



# Business Continuity Management

Implementation date: August 2015

## Table of Contents

<b>STANDARD POLICY SECTIONS .....</b>	<b>3</b>
<b>1. INTRODUCTION.....</b>	<b>3</b>
<b>2. PURPOSE.....</b>	<b>4</b>
<b>3. SCOPE .....</b>	<b>4</b>
POLICY OBJECTIVES.....	4
BCM PROGRAMME OBJECTIVES.....	4
ALIGNMENT TO INTERNATIONAL STANDARDS .....	5
<b>4. POLICY STATEMENTS.....</b>	<b>6</b>
4.1. STATEMENT 1: BUSINESS CONTINUITY MANAGEMENT POLICY.....	6
4.2. STATEMENT 2: BUSINESS IMPACT ANALYSIS (BIA) .....	6
4.3. STATEMENT 3: THREAT ASSESSMENT (TA) .....	6
4.4. STATEMENT 4: BUSINESS CONTINUITY STRATEGIES/SOLUTIONS.....	6
4.5. STATEMENT 5: BUSINESS CONTINUITY PLANS.....	6
4.6. STATEMENT 6: INCIDENT MANAGEMENT.....	6
4.7. STATEMENT 7: BCM TESTING AND EXERCISING.....	6
4.8. STATEMENT 8: BCM AWARENESS .....	7
4.9. STATEMENT 9: BCM TRAINING.....	7
4.10. STATEMENT 10: BUSINESS CONTINUITY OF KEY SERVICE PROVIDERS.....	7
4.11. STATEMENT 11: CORRECTIVE ACTIONS .....	7
4.12. STATEMENT 12: SIGNIFICANT CHANGE(S) .....	7
<b>5. ROLES, RESPONSIBILITIES AND ACCOUNTABILITIES.....</b>	<b>8</b>
COMPLIANCE TO THIS POLICY .....	9
DIRECTIVES.....	10
APPROVAL AND DISTRIBUTION OF THIS POLICY.....	10
<b>6. GLOSSARY OF ABBREVIATIONS AND DEFINITIONS .....</b>	<b>11</b>
<b>7. ADMINISTRATION AND APPROVAL OF THIS POLICY .....</b>	<b>13</b>
<b>ANNEXURE A: LEGISLATIVE FRAMEWORK.....</b>	<b>15</b>
<b>ANNEXURE B: REFERENCE DOCUMENTATION .....</b>	<b>16</b>

## STANDARD POLICY SECTIONS

### 1. Introduction

The BCM programme is considered an integral part to support the management and mitigation of risk to the organisation. AF makes every effort to ensure that it is protected against risks and threats that could materially impact its operations. However, it is recognised that the unexpected could and may happen, the effect of which could compromise the ability to meet acceptable standards of business. AF is also committed to providing the best possible value to its customers and the best possible relationships with employees, shareholders and suppliers. For these reasons, a Business Continuity Management programme is implemented.

BCM is not a regulated discipline in all the jurisdictions in which we currently operate, however there are industry and corporate governance best practices to which AF are obliged to comply for the implementation of BCM. In South Africa these include:

- King IV Report on Corporate Governance, the Board is responsible for the governance of risk and continuity of operations. Part 5.4: “The establishment and implementation of business continuity arrangements that allow the organisation to operate under conditions of volatility, and to withstand and recover from acute shocks”.
- Board Notice 158 of 2014, issued by the Financial Services Board for Long-Term and Short-Term Insurance, covering Governance and Risk Management Framework for Insurers, Part 4: Risk Management System, Section, 3, paragraph (f) – “The risk management system must, at least, include - processes for ensuring adequate contingency planning, business continuity and crisis management.”
- Prudential Standard GOI 3.2 Business Continuity Management (BCM). This Standard applies to all insurers licensed under the Insurance Act, 2017, other than micro insurers, Lloyd’s and branches of foreign reinsurers. The application of these Standards to insurance groups that have been designated as such by the Prudential Authority, under Section 10 of the Insurance Act, 2017, is addressed in a separate standard, GOG 1 (Governance and Operational Standard for Groups). Objectives and Key Requirements of this Prudential Standard: This Standard requires insurers to implement an enterprise-wide approach to business continuity management, designed to minimise the impact on critical business operations that could arise from a business disruption.

The key requirements of the Standard are that an insurer must:

- Have a board-approved policy and related procedures for its objectives and approach in relation to BCM;
- Conduct Business Impact Analysis that identifies all its critical business operations and assesses the impact of a material disruption on each of these;
- Business Continuity Plans that includes incident management and recovery plans; and
- A programme for review and testing of the Business Continuity Plans.

Notifications requirements:

- IN SA the Prudential Authority will be notified no later than 24hrs after experiencing a major disruption that has the potential to have a material impact on AF risk profile or affect its financial soundness. The notification will cover the nature of the disruption, the action being taken, the likely affect and the timeline for returning to normal operations. AF will notify the Prudential Authority when normal operations resume. Botswana, Nigeria, Jersey and Namibia will be subject to their respective regulators.

The executive committee of each company within the organisation is to familiarise itself with the specific laws, practices and standards that might be applicable to it from time to time. However, adherence to Group standards is overarching and should be adhered to.

## 2. Purpose

The Business Continuity Management (“BCM”) Policy serves as an overarching governing policy for the use, management and implementation of Business Continuity at Alexander Forbes Group Holdings (“AF”) and subsidiaries/associated companies

AF defines BCM as a holistic management process that identifies potential threats to the organisation and the impacts to business operations that those threats might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

This policy assures that there is a satisfactory level of Business Continuity to provide a level of protection from a range of threats, ensuring continuity of business operations, service delivery and maximising the return on investments of business interests.

## 3. Scope

AF shall be prepared for scenarios including, but not limited to, natural disaster, power outage, loss of strategically important premises, loss of technology, data corruption, pandemics, loss of employees, irrespective of their function, grade or standing.

BCM will be implemented with due regard to the acknowledgement that certain catastrophic events may incur casualties and loss of life.

The products, services and locations in scope for BCM are defined in the BCM Framework document.

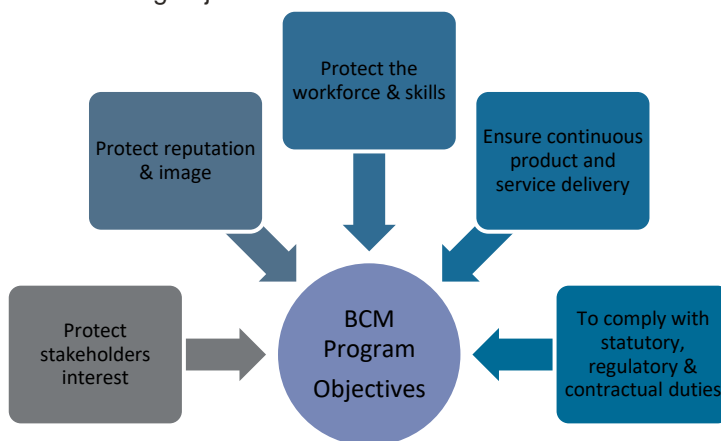
### Policy Objectives

The objectives of this policy are to support the BCM Programme to achieve:

- A programme that is formally established and maintained to support business resilience and remains fit-for-purpose.
- Ensure key products, services and locations, their supporting critical activities, processes and resources, are identified.
- Invocation of business continuity plans can be managed and executed effectively.

### BCM Programme Objectives

- This policy supports the implementation and maintenance of a BCM programme, which aims to achieve the following objectives:



### Alignment to International Standards

- The BCM programme implementation and maintenance will be aligned to leading global BCM standards and guidelines.
- Currently this includes the Business Continuity Institute Good Practice Guidelines (2018) The AF BCM programme is maintained in line with the BCM lifecycle below:



## 4. Policy Statements

### 4.1. Statement 1: Business Continuity Management Policy

A formal review of this policy shall be carried out at least annually, or sooner if required, by the AF Group BCM Manager and input and approval obtained from Group Exco and the Board.

### 4.2. Statement 2: Business Impact Analysis (BIA)

A formal business impact analysis shall be carried out at least once a year by all BCM Business Units teams in order to determine or review the requirements for the various Business Continuity Plan(s). The BIA will cover critical business operations (functions, resources and infrastructure) and recovery levels and time targets for each critical business operation. Triggers, such as major changes in processes, technology or people will prompt an earlier BIA to be carried out, which will feed into a review and reassessment of the BCM Strategy, BCPs and recovery solutions. The BIAs are to be signed off by the BCM Plan owner. The business head for each platform is responsible to have oversight and agreement for all the BCPs in their platform.

### 4.3. Statement 3: Threat Assessment (TA)

A formal threat assessment to assess 'continuity' and 'availability' threats shall be reviewed as part of the BIA process. The BCM BU teams should determine threats that may impact the continuity of operations, arising from all material risks including but not limited to risks relating to Information Technology and Cyber-attacks. This should be viewed in conjunction with the AF Enterprise Wide Risk Management ("EWRM") framework.

### 4.4. Statement 4: Business Continuity Strategies/Solutions

A formal review of the business continuity strategies to meet requirements of Business Continuity shall be carried out at least once a year as part of the BIA process, for critical business operations by the BCM BU teams to ensure the appropriateness of its recovery and continuity capability. Implementation of all strategies will be tracked by the AF Group BCM Manager, but responsibility for ensuring they are in place, remains with the respective BU's and or executives.

### 4.5. Statement 5: Business Continuity Plans

A formal review of the Business Continuity Plans (BCP) shall be carried out at least once a year by BCM BU teams to ensure their readiness for use in an incident to enable functional teams to continue to deliver its critical products and services at an acceptable predefined level. The plans will cover the resources and infrastructure required, as well as roles and responsibilities and the authority to act in relation to the plan. The BCPs will be signed off by the Business Continuity Plan owner or Deputy.

### 4.6. Statement 6: Incident Management

The Incident Management team members will be nominated by the Group BCM Manager and approved by Group Exco. The Group BCM Manager will also develop an Incident Management Process that details the process in order to manage the incident. The Incident Management plan includes a communications plan which covers internal and external, digital and customer stakeholders.

### 4.7. Statement 7: BCM Testing and Exercising

The scope of BCM testing will include:

- Desktop walkthroughs with BCM BU Teams
- The results of testing will be formally reported to the relevant committees and ultimately to the Board of Directors.

- All relevant documents will be updated with any shortcomings identified as a result of review and testing as required.
- Scenario/simulation exercises with the following crisis teams:
  - Incident Management Team
  - Communications Team
  - Facilities/OHS Team
  - HR Team
- IMT and communications should be exercised at least once a year, and modifications shall be made where necessary to take account of the exercise results.

Our offices are our recovery sites which are used daily so no testing of recovery sites is required

**Note:** This policy does not cover IT Disaster Recovery policy, plans, solutions and testing or Cyber Security. It is important that this policy is read in conjunction with the IT DR Strategy/Policy.

#### **4.8. Statement 8: BCM Awareness**

All staff shall, through various awareness campaigns and an assessment (at least once a year), be made aware of AF BCM arrangements to ensure familiarity. BCM is to be included in induction for new employees.

#### **4.9. Statement 9: BCM Training**

Whereas awareness is generally targeted at all staff, training is directed at staff with specific BCM functions and responsibilities. Formal training shall be conducted as required for all staff involved in the recovery to be equipped and adequately prepared with the necessary knowledge and skill to undertake recovery activities. Staff that are part of the IMT must attend training/exercising at least once a year as per their signed acceptance of the role.

#### **4.10. Statement 10: Business Continuity of key service providers**

AF Procurement will ensure that Business Continuity arrangements of critical service providers, as identified by business are evaluated; concentrating its efforts on services whose failure would most quickly disrupt AF prioritised activities. Techniques may include specification of requirements in tenders and contracts, or periodic audit of supplier BCP's. It is noted that this may take time to achieve.

#### **4.11. Statement 11: Corrective Actions**

AF shall take actions to eliminate the causes of nonconformities identified with the implementation and operation of the BCM to prevent their recurrence. All such actions taken shall be documented.

#### **4.12. Statement 12: Significant Change(s)**

All reviews of the various BCM elements will be conducted in line with the above policy statements, or earlier as required should there be any significant changes on the business ownership, locations, technical infrastructure, BCM roles, regulations or product lines / brands and services offered. All such changes shall be documented.

## 5. Roles, Responsibilities and Accountabilities

Through the approval of this policy, AF Group Executive Committee (“EXCO”) demonstrates its commitment to BCM. The EXCO reports to the AF Board, and the Board is ultimately accountable for the successful implementation of the BCM programme, and forms part of the overall risk management strategy, as per the governance requirements of the Prudential Authority, Financial Conduct Authority and King IV. The mandate of the Group Exco (Steering Committee) is to approve the strategy for delivering the BCM provisions made by the BCM policy and give direction on how the programme of work will be prioritised, delivered, managed and maintained.

AF’s internal audit function will periodically review the Business Continuity approach and provide assurance to the Board of Directors that it is consistent with the BCM policy. Internal audit will provide assurance regarding compliance to the Prudential Authority if requested.

The Business Continuity Manager will ensure the provision of a formal budget to fund the resource requirements for an effective and well maintained BCM programme to cater for all BCM capex and non-capex items (if and when they become applicable) including but not limited to:

- Personnel to support the continued improvement of the BCM;
- BCM training and awareness costs, including refresher training and exercises;
- BCM maturity reviews and BCM testing;
- Consulting and Advisory expenses; and
- Other utility or related operating costs.

The table below outlines the roles and responsibilities of the stakeholders responsible for the governance of this Policy:

STRUCTURE / FUNCTION	ROLE	INTEREST, DUTIES & RESPONSIBILITIES
<b>Board of Directors</b>	Accountable	X
	Oversight	
	Strategy	
	Governance	
<b>Executive Committee (Group Exco)</b>	Enforcement	X
	Governance	
	Approval	X
	Operations	
<b>Compliance</b>	Notification	X
	Ownership	
	Monitoring	X
	Oversight	X
	Review and Reporting	

STRUCTURE / FUNCTION	ROLE	INTEREST, DUTIES & RESPONSIBILITIES
<b>Audit and Risk Committee (Group ARC)</b>	Governance	X
	Monitoring	
	Reporting	X
<b>Accountable Business Units</b>	Governance	
	Operations	X All business units across the Group are responsible for implementation and maintenance
	Monitoring	X
	Reporting	X

A more detailed breakdown of the various BCM role players is provided below:

## RACI chart

Implementation & Maintenance					
	BU Plan owner	BCM Champion	Platform Manco's	Group BC Manager	Group Exco
<b>BCM Policy</b>	Acknowledge	Contribute	Informed	Compiler	Review/Approval
<b>BIA's &amp; Threat Analysis</b>	Compile in toolkit annually or earlier if required	Review & QA	Approval	Group wide consolidation	Informed
<b>Strategies</b>	Compile in toolkit annually and update as required	Review & QA	Informed	Group wide consolidation	Approval
<b>BC Plans</b>	Compile in toolkit annually and update as required	Review & QA	Oversight	Oversight	Informed
<b>Testing</b>	Participate	Co ordinate	Participate	Co ordinate	Informed of testing outcome
<b>Awareness</b>	Be ambassador	Co ordinate	Endorse	Co-ordination & oversight	Informed
<b>Maintenance</b>	Update in toolkit as changes occur ie names, cell numbers etc	Accountable for cluster maintenance	Informed	Assistance & oversight	Informed

It is the Business Unit (BU) leader's responsibility to assign accountability, responsibility, and authority to designated teams/individuals to ensure that the BU complies to the requirements with this policy. These additional responsibilities should be included in their job descriptions.

Refer to "BCM Framework" for additional governance details.

### Compliance to this policy

Consistent compliance with this policy is essential to its effectiveness. All employees are required to:

- Read and understand the requirements as stated in this policy via Policy Passport system;
- Co-operate with the Company with duties and requirements imposed by relevant statutory provisions and Company Procedures as indicated in this policy; and
- Support the activities required to protect company assets, mission and survivability.
- Failure to comply with this policy may result in disciplinary action being taken against an employee under AF disciplinary procedures, which may, depending on the circumstances, include the withdrawal of permission to use the company's equipment for personal purposes and / or a formal written warning or summary dismissal.
- Where applicable, BCM has been embedded in employee performance management contracts, but it is mandatory for all employees to actively participate as required, which includes completion of the annual BCM assessment

### **Directives**

- The Company reserves the right to issue Group Directive/s which will provide practical guidance in the event of an emergency and ensure business continuity.
- Any such Group Directive/s will be issued by or on behalf of EXCO and will override all other instructions, policies and employment contracts, subject to compliance with legislation.
- The Group Directive/s will be limited to those steps considered necessary for business continuity and will be in place for a stipulated period of time, which may be extended from time to time subject to the management of the relevant emergency incident.

### **Approval and Distribution of this policy**

- The Group EXCO and the Board must review the policy and formally approve the document.
- It will be saved on Policy passport.

## 6. Glossary of Abbreviations and Definitions

This section includes definitions for all terms used within this policy, including acronyms where applicable.

Use the following outline and be sure that all terms appear in alphabetical order.

TERM	ACRONYM	DEFINITION
Business Unit	BU	Business Unit or BU refers to a division, facility or department of an organization. Notes (1): Examples of business units include retail outlets and human resource department. A business unit can perform a number of business functions.
Group Business Continuity Manager	-	A Senior representative who has the responsibility (Group level) for co-ordination of the overall BCM planning programmes.
Business Continuity Management	BCM	A holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
Business Continuity Plan (BCP)	BCP	A documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical activities at an acceptable pre-defined level. Although the term 'Business Continuity Plan' (BCP) implies a single document, in reality this covers a number of different activities and will usually consist of multiple plans, including IT Disaster Recovery.
Business Continuity Policy	-	A BCM policy sets out an organisation's aims, principles and approach to BCM, what and how it will be delivered, key roles and responsibilities and how BCM will be governed and reported upon.  Good Practice Guidelines states that the primary purpose of a BCM Policy is communication and should be owned by executive management and demonstrates their commitment.
Business Impact Analysis (BIA)	BIA	The process of analysing business functions, skillsets, equipment, suppliers, IT systems, documents and the effect that a business disruption might have upon them and to collect information to resume and continue the business activities at a level required to support the organisation's objectives and obligations.
BCM Business Unit Team	BCM BU Team	A staff member/s appointed by a business unit to serve as the liaison person/champion responsible for all BCM activities within the business unit.
Employee / Staff	-	Any person appointed on a contract of employment, irrespective of function or grade.

TERM	ACRONYM	DEFINITION
AF Group Executive Committee	EXCO	Committee or group of an organization is a committee within that organisation which has the authority to make decisions and ensures that these decisions are carried out.
Information Technology	IT	Information Technology (IT) is the use of any computers, storage, networking and other physical devices, infrastructure and processes to create, process, store, secure and exchange all forms of electronic data.
King IV Report on Corporate Governance	King IV	King IV is structured as a Report that includes a Code, with additional, separate sector supplements for SME's, NPO's, State-Owned Entities, Municipalities and Retirement Funds. The King Code contains both principles and recommended practices aimed at achieving governance outcomes.
Threat Assessment	TA	The process of evaluating threats to identify unacceptable concentrations of risk to activities and single points of failure.

## 7. Administration and Approval of this Policy

<b>POLICY NAME</b>	Business Continuity Management	
<b>POLICY OWNER</b>	Group BCM Manager	
<b>EFFECTIVE DATE</b>	August 2015	
<b>LAST APPROVED DATE</b>	March 2020	
<b>APPROVAL</b>	Required forum (AFGH Board, Sub-committee, Group Exco)	
<b>VERSION</b>	1.10	
<b>LAST REVIEW DATE</b>	June 2022	
<b>NEXT REVIEW DATE</b>	June 2024	
<b>DISTRIBUTION LIST</b>	ALL Staff	
<b>PROCESS REQUIRED FOR IMPLEMENTATION</b>	Acknowledgement only	x
	Basic understanding test	
	Detailed understanding test	
	Training required	

### Policy Approver Disclaimer:

I have read the Policy.	x
I undertake to comply with the provisions of the Policy and agree that I will not breach such provisions.	x
I agree that I will lead and encourage compliance by staff and management with the Policy.	x

### Process for Policy updates

Version	Date	Revision Author	Summary of changes
1.1	August 2015	Stephanus Burger, Continuity SA	Policy created
1.2	September 2017	Susan Mercer, Tracey Linnell (TLC)	Policy review
1.3	January 2018	Susan Mercer	Additional Polices added
1.4	May 2018	Susan Mercer	Alignment to GPG 2018
1.5	July 2018	Susan Mercer	Changes in terminology for FSB and Board notice 158

---

1.6	Dec 2018	Susan Mercer	Inclusion of JSE listed requirements. Changes to 3.2.2 and 3.25 to included sign off requirements
1.7	January 2019	Susan Mercer	Annual review to align closer to Prudential Authority GOI.3
1.8	March 2020	Susan Mercer	Annual review
1.9	Sept 2020	Susan Mercer	Revision due to remote way of work
1.10	Nov 2020	Susan Mercer	Transfer to Group Policies template and updated review date to every two years
1.11	June 2022	Susan Mercer	Minor changes in Sections 3,5 and 4.3, 4.4, 4.6, 4.7, 4.10

## Annexure A: Legislative Framework

This section should state the laws, regulations and best practice guidance that were considered in developing the policy. If possible, these should be listed in order of priority and importance.

No.	NAME OF LEGISLATION, REGULATION, FRAMEWORK OR GUIDELINE
1	Prudential Standard GOI 3.2 Business Continuity Management (BCM)
2	Board Notice 158 of 2014, issued by the Financial Services Board for Long-Term and Short-Term Insurance, covering Governance and Risk Management Framework for Insurers, Part 4: Risk Management System, Section, 3, paragraph (f)
3	King IV Report on Corporate Governance

## Annexure B: Reference Documentation

If this policy is related to any other important governance documentation it should be referenced here, so that changes to this policy can consider changes which may be required in other policies, procedures, standards or guidelines.

The following relationships are identified:

- **Governed by:** Any over-arching policies with which this policy must comply.
- **Referenced:** Any policy or governance documentation which has been used or referenced in the creation of this policy. Updates or changes to any of these policies may impact this policy.
- **Linked to:** Any other governance documentation which may be affected should this policy be changed or updated.

POLICY NAME	RELATIONSHIP
Occupational Health and Safety Policy (OHS)	Referenced
AFGIT Disaster Policy	Referenced
Information Security Policy	Referenced
Emergency Response Plan (ERP).	Referenced
Human Resources Policies	Referenced
EWRM framework	Referenced