spokesperson is responsible for the development and implementation of all internal and external communication to stakeholders, media, staff, next of kin, suppliers, service providers and customers regarding the details and impact of a business disruption. The spokesperson of the OPFA is the PFA or any other official delegated by the PFA.

6.4 Risk Management

The Risk and Compliance Officer is responsible for oversight and risk management advisory activities of the BCM program, including risk assessment, business impact analysis, as well as overall BCM program management integration into the enterprise risk management program.

6.5 Business Continuity Management (BCM) Manager

- The Risk and Compliance Officer is the BCM Manager and is responsible for the overall management of enterprise-wide Business Continuity Management Programme in line with the signed appointment letter.
- The BCM Manager shall ensure that BCM awareness is increased, and that all risk mitigation controls, plans and solutions are exercised on at least once annually.
- The BCM Manager is responsible for reporting the status and effectiveness of the BCM programme to MANCO.

6.6 Management and/or Team Leaders

Management (MANCO) and/or Supervisors are responsible for:

- Updating and implementing the BCM in their respective departments.
- The annual review of business unit Business Continuity Plans.

- The annual testing of business unit Business Continuity Plans.
- Involvement of all business unit employees in BCM.
- Managing, implementing and executing BCP responsibilities in line with the BCP appointment letter(s) for BCM Business Unit Champion and Deputy Champion.

6.7 Strategic Incident Management Team /Crisis Management Team

The Strategic Incident Management Team (SIMT) also known as Crisis Management Team (CMT) is responsible for disaster management in the event of a disaster up to a point when order is restored. It constitutes the central decision-making unit during a BCM invocation.

In the event of any incident causing an operational disruption, the SIMT will be responsible for the following actions:

- Declaring a disaster and invoking the Business Continuity Plans (BCPs);
- Project managing the response and recovery efforts until resumption of normal business operations;
- Ensuring the recovery of business functions within the set recovery time objectives;
- Updating the Accounting Authority on the progress of all recovery actions and processes.

The SIMT consists of the following roles and associated responsibilities:

Pension Funds Adjudicator (PFA):

- Overall accountability for the continuity of the OPFA rests with the PFA, who is the BCM Team Leader.

BCM Team Leader:

- Accountable for ensuring the recovery and resumption of the OPFA operations in the event of an incident;
- Appoint the BCM Tactical Team;
- Appoint/approve appointment of the BCM Manager;
- Appoint/approve appointment of the business unit BCM Champions;
- Define the BCM scope;
- Prepare and obtain approval of the BCM budget;
- Monitor the performance of the BCM Programme;

- Promote BCM within the OPFA;
- In the event of an incident: Manage the recovery process.

Strategic Incident Management Team Members:

- Promote BCM within their areas of responsibilities in the OPFA;
- Support the implementation of the BCM Programme within their areas of responsibilities in the OPFA;
- Monitor the performance of the BCM Programme within their areas of responsibilities in the OPFA;
- In the event of an incident: Participate in the management of the recovery process.

6.8 Employees

The responsibilities of employees for BCM at the OPFA are as follows:

- All employees are responsible for contributing to the BCM programme with appropriate guidance, as well as assisting with response and recovery actions following a crisis, emergency or disaster event.
- Employee job descriptions and performance agreements should adequately reflect the nature and extent of key BCM roles and responsibilities**.**

7. POLICY APPLICATION

7.1 Business Impact Analysis (BIA) and Risk Assessment

For business-critical processes, the impact of a complete or partial failure of the corresponding resources is assessed by means of an impact analysis.

This assessment also considers mutual interdependencies between business departments and dependencies in connection with external providers (outsourcing).

The BIA is intended to indicate:

- the desired extent to which business-critical processes are to be recovered.
- the maximum period until the recovery of business-critical processes.
- the minimum scope of (replacement) resources (buildings, staff, IT infrastructure and systems, data, external providers).

The Risk and Compliance Officer and IT Senior Manager shall annually update the BIA to identify and prioritise the critical business processes. The OPFA BIA shall cover the major business processes that cut across respective departments. It shall identify the business process availability Recovery Time Objectives (RTOs) and business process Recovery Point Objectives (RPOs).

7.2 OPFA Business Continuity Solutions/Strategy(ies)

The BCM Solution document shall focus on the high-level strategies that the OPFA will adopt in ensuring the continuation of its value-creating processes in the aftermath of a major business interruption event.

The central intent of the OPFA's BCM Strategy is to provide an appropriate level of resilience and response measures aimed at:

- ensuring the continuity of the critical processes through which services are delivered, before the OPFA's survival is threatened by their loss; and
- limiting the period and impact of an operational disruption.

7.3 Business Continuity Plans (BCPs)

All business units shall develop and annually update BCPs that are business unit specific.

During a business interruption event, the Strategic Incident Management (SIMT) shall activate the alternative site if required. The SIMT shall work with the affected business units to ensure smooth execution of the institutional and department/unit specific BCPs requiring activation of the alternate site.

In some cases, it may not be necessary to relocate employees to the alternate site.

7.4 Business Continuity Plan and DR Testing

Business Continuity tests shall test and review the implementation of the respectivebusiness unit Business Continuity Plans and the capability of the crisis management organisation.

The OPFA's BCP shall be tested annually to ensure credible recovery preparedness. Business Unit BCPs shall also be tested at least annually. The respective Managers andthe Risk and Compliance Officer shall work together to perform these business unit specific tests.

Testing shall include familiarising team members with plan invocation and response, plan components and associated procedures.

7.5 Disaster Recovery

The Disaster Recovery strategies and plan will be aligned to the overall business continuity recovery requirements and timeframes. The organisation's Recovery Time Objectives and Recovery Point Objectives will be used to determine the system recovery order.

7.6 Training

All OPFA employees must be made aware of the BCM Programme. The Risk and Compliance Officer and OPFA staff must be trained about their business resumption and recovery roles.

7.7 BCP Maintenance

The OPFA and respective business unit-specific BCPs shall be updated annually. Additional to this, all departments shall update their BCPs as often as changes require, with notification of changes to the BCM Manager.

Reporting business continuity planning status and progress is a key element of creating an effective BC program in the OPFA. The BCM Manager shall report the status and progress of the BC program to MANCO on an annual basis or after every BCM test.

7.8 Communication

External communication during time of crisis, disruptive event or a disaster is a critical business process. The Spokesperson shall develop the communication plan, processes and messages that will be communicated to the press, suppliers, service providers, customers, next of kin and to employees in the event of an OPFA or business unit-specific business interruption.

7.9 Audit

Ongoing validation of BCM will be subjected to the scrutiny of external and internal auditors, to ensure that organizational resilience is continually improved.

7.10 Budget

Management will ensure the provision of a formal budget to fund the resource requirements for an effective and well maintained BCM programme.

8. BUSINESS CONTINUITY AWARENESS

The BCM Manager shall implement a Business Continuity Awareness Programme for all OPFA employees.

9. POLICY COMPLIANCE

The success of Business Continuity Management relies on the collective ownership of the BCPs and BCM processes by all OPFA employees.

10. EFFECTIVE DATE

This policy is effective from the date of approval by the Accounting Authority and shall replace all previous policies that were in force prior to the commencement of this policy.

11. IMPLEMENTATION OF POLICY

The responsibility for implementation of this policy rests with the Risk and Compliance Officer.

12. REVIEW AND UPDATE PROCESS

The Risk and Compliance Officer must ensure that this policy and its associated directives/procedures is reviewed and updated every 2 years. Amendments shall be made to the policy and directives as the need arise.

13. BCM DEFINITIONS, TERMS AND ACRONYMS

Glossary of terms		
Term	**Acronym**	**Description**
Business Continuity	BC	The capability of the organisation to continue delivery of products or services at acceptable pre-defined levels following disruptive incident.
Business Continuity Management	BCM	A holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interest of its key stakeholders, reputation, brand and value-creating activities.
Business Continuity Management Programme		The ongoing management and governance process supported by Top Management and appropriately resourced to implement and maintain business continuity management.
Management		Person or group of people who directs and controls an organisation at the highest level
Business Continuity Plan	BCP	Documented procedures that guide organisations to respond, recover, resume and restore to pre-defined level of operation following a disruption.
Business Impact Analysis	BIA	Management level analysis by which the OPFA assesses the quantitative (financial) and qualitative (non-financial) impacts, effects and losses that might result if the organisation were to suffer an emergency, incident or disaster. The findings from the BIA are used to make decisions concerning business continuity management strategies and solutions.
Business Resumption		Temporary solutions for business processes used in order to resume business activities. This can be applied on a step-by-step basis until ordinary business activities or full business capacity is recovered.
Strategic Incident Management Team/Crisis Management Team	SIMT/CMT	The team responsible for disaster management in the event of a disaster upto the point when order is restored.
Disaster		An unforeseen event that renders critical business processes unavailablefor a period of time that is unacceptable.
Disaster Recovery	DR	The strategies and plans for recovering and restoring the FSCA's technological infrastructure and capabilities after a serious interruption.
Disruptive Event		An event that interrupts normal business, functions, operations, or processes, whether anticipated (e.g., severe weather or political unrest) orunanticipated (e.g., power outages, technology failure or fire).
Incident Management		The methodology used by the organisation to mitigate the impact of a disruption in progress.
ICT Disaster Recovery		ICT DR means the ability of the ICT elements of an organisation to support its critical business functions to acceptable levels within a pre-determined period of time following a disruption.

Risk Management		Means the Coordination of activities to direct and control an organisationwith regards to risk.
Risk Assessment		The overall process of risk identification, analysis and evaluation.
Threat		Potential cause of unwanted incident, which can result in harm to individuals, a system or organisation.
Threat Analysis		The process of evaluating threats to identify unacceptable concentrations ofrisk to activities and single points of failure.
Recovery Time Objective	RTO	The period of time within which systems, applications, or functions must be recovered after an outage (e.g. one business day). RTOs are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation.
Recovery Point Objective	RPO	The point in time to which systems and data must be recovered after an outage (e.g. end of previous days processing). RPOs are often used as the basis for the development of back-up strategies, and as a determinant of the amount of data that may need to be recreated after thesystems or functions have been recovered.
Policy and Programme Management	PP1	The first stage of the BCM Lifecycle. It a professional Practice that defines the organisation policy relating to Business Continuity and how that policy will be implemented, controlled and validated through BCM programme.
Alert and Invocation		**Alert –** A formal notification that an emergency that an emergency, incident and/or crisis has occurred which may develop into Business Continuity Management or Crisis Management invocation/activation. **Invocation** – The act of declaring that an organisation's business continuity arrangements need to be put into effect in order to continue delivery of key products and services.
Organisation	OR	The ability for an organisation to absorb and adapt in changing environment.