VERSION 1.1

OCTOBER 31, 2018

the gpaa

Department:
Government Pensions Administration Agency
REPUBLIC OF SOUTH AFRICA

BUSINESS CONTINUITY STRATEGY

2018-2022

PRESENTED BY: DR CLIFFORD FERGUSON

GPAA HEAD OFFICE

34 HAMILTON STREET., ARCADIA, PRETORIA, 0001

STRATEGY SIGN-OFF

The undersigned accept the BCM strategy as contained herein:

Dr CS Ferguson	Chairperson BC Committee	Signature	Date
Ms Ramabele Magoma-Nthite	Vice Chair BC Committee	Signature	Date
Dr SB Khumalo	GM Strategic Support	Signature	Date
Mr M Coetzee	CIOe	Signature	Date
Mr Krishen Sukdev	CEO	Signature	Date

CEO FOREWORD

Mr Krishen Sukdev
Chief Executive Officer
Government Pensions Administration Agency
(GPAA)

The GPAA strategic goals revised during the Strategic Planning Lekgotla, held in May 2018 are as follows:

1. Optimal core services,
2. Valid, accurate and complete contributions,
3. Less than 30-day turnaround time for the payment of benefits,
4. Well preserved pension funds, and
5. Realigned organisation

The revised strategic goals of the GPAA will drive its mission "to provide administration services to the GEPF and National Treasury Programme 7" through core business functions, which include the admission of new members, management of contributions and provision of benefits, Communication to members and the maintenance of member and beneficiary data.

The GPAA has recorded progress in terms of implementing Business Continuity Management (BCM) and resilience through the modernisation programme. The GPAA BCM ensures that contingency plans are in place to provide modernisation systems availability and resilience by having replica data centres and disaster recovery centres to be able to cope better with disturbances.

The GPAA believes that if it successfully continues with the Modernisation Programme and Business Continuity Management, its approach and practices towards service delivery will greatly improve client experience consistently and provide allocative efficiency.

In its ninth year of existence, the GPAA will build on the solid foundations it has laid in becoming a modernised pension fund and benefits administrator through embedding a culture of business continuity to improve on its ability to provide services delivery as envisaged.

Ultimately, the GPAA wants to be on the forefront of service resilience to offer a respectable retirement for government employees and other beneficiaries of its administrative services and with a constant reminder of the stakeholders we serve, we believe that our continued diligence will achieve this.

Mr Krishen Sukdev
CHIEF EXECUTIVE OFFICER
Government Pensions Administration Agency
(GPAA)

FOREWORD HEAD OF STRATEGY, POLICY AND BCM

The GPAA has been operating in the Business Continuity space since 2010, where the GPAA EXCO and MANCO officials qualified as CBCi practitioners after writing the GPG 2010 examination. The BC committee was appointed in 2010, thereafter the sub-committees, SHERQ, Process recovery, and systems recovery committees were appointed, each with its own Terms of Reference.

GPAA has matured to the extent that it was recovering systems in more that 72 hours in 2010/11 whereas it recovers systems in some cases in less than 10 minutes. In other cases resiliency has increased to the extent where recovery is not necessary due to automatic and manual switching over from site to site. Also built in redundancy in the Oracle stack allows for switchover in case of server failure.

The Mainframe is equally resilient due to its switchover capacity and capability with an recovery time objective of about 20 minutes and a recovery point objective of seconds. Yet, even though systems are mature, it was found that the auxiliary systems in the recovery process are failing, this in the systems utilised by Internal Audit, Finance, HR and Risk Management.

The GPAA is embarking on a BCM boot-camp, November 2018, wherein about 22 BC committee members will be receiving lead implementer training on the BC standard ISO 22301. This will increase the BCM capability of the GPAA and that of National Government.

The Strategy outlines the requirements for GPAA to be more resilient, to be able to manage simple and complex incidents and lastly to be able to recover from a disaster without adversely affecting service to the 1.8 million clients it serves.

CONTENTS

1 INTRODUCTION AND BACKGROUND

The Government Pensions Administration Agency (GPAA) is a government component mandated to administer pensions as instructed by service level agreements signed with its tow customers Government Employees Pension Fund (GEPF) and the National Treasury (NT). As at March 2017, Client base for GEPF and NT programme 7 combined is equals to more than 1.84 million, which equates to 31 % of South African population. The increase number of GPAA client base compelled the GPAA to draft a five year (2017/18 – 2020/21) strategic plan which articulates its vision, mission, and the set goals and objectives (Strategic Framework) to realise its envisioned state with cognizance of client centricity.

The GPAA strategic plan is based on the need to realise the following:

- Built sustained relationships with customers, clients and stakeholders and improve service delivery,
- Built capacity to meet increased/ ever-changing service demands/needs,
- service and operational levels as per the agreements, demand plans and overall requirements attainment, and
- Transition to an agile organisational.

The GPAA realises that delivery of its services directly affects the livelihoods of its 1.84 million clients their dependants. (Sibonelo Radebe, 2017) Concurred by stating that In the 2017/18 fiscal year of the 17 million grant beneficiaries, the number of dependants exceeds the number of social grant beneficiaries by a considerable margin. In most cases grants, which include pensions, disability payments and child support grants, support entire households. These households will be destitute if they do not receive grant or pension payments in a timely fashion.

Given the nature of the GPAA business, increased clientele and their dependents it's important to ensure resilience and business continuity at all times. In an increasingly competitive and changing environment times of today, implementing systems and methods for maintaining business continuity is no longer an optional requirement for the GPAA, especially since it is dependent on physical Infrastructure and Information Communication Technology (ICT). The efficiency of the GPAA work depends on its business continuity or disaster recovery management infrastructure. Implementing a sound enterprise ICT and infrastructure business continuity or disaster recovery solution has almost become a mandatory requirement for the GPAA. Costs incurred during business downtime are usually significant, thereby dictating a need for implementing a business continuity solution.

The GPAA's business continuity processes are designed to:

- To minimise any risk of disruption to services, by building resilience into internal structures and processes
- To ensure we can maintain our essential services during disruptions with different levels of severity
- To assist staff in the event of an incident and to ensure staff are able to cope with the disruption
- To ensure that if a disruption does occur, the main priority will be the recovery of key services within agreed timeframes.

2 BCM OBJECTIVES

The following BCM objectives have been set for the GPAA.

2.1 OBJECTIVES

The BCM Strategic objectives are

- To manage disruptive incidents without calling for recovery invocation
- To ensure recovery within the Maximum Tolerable time of Disruption (MTTD)
- To ensure recovery of systems within the required RTO
- To ensure recovery of systems within the required RPO
- To ensure instil an enterprise wide BC culture
- To ensure risk practitioners are suitable certified in BCM

2.2 GOVERNMENT DR SPACE SHARING

The GPAA shall partner with the following Departments for BCM and the sharing of recovery sites and ICT:

- Recovery sites:
    - National Treasury
- ICT Resilience
    - SITA
- Data Centres
    - SITA

3 CORE BUSINESS AND PROGRAMME STRUCTURE

GPAA's core purpose is to administer Funds and benefits on behalf of the GEPF and NT as delegated in the administration agreements and SLA's with each.

GPAA structure is depicted in Figure 1 - Organisational structure

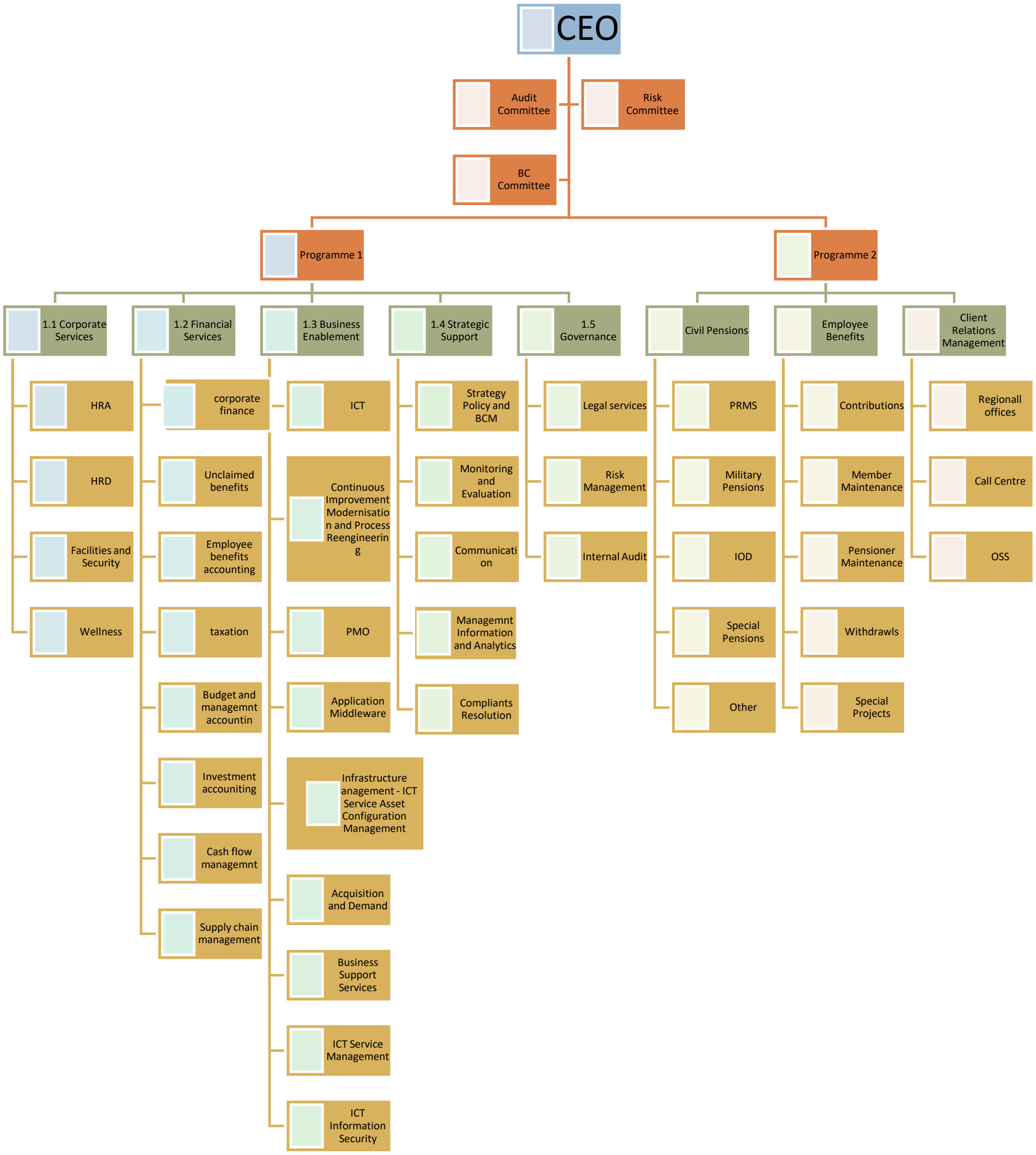

FIGURE 1 - ORGANISATIONAL STRUCTURE

4 BCM METHODOLOGY AND STRUCTURE

GPAA is following the government structure and methodology as advised by the Office of the Accountant General and the Nation BCM Forum.

4.1 BCM METHODOLOGY

The BCM Methodology is contained with the ISO 22301 standard and / or the Business Continuity Best Practice guide 2018. The methodology for the strategy and the business continuity plan (BCP) are presented in Figure 2 - Business Continuity Methodology.

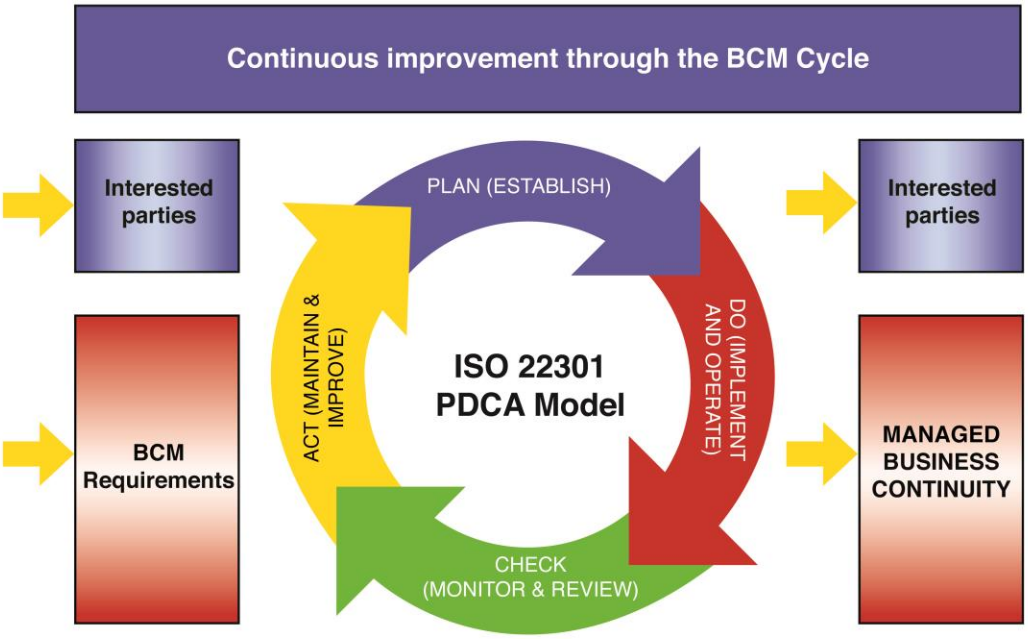

FIGURE 2 - BUSINESS CONTINUITY METHODOLOGY

The GPAA's Business Continuity Programme is managed and maintained by virtue of the PDCA model and the BCi Good Practice Guide 2018. The Policy has been updated and reviewed to include the aforementioned standards.

The BCM strategy is managed by the Business Continuity EXCO that oversees all BCM activities and ensures that the GPAA and its BCM activities are in line with prescripts of the PFMA, Treasury Regulations, KING IV and the posited standards.

The Strategy relates to how BC management will take place in the next three years and what will be required of each sub-committee to ensure the strategy is implemented on time. The three strategic pillars are depicted in Figure 3 - Four pillars of BCM at GPAA

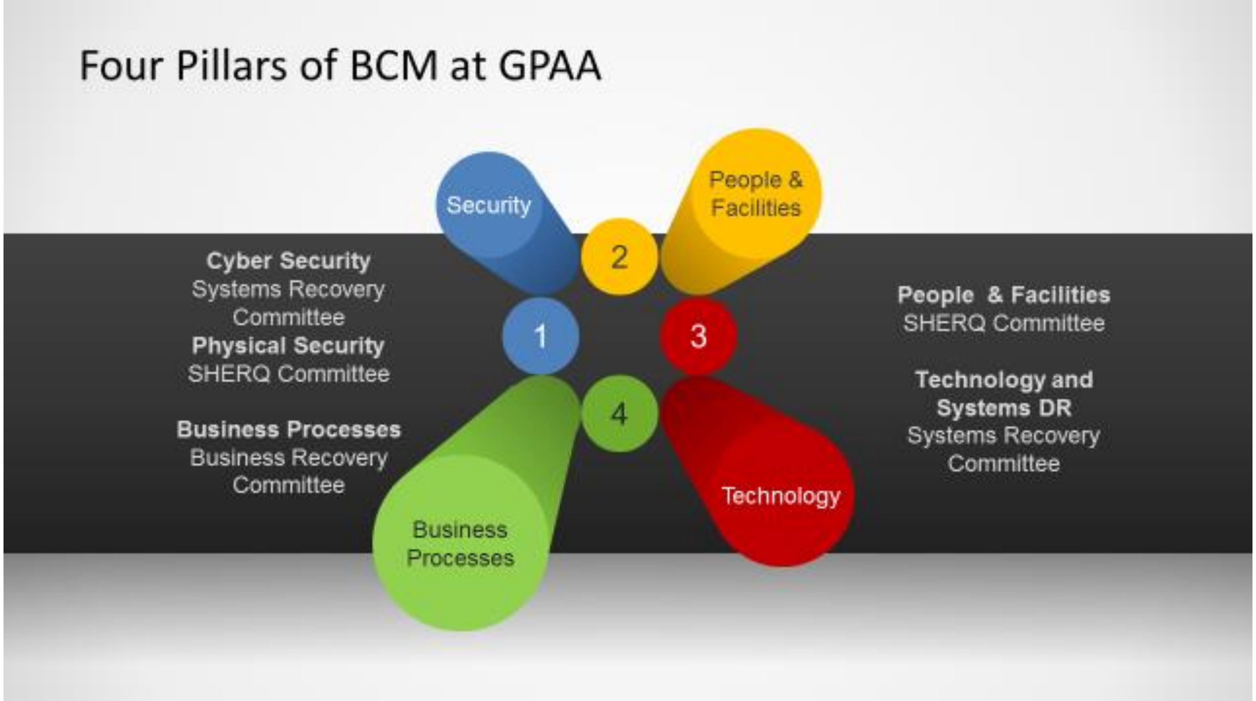

FIGURE 3 - FOUR PILLARS OF BCM AT GPAA

The four pillars directly related to the ability of the GPAA to deliver on its strategic and annual performance plans. The GPAA does not have a direct budget for BCM, each component of business budgets and integrates BCM into the annual budget. The integrated approach is linked to a volunteering system where BCM practitioners may come from any area of business. This includes but is not limited to Corporate services for the SHERQ Committee, physical security and OHS, the business recovery committee, representing core programme 2 with its sub-programmes, the systems recovery committee is reliant on the business enablement sub-programme to allow for systems recovery, disaster recovery (DR) and work area recovery (WAR).

Thus to ensure an encapsulated approach to resilience and business continuity management (BCM) in the government forum, GPAA complies with the templates designed for such.

The strategy will relate directly to:

1. Safety, health, environment, risk and quality management (SHERQ) in line with the OHS Act 85 of 1993 as amended in 2014.
2. Process recovery – Most importantly the core business processes of the GPAA that allow for the delivery on the GEPF and NT Programme 7 SLA's.
3. Resilience, work area and disaster recovery- the work area of the GPAA of at least 140 seats, the replicated Oracle and mainframe systems and bac-up recovery at realistic and specific Recovery Time Objectives (RTO) and specific and realistic recovery point objectives (RPO).
4. Damage assessment – as an ad-hoc service via the OHS appointee and subject matter experts as and when damage occurs through disruptive incidents.

The structure has been formulated to cater for the committees together with EXCO oversight.

4.2 BCM STRUCTURE

The BCM structure of the GPAA is depicted in Figure 4 - BCM Structure

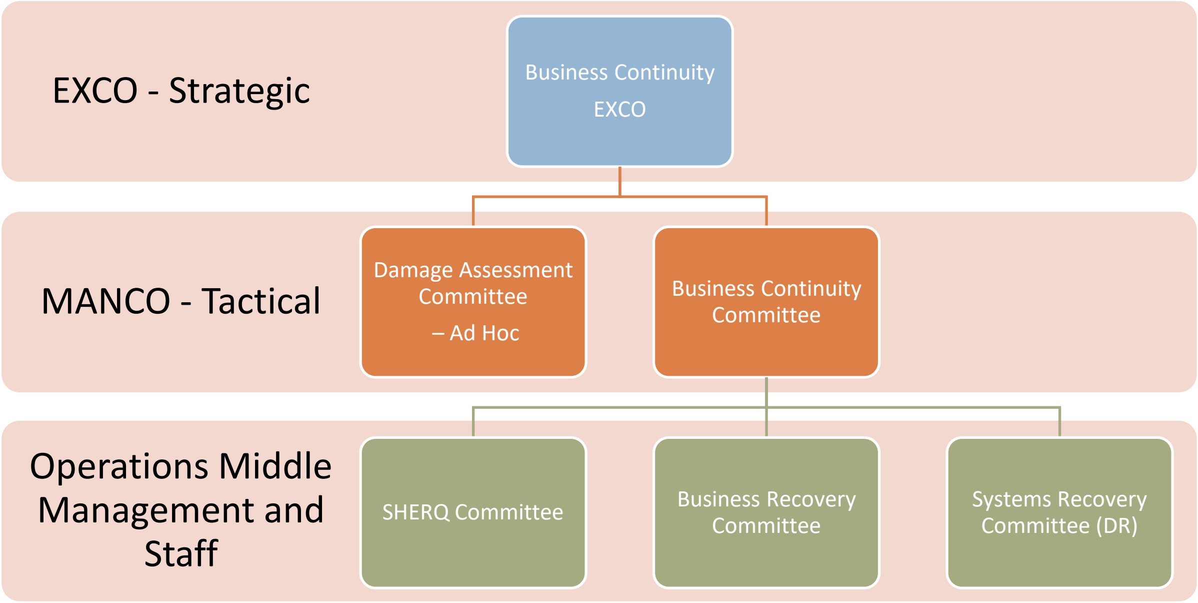
EXCO - Strategic
Business Continuity EXCO
MANCO - Tactical
Damage Assessment Committee – Ad Hoc
Business Continuity Committee
Operations Middle Management and Staff
SHERQ Committee
Business Recovery Committee
Systems Recovery Committee (DR)

FIGURE 4 - BCM STRUCTURE

The structure for BCP functions at GPAA, with a clear mandate for each committee with its own terms of reference. The BC EXCO take full accountability on behalf of EXCO in the time of a disastrous event and remain accountable for the events that affect the business in any way.

The responsibilities of each committee are linked to their mandate as they play a role to cause a resilient organisation, or if they play a part in recovery after an event. Therefore the roles and responsibilities of the committees are listed in each’s Terms of Reference.

5 INCIDENT MANAGEMENT

The plan depicted in Figure 5 - Incident management, is a graphical display of the workflow for incident management. The incident management BCP is attached – Annexure A – Incident management BCP

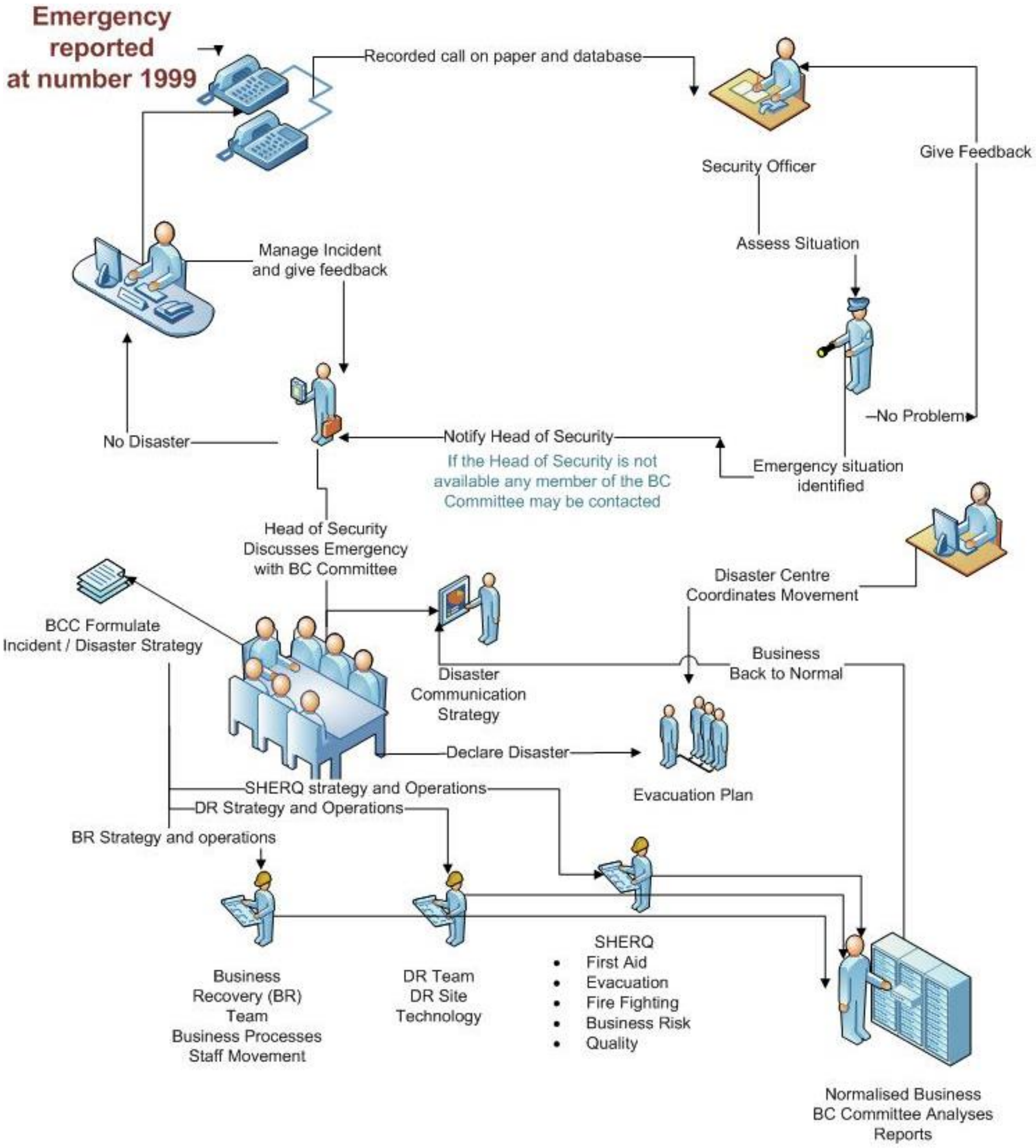
Emergency reported at number 1999
Recorded call on paper and database
Security Officer
Give Feedback
Assess Situation
Manage Incident and give feedback
No Problem
No Disaster
Notify Head of Security
If the Head of Security is not available any member of the BC Committee may be contacted
Emergency situation identified
Head of Security Discusses Emergency with BC Committee
Disaster Centre Coordinates Movement
BCC Formulate Incident / Disaster Strategy
Business Back to Normal
Disaster Communication Strategy
Declare Disaster
Evacuation Plan
SHERQ strategy and Operations
DR Strategy and Operations
BR Strategy and operations
Business Recovery (BR) Team
Business Processes
Staff Movement
DR Team
DR Site
Technology
SHERQ
• First Aid
• Evacuation
• Fire Fighting
• Business Risk
• Quality
Normalised Business
BC Committee Analyses
Reports

FIGURE 5 - INCIDENT MANAGEMENT

6 DISASTROUS RISKS

Disastrous risks shall be lodged on the GPAA Barn-Owl system, by the Risk management team, reporting to the Risk Management Committee via the Chief Risk Officer.

6.1 MITIGATING DISASTROUS RISKS

The GPAA's disaster risk mitigation comprises all forms of activities, including structural and non-structural measures to avoid (prevention) or to limit (mitigation and preparedness) adverse effects of hazards. Risk assessments workshops and meetings shall be held annually, records to be contained in a risk register report comprising of all risks susceptible to the GPAA environment and their individual mitigating strategies/activities. Monitoring of mitigating strategies/activities shall be conducted.

6.2 RECOVERY TIME OBJECTIVE (RTO)

- An assessment to determine an acceptable Recovery Time Objective (RTO) (after which time GPAA's viability could be threatened) shall be conducted.
- The RTO evaluation shall be conducted within the BIA to identify, where possible, the estimated tangible / financial impacts, and the intangible operational and reputational impacts.
- The GPAA RTO distinct to different business units to be documented and updated annually in individual business impact analysis reports.
- RTOs to be determined, and aligned, to the recoverability of the corresponding systems.
- The ICT landscape shall incorporate a fully resilient environment through the development of a hot standby / replicated environment.
- The Oracle Supercluster, Mainframe, Wintel, Wide Area Network (WAN) and Metro Ether environment shall each be replicated to a nearby site that would allow for an RTO well within the specifications of the BIA as well as maximum RPO of no longer than 15 minutes.

6.3 RECOVERY POINT OBJECTIVE (RPO)

1. RPO is the acceptable amount of data loss once data has been restored / recovered after a disruption. The RPO determines the recovery solution with regard to the required frequency of data back-ups and replication solutions implemented.
2. The GPAA RPO distinct to different business units to be documented and updated annually in individual business impact analysis reports.
3. The Time Critical Activities, RTOs and RPOs shall be realistic and ratified, and strategic solutions shall be identified to achieve them.

6.4 DISASTER RECOVERY

The disaster recovery and backup schedule and continuous replication of systems between GPAA Data Centre and Galo Manor in Sandton are to be utilised for speedy recovery within relevant RPO's and RTO's.Figure 6 - Disaster recovery Schedule depicts the back-up, replication, RTO, RPO when a majour incident occurs requiring a recovery process. It is in the interest of GPAA and its customers the recovery process is as resilient and seamless as possible, in some cases a majour event may not be disruptive, due to the absorption capabilities and elasticity of the GPAA. Such elasticity develops through a maturing BCM programme.

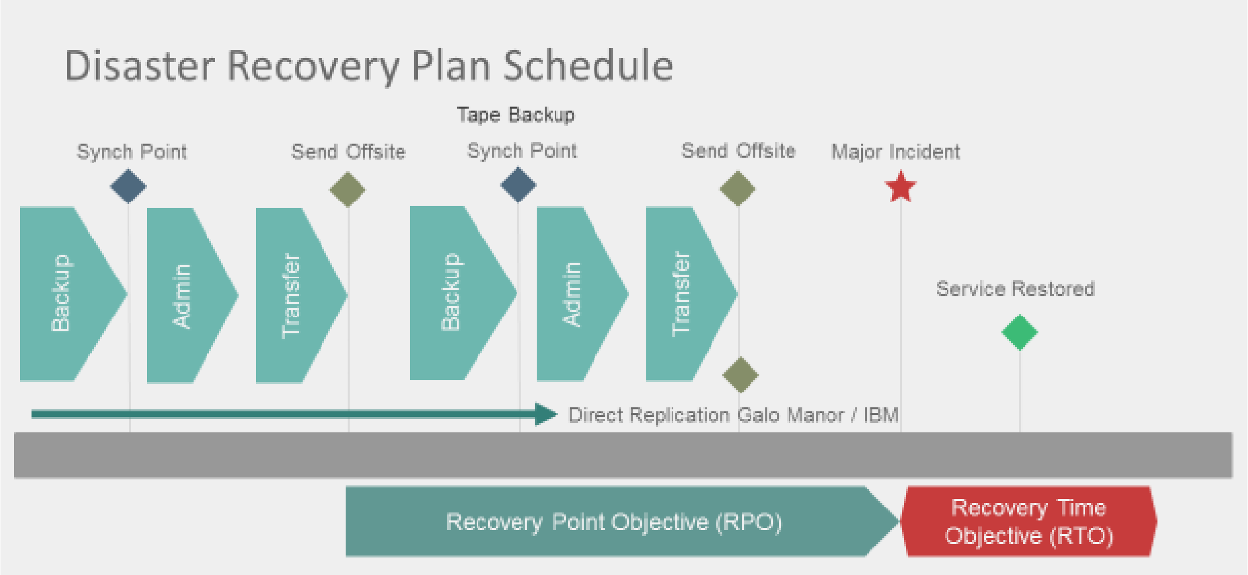
Disaster Recovery Plan Schedule
Tape Backup
Synch Point
Send Offsite
Synch Point
Send Offsite
Major Incident
Backup
Admin
Transfer
Backup
Admin
Transfer
Service Restored
Direct Replication Galo Manor / IBM
Recovery Point Objective (RPO)
Recovery Time Objective (RTO)

FIGURE 6 - DISASTER RECOVERY SCHEDULE

6.4 DISASTER RECOVERY STRATEGIES AT GPAA:

The disaster recovery (DR) strategies at GPAA coincide with the concepts prescribed by the National Government BCM forum, i.e. shared government resources. The failover plans encompass the GPAA requirements with a number of DR options for the head office, call centre, regional offices and data centre.

6.4.1 HEAD OFFICE

Head office has two replication sites namely Galo Manor, for Oracle and the HP servers and IBM in Randburg for the IBM mainframe. The head office houses about 680 staff of which head office business units, about 40 have their own BC plans. Head office staff in case of a disaster will recover in two ways, one by working in a designated work area, or working remotely form home.

1. GPAA Laptop Users - work remotely via virtual private network (VPN)
2. Desktop users - work at designated work areas
3. Alternate work areas:

   a. 40 Church Street 20 seats
   b. Hotels with 3G or mobile van connectivity – 25 - 60 employees per mobile van connection
   c. School hall or Thusong centres -25 – 60 employees per 3G mobile connection
   d. Regional Office boardrooms – 12 employees per boardroom
   e. Shared Government offices – 20 per office- future plans

By utilising the 3G network, hotels or Thusong centres GPAA can comfortably accommodate 60 employees in each of the designated sites. The technical specification of the DR solution shall be presented by ICT in the DR plan.

Alternate water supply is available at GPAA Head office together with a single diesel generator. A second diesel generator shall be purchased for the purpose of resiliency.

6.4.2 CALL CENTRE

The call centre is the heartbeat of GPAA and should be up and running with 1 hour of a disastrous event. To this end GPAA has contracted with Treasury for 40 call centre seats, dedicated to GPAA, at 40 Church street, Church Square, Pretoria. Also the GPAA call centre will do automated switchover to the regional offices after invocation of the BC Plan. This will allow for a total of 95 call centre service point nationally. The call centre will be set up on softphones with headsets on desktop computers.

1. 40 call centre seats at 40 Church street
2. 5 Call centre seats at each regional office = 55 seats

6.4.3 TREVENA CENTRE

The Trevena centre houses both the call centre and walk in centres of Pretoria for the GEPF. The call centre failover as discussed in the previous section would obviously suffice if transport is made available to 40 Church street.

The walk in centre would move to head office, with official announcements and notices, this will ensure service continuity to the clients.

6.4.4 REGIONAL OFFICES

Regional offices have two options for a DR situation. One to use the mobile van at a Thusong centre and connect via CLO laptops, with a later delivery of desktop machines. Two, a cohabitation with another government department, like National Treasury, SARS, Home Affairs or the like.

6.4.5 DATA CENTRE

1. Emergency supply
   a. Generators at GPAA
   b. UPS
   c. Water
2. Back-Up Tapes
   a. Back up of servers to tape – every 24 hours
3. Direct Replication
   a. Direct server replication to Galo Manor
   b. Direct Server Replication to IBM
4. Direct switchover of call centre
   a. To be introduced as an emergency measure
5. Server rebuilds
   a. Server rebuilds via live replication
   b. Tape back-up rebuild

6.5 SEATING REQUIREMENTS

- Business impact analysis meetings and workshops shall be held annually between business continuity sub Programme manager and the GPAA business units representatives for data collection to update statistics for a BIA, the seating requirement have been calculated to be 180, will be 40 call centre seats and 20 payment processing seats at 40 Church street. 120 other seats are in line with the Thusong or hotel strategy.
- The BIA shall determine seating requirements that would enable critical processes to be recovered over different time periods,

- Recovery time periods shall be classified under 2 hour, 6 hours, 1 day, 2 days, 1 week, 1 month and longer and the seating arrangement/staff compliment shall be adapted to different recovery time periods, more seats will be required should it take longer periods to recover.
- The staff compliment shall be determined in terms of certain percentage of the normal/overall staff complement because not all GPAA staff compliment requires seats at the disaster recovery site seats can be shared between numbers of staff on a shift basis.
- The disaster recovery site shall be tested for capability and efficiency twice a year.

6.5 MITIGATING STRATEGIES

Risk mitigation is defined as taking steps to reduce adverse effects, mitigation strategies unique to Business Continuity and Disaster Recovery are as follows:

- Risk Acceptance: Risk acceptance does not reduce any effects however it is still considered a strategy. This strategy is a common option when the cost of other risk management options such as avoidance or limitation may outweigh the cost of the risk itself.
- **Risk Avoidance:** Risk avoidance is the opposite of risk acceptance. It is these actions that avoid any exposure to the risk whatsoever. Risk avoidance is usually the most expensive of all risk mitigation options.
- **Risk Limitation:** Risk limitation is the most common risk management strategy used by businesses. This strategy limits a company's exposure by taking some action. It is a strategy employing a bit of risk acceptance along with a bit of risk avoidance or an average of both. An example of risk limitation would be a company accepting that a disk drive may fail and avoiding a long period of failure by having backups.
- **Risk Transference:** Risk transference is the involvement of handing risk off to a willing third party. For example, numerous companies outsource certain operations such as customer service, payroll services, etc. This can be beneficial for a company if a transferred risk is not a core competency of that company. It can also be used so a company can focus more on their core competencies.

For each meaningful risk identified and prioritized, a suitable mitigation strategy shall be applied.

6.6 CRISIS MANAGEMENT AND COMMUNICATION

The GPAA's approach to crisis management goes far beyond managing the organisation's image and reputation. A threat shall provide the GPAA with an opportunity to learn from the event, communicate honestly and ethically and work to minimise harm to those directly impacted by the crisis and develop the perspective vision with which the organisation can move forward. The GPAA intends to enact a strong and positive ethical core values and effective crisis communication principles to their crisis response by:

- Having an annually updated crisis management plan,
- A designate crisis management team that is properly trained,
- Conducting exercise at twice a year to test the crisis management plan and team,
- Pre-drafting selected crisis management messages including content for dark web sites and templates for crisis statements, and
- Having the legal department review and pre-approve these messages.

6.7 ALTERNATE WATER AND ELECTRICITY SUPPLIES

GPAA head Office, DR Sites and regional offices shall be fitted with automated changeover systems for alternate water and electricity supplies. GPAA offices shall have at minimum, an on-site water capacity of 3 days. Current state of alternate water and electricity supplies are tabulated in Table 1 - Alternate Water and Electrical supplies

.	Office	Current Location	Water tank Installed	Generator Installed	Comments
1	Johannesburg Office	2nd Floor, UCB House, 78 - 74 Marshall Street, Marshalltown	Yes	No.	To be procured for the new office
2	Gauteng Regional Office (Customer Contact Centre)	Trevenna Campus, Sunnyside, Pretoria.	No	Yes.	Water Tank to be procured
3	Bloemfontein Office	No. 2 President Brand Street, Bloemfontein	No	Yes.	Water Tank to be procured
4	Phuthaditjaba Office	Mandela Park Shopping Centre, 712 Public Road, Phuthaditjhaba	Yes.	Yes.	
5	Kimberley Office	11 Old Main Road, Kimberley	Yes	Yes.	
6	Durban Office	407 Anton Lembede Street, Salmon Grove Chambers, Durban	Yes.	No.	Generator to be procured in the 2019/20 budget
7	Pietermaritzburg Office	Brasfort House, 3rd Floor, Chief Albert Luthuli Street, Pietermaritzburg	No.	Yes.	Water Tank to be procured
8	Mthatha Office	Ground Floor, Madeira Plaza, Cnr Sutherland and Madeira Streets, Mthatha	Yes.	No.	Generator to be procured for new office in the 2019/20 budget
9	Bisho Office	No. 12 Global Life Office Centre, Circular Drive, Bisho	Yes.	Yes.	
10	Port Elizabeth Office	Ground Floor, Sivuyile Mini-Square, Kwantu Towers, next to City Hall, Port Elizabeth	No.	No.	Generator and Water tanks to be installed
11	Cape Town Office	21st Floor, LG Building, Long Street, Thibault Square, Cape Town	Yes.	Yes	
12	Polokwane Office	87(a) Bok Street, Polokwane	Yes.	Yes.	
13	Thohoyandou Office	2010 Complex, next to SABC's Phalaphala FM, Thohoyandou	Yes.	Yes	.
14	Nelspruit Office	28 Samora Machel Drive, Imbizo Place, Nelspruit	No.	Yes	Water tank to be installed
15	Rustenburg Office	149 Leyds Street, Rustenburg	No.	Yes.	Water tank to be installed
16	Mafikeng Office	Mmabatho Mega City, Office 4/17, Ground Floor, Entrance 4, Mafikeng	Yes	Yes.	
17	GPAA Head Office	34 Hamilton Street, Arcadia, Pretoria	Yes	Yes	Replacement of second generator in process.

TABLE 1 - ALTERNATE WATER AND ELECTRICAL SUPPLIES

7 ROLES AND RESPONSIBILITIES

To effectively constitute the implementation of the BCM strategy and the BC Plan the roles and responsibilities have been clearly outlined.

7.1 BC EXCO:

- Safeguarding the GPAA and stakeholder intellectual property
- Reporting to the CEO or EXCO on matters pertaining to BCM and resilience
- The BCM Strategy
- The BCM Policy
- The BC Plan

7.2 BC COMMITTEE:

- Adhering to the BC Policy
- Implementing the BC Strategy
- Implementing the BC Plan
- Constituting the subcommittees, namely: SHERQ, Business Recovery, DR and Damage assessment;
- The authority to declare the state of emergency and disaster and to give relevant emergency instructions to all GPAA employees;
- Implementing and maintaining the BCM policy and strategy;
- Maintaining a high level BCM coordination within the GPAA;
- Storing all BC documents in a central location according to the National Archives standards;
- Participating in all BCM programme activities;
- Facilitating the BC programme management lifecycle and drafting documents through the Strategy and Policy unit;
- Overseeing the activities of tactical level committees; and
- Providing the BIA and CRA for the GPAA.

7.3 BUSINESS RECOVERY COMMITTEE:

- Highlighting all circumstances that may disturb the institutional operations;
- Manifesting resilience during any operational disruption;
- Participating in the entire BCM programme implementation; and
- Conducting business recovery tests according to plans.

7.4 SHERQ COMMITTEE:

- Facilitating evacuation, safety and wellness of employees;
- Ensuring adherence to the OHS Act;
- Reporting to the BCC during a disaster;
- Reporting to the BCC in terms of evacuation plans and readiness;
- Implementing the BCM programme at operational levels of the institution;
- Identifying all physical threats that can hamper the institution’s facilities and security; and]
- Assisting the BC committee in creating staff awareness on the BCM programme.

7.5 DISASTER RECOVERY COMMITTEE:

- Reacting to business requests for technology and systems in times of incidents and emergencies;
- Reporting to the BCC in times of a disaster;
- Reporting to the BCC in terms of DR plans and readiness;
- Maintaining ICT equipment that will assist the BCC in times of a disaster;
- Identifying and maintaining disaster recovery sites; and
- Arranging a disaster recovery team.

7.6 SUPPLY CHAIN:

- Providing emergency supplies in the disaster or incident;
- Mandating suppliers to have a BC plan in place;
- Providing the BC committee with updates regarding the GPAA's outsourced activities; and
- Participating in the BCM programme.

7.7 LEGAL SERVICES DIVISION:

- Providing legal opinions; and
- Participating in the BCM programme.

7.8 RISK AND AUDIT UNIT:

- Reviewing all BC plans in all levels – strategic, tactical, and operational level; and
- Coordinating with all GPAA divisions and stakeholders in evaluating risks for BCM purposes.

7.9 COMMUNICATION UNIT:

- GPAA and Customer reputation management;
- Drafting a communication strategy for BCM programme; and
- Communicating with management and staff on BCM issues during a declared disaster.

7.10 CORPORATE MONITORING AND EVALUATION UNIT:

- Monitoring Adherence to BC good practice guidelines;
- Monitoring and reporting post incidents and tests; and
- Evaluating according to BC good practice guidelines.

7.11 THE INTERNAL AUDIT UNIT:

- Post exercise audits.

7.12 THE BCP OUTLINE

The incident BCP outline is listed below and will be utilised to manage incidents and/or invocations.

1. Incident Management Plan Introduction and Scope
2. Relationship to Business Continuity Planning
3. GPAA Strategy for Incident and Crisis Management
4. Invocation Authority and Method

   Summary of GPAA's Invocation Actions

   Summary of Incident Management BCP Invocation Actions

   BCP Invocation Actions Flowchart
5. Emergency Meeting Agenda
6. Outstanding Actions

The Invocation Plan outline for the BC Coordinator follows:

1. Summary of GPAA's Invocation Actions
2. High Level Incident Invocation Flowchart
3. BCP Invocation Actions Flowchart
4. Recovery Site Invocation Procedures
5. Resource List
6. Recovery Sequence Requirements – Situational Analysis
7. Additional Information about the BCPs
8. Resource Lists
   - 8.1 Battle Box Contents
   - 8.2 Emergency Disaster Finance
   - 8.3 Asset Register
   - 8.4 Emergency Equipment
9. Outstanding Actions
   - 9.1 Time Restrictions and Recovery Timeline
10. Business Continuity Plans Issued
11. Management Team Meeting Minutes Template
12. Control Sheet

8 BCM OFFICE REQUIREMENTS

The integrated BCM Management system allows costs to be defrayed enterprise wide, with a lesser direct cost implication to a single department. The budget table is linked to the strategy department.

8.1 BC MANAGER

The resident BC Manager for GPAA needs to be recruited and needs to have at least 5 years experience with either a ISO 22301 lead implementer certification or at an least AMBCI registration with the Business Continuity Institute. The manager shall report to the head of Strategy, Policy and BCM.

8.2 BCM BUDGET

The business continuity budget is within Cost Centre 71 – Management Support unit, whilst the BCM training budget is accommodated within the HR Development business unit.

The DR budget has been integrated into the ICT budget whilst the SHERQ budget remains the responsibility of the Facilities Management Unit.

8.3 BCM TRAINING PLAN

Training	Proposed date	Duration	Audience	Number of certifications
BCM Masterclass	8 November 2018	1 day	Chairperson BCC and National Forum	2
ISO 22301 lead Implementer	19-23 November 2018	5 days with certification	EXCO and BC Committee	22
ISO 22310 lead Auditor	4-9 February 2018	5 days with certification	Strategy and IA	4
BC Awareness	May 2019	4 Hour Awareness workshop	Head Office Staff	200 Attendees
BC Awareness	May 2019	Morning Awareness	Trevena Staff	60 Attendees
BC Awareness	February 2019	Morning Awareness	Bisho & Mthata Office	30 Attendees
BC Awareness	March 2019	Morning Awareness	Durban & PMB	30 Attendees
BC Awareness	June 2019	Morning Awareness	PE	15 Attendees
BC Awareness	July 2019	Morning Awareness	Kimberly	15 Attendees
BC Awareness	August 2019	Morning Awareness	Mmabatho	13 Attendees
BC Awareness	September 2019	Morning Awareness	Nelspruit	15 Attendees
BC Awareness	October 2019	Morning Awareness	Limpopo	15 Attendees
BC Awareness	November 2019	Morning Awareness	Cape Town	15 Attendees
BC Awareness	January 2020	Morning Awareness	Bloemfontein	15 Attendees

TABLE 2 - BCM TRAINING PLAN

9 RECOVERY

The recovery after invocation could happen in three phase:

1. Live online switchover on the MPLS to regional offices
2. Live transfer of the call centre to about 15 regional offices
3. VPN access via about 400 laptops
4. The WAR site to link via the MPLS as a pre-configured office with a VPN tunnel with a capacity of at least 200 desktop users

9.1 PROCESS

The recovery process is listed in sequence to ensure business capability and flexibility after invocation.

9.1.1 USER APPLICATION RECOVERY SEQUENCE OF ICT SYSTEMS

From the detail listed above, the following table depicts the actual required recovery sequence of the user systems as defined by the user's given RTO's of these systems.

	Interface	RTO	
1	AD	1	Hour
2	Internet	1	Hour
3	Call Centre	1	Hour
4	Backup solution recovery from cassette	2	Hour
5	Email	1	Hour
6	CIVPEN	1	Hour
7	Shared Drive	12	Hour
8	PCM	2	Hour
9	PORTAL	2	Hour
10	BPA	2	Hour
11	Printing service	2	Hour
12	ECM	2	Hour
13	PEKWA	2	Hour
14	Digital Signatures	2	Hour
15	Self Service	8	Hours
16	OBIEE	2	Hour
17	PERSAL / PERSOL	2	Hour
18	QMS	8	Hour
19	ABSA Interface	2	Hour
20	EDMS	2	Hour
21	Teammate	8	Hour
22	Security Vetting Information System	8	Hour
23	Actuarial Extractions	6	Weeks

TABLE 3 - USER APPLICATION RTO'S

9.2 RECOVERY SEATING AND ALTERNATE WORK AREA FACILITIES

From the information provided by the business units, during the business impact analysis meetings and workshops, the offsite seating required to recover critical business processes is detailed in the table below

Normal Staff Count	Seats Required	2 Hours	6 Hours	1 Day	2 Days	1 Week	1 Month and Longer
(GPAA) 1181 (GEPF) 64	188	61	92	124	126	188	188

TABLE 4 - WORK AREA RECOVERY SEAT REQUIREMENT

9.3 DESKTOP SYSTEM REQUIREMENT BY PROGRAMME

Service	1.1 Corporate Services	1.2 Finance	1.3 Business Enablement	1.4 Strategic support	1.5 Governance	2.1 Civil Pensions	2.2 EB	2.3 CRM
Windows 10 Pro	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS Office Pro 2016	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Outlook 2016	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Visio 2016	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RightFax	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS Project 2016	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mindjet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Attachmate	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AccPac	Yes	Yes		Yes				
VRM		Yes		Yes				
Eworkflow	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Citrix			Yes			Yes	Yes	Yes
PERSAL	Yes	Yes						
BAS	Yes	Yes	Yes			Yes		
ABSA							Yes	
BI		Yes	Yes	Yes		Yes	Yes	Yes
Portal		Yes	Yes			Yes	Yes	Yes
PCM		Yes	Yes			Yes	Yes	Yes
Shared Drive	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Equitrac								
CIVPEN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CIVPEN – DR	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
FTP Link Icon		Yes	Yes			Yes	Yes	Yes
KASEYA Self Service	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPN Access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CISCO Anyconnect	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ODS Tax	Yes	Yes	Yes				Yes	
McAfee	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Teammate			Yes	Yes	Yes			
Equate	Yes							
OrgPlus	Yes							
Barnowl					Yes			
Aris			Yes					
ITC		Yes					Yes	
DoHA		Yes	Yes			Yes	Yes	
Easyfile		Yes						
Adobe (Reader)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Firefox	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Edge	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Google Chrome	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Call Centre CIC			Yes					Yes
ACL					Yes			
Safety Web		Yes	Yes					

TABLE 5 - DESKTOP APPLICATION RECOVERY REQUIREMENT

9.4 THE RECOVERY POINT AND TIME OBJECTIVES

Application	RPO	Programme / Process
ABSA Interface	N/A	Sub Programme 2.2: Electronic Contributors
	N/A	Sub Programme 2.2: Manual Contributors
	N/A	Sub Programme 2.2: Additional Liabilities
Payment Services	60 Seconds	Sub Programme 2.2: Business Support Services
Accpac accounting	24 Hours	Sub Programme 1.2: Budgeting And Reporting
	24 Hours	Sub Programme 1.3: Applications
	24 Hours	Sub Programme 2.1: Support Services
	60 Seconds	Sub Programme 2.2: Additional Liabilities
Actuarial Extractions	24 Hours	Sub Programme 1.3: : Modernisation
ARIS	24 Hours	Sub Programme 1.5: Enterprise Wide Risk Management
Barn Owl	60 Seconds	Sub Programme 2.1: Medical Benefits
BAS	24 Hours	Sub Programme 2.1: Military Pensions
	24 Hours	Sub Programme 2.1: Support Services
	24 Hours	Sub Programme 1.3: Applications
Benefit Calculator/Excel based	24 Hours	Sub Programme 1.1 Physical Security
CCTV	24 Hours	Sub Programme 2.3: Quality Assurance
Call Centre Services	24 Hours	Sub Programme 2.3: Call Centre
	24 Hours	Sub Programme 2.3: CRM – Regional Offices
	24 Hours	Sub Programme 2.1: Military Pensions
Cisco Telephony	24 Hours	Sub Programme 1.3: Applications
PEKWA, Scanning, Indexing and Workflow	24 Hours	Sub Programme 2.3: OSS – Inbound
	24 Hours	Sub Programme 2.3: OSS – Indexing
	24 Hours	Sub Programme 2.3: Call Centre
Civpen	1 Hour	Sub Programme 2.2: Business Support Services
	60 Seconds	Sub Programme 1.2: Investment Accounting
	24 Hours	Sub Programme 1.2: Debtors
	24 Hours	Sub Programme 1.2: Employee Benefits
	24 Hours	Sub Programme 1.2: Taxation
	24 Hours	Sub Programme 2.1: Special Pensions
	24 Hours	Sub Programme 2.3: CRM – Regional Offices
	24 Hours	Sub Programme 2.1: Injury on Duty
	24 Hours	Sub Programme 2.1: Medical Benefits
	24 Hours	Sub Programme 2.1: Military Pensions
	24 Hours	Sub Programme 1.5: Legal Support
	24 Hours	Sub Programme 1.2: Cash Flow Management
	24 Hours	Sub Programme 2.3: Quality Assurance
	24 Hours	Sub Programme 2.3: OSS – Indexing
	24 Hours	Sub Programme 1.2: Unclaimed and Re
	24 Hours	Sub Programme 1.5: Forensic and Fraud Prevention
	24 Hours	Sub Programme 2.2: Special Projects
	24 Hours	Sub Programme 2.2: Membership
	24 Hours	Sub Programme 2.2: Withdrawals
	24 Hours	Sub Programme 2.2: Funeral Benefits
	24 Hours	Sub Programme 2.2: Pensioner Maintenance
	24 Hours	Sub Programme 2.2: Manual Contributors
	24 Hours	Sub Programme 2.2: Additional Liabilities

	24 Hours	Sub Programme 2.2: Electronic Contributors
	24 Hours	Sub Programme 2.1: Support Services
	24 Hours	Sub Programme 1.1 Physical Security
Physical Access Control	8 Hours	Sub Programme 2.1: Special Pensions
ITC Interface	8 Hours	Sub Programme 1.5: Legal
	8 Hours	Sub Programme 2.2: Special Projects
	8 Hours	Sub Programme 2.2: Withdrawals
	8 Hours	Sub Programme 2.2: Membership
	8 Hours	Sub Programme 2.2: Special Projects
	8 Hours	Sub Programme 2.2: Pensioner Maintenance
	8 Hours	Sub Programme 2.2: Business Support Services
	8 Hours	Sub Programme 2.2: Funeral Benefits
	8 Hours	Sub Programme 1.2: Unclaimed and Re
	24 Hours	Sub Programme 1.2: Taxation
Email	24 Hours	Sub Programme 1.3: Information Security
	24 Hours	Sub Programme 2.3: OSS – Inbound
	24 Hours	Sub Programme 1.2: Investment Accounting
	24 Hours	Sub Programme 1.2: Cash Flow Management
	24 Hours	Sub Programme 1.2: Employee Benefits
	2 Hours	Sub Programme 1.5 Secretariat
	24 Hours	Sub Programme 1.3: Infrastructure
	24 Hours	Sub Programme 2.2: Business Support Services
	24 Hours	Sub Programme 1.2: Debtors
	24 Hours	Sub Programme 2.1: Special Pensions
	24 Hours	Sub Programme 2.1: Injury on Duty
	24 Hours	Sub Programme 2.1: Medical Benefits
	24 Hours	Sub Programme 2.1: Military Pensions
	24 Hours	Sub Programme 1.5: Legal
	24 Hours	Sub Programme 2.3: CRM – Regional Offices
	24 Hours	Sub Programme 2.3: Quality Assurance
	24 Hours	Sub Programme 2.3: Trevena C Centre
	24 Hours	Sub Programme 1.3:Management Information Services
	24 Hours	Sub Programme 1.4 Monitoring and Evaluation
	24 Hours	Sub Programme 1.3:Quality Management
	24 Hours	Sub Programme 1.3: Projects Management Office
	24 Hours	Sub Programme 1.4: Communication Services
	24 Hours	Sub Programme 1.5: Internal Audit
	24 Hours	Sub Programme 1.4: Strategy and Policy
	24 Hours	Sub Programme 1.2: Unclaimed and Re – Issues
	24 Hours	Sub Programme 1.1 Human Resource Administration
	24 Hours	Sub Programme 1.1 Organisational Design and Development
	24 Hours	Sub Programme 1.1 Labour Relations
	24 Hours	Sub Programme 1.1 Employee Health and Wellness
	24 Hours	Sub Programme 1.3: Knowledge Management
	24 Hours	Sub Programme 2.1: Support Services
	24 Hours	Sub Programme 2.3: OSS – Indexing
	24 Hours	Sub Programme 1.1 Physical Security
	24 Hours	Sub Programme 1.1 Facilities
	24 Hours	Sub Programme 1.1 Change Management
	24 Hours	Sub Programme 1.5: Forensic and Fraud Prevention
	24 Hours	Sub Programme 2.2: Funeral Benefits
	24 Hours	Sub Programme 2.2: Special Projects
	24 Hours	Sub Programme 2.2: Pensioner Maintenance
	24 Hours	Sub Programme 2.2: Membership
	24 Hours	Sub Programme 2.2: Manual Contributors
	24 Hours	Sub Programme 2.2: Withdrawals

	24 Hours	Sub Programme 1.2: Budgeting And Reporting
	24 Hours	Sub Programme 1.5: Enterprise Wide Risk Management
	24 Hours	Sub Programme 1.3: Applications
	24 Hours	Sub Programme 1.2: Supply Chain Management
	24 Hours	Sub Programme 2.2: Electronic Contributors
	24 Hours	Sub Programme 1.1 Training
	24 Hours	Sub Programme 1.1 Physical Security
Employers Profile and Vetting	24 Hours	Sub Programme 1.1 Physical Security
Fire Communication System	12 Hours	Sub Programme 1.2: Cash Flow Management
FTP Server	12 Hours	Sub Programme 2.2: Business Support Services
	12 Hours	Sub Programme 1.2: Debtors
	12 Hours	Sub Programme 1.2: Employee Benefits
	12 Hours	Sub Programme 1.2: Taxation
	12 Hours	Sub Programme 2.1: Military Pensions
	12 Hours	Sub Programme 2.2: Membership
	12 Hours	Sub Programme 2.2: Withdrawals
	12 Hours	Sub Programme 2.2: Manual Contributors
	12 Hours	Sub Programme 2.2: Additional Liabilities
	12 Hours	Sub Programme 2.2: Electronic Contributors
	N/A	Sub Programme 1.3: Applications
Home Affairs Interface	N/A	Sub Programme 2.1: Special Pensions
	N/A	Sub Programme 1.5: Legal
	N/A	Sub Programme 2.2: Business Support Services
	N/A	Sub Programme 1.2: Debtors
	N/A	Sub Programme 1.5: Forensic and Fraud Prevention
	N/A	Sub Programme 2.1: Injury on Duty
	N/A	Sub Programme 2.1: Medical Benefits
	N/A	Sub Programme 2.1: Military Pensions
	N/A	Sub Programme 2.2: Special Projects
	N/A	Sub Programme 2.2: Membership
	N/A	Sub Programme 2.2: Withdrawals
	N/A	Sub Programme 2.2: Funeral Benefits
	N/A	Sub Programme 2.2: Pensioner Maintenance
	N/A	Sub Programme 1.2: Unclaimed and Re
	N/A	Sub Programme 2.2: Business Support Services
	24 Hours	Sub Programme 1.1 Physical Security
Access Control System	N/A	Sub Programme 1.2: Cash Flow Management
Internet for PCM	N/A	Sub Programme 1.2: Investment Accounting
	N/A	Sub Programme 1.2: Employee Benefits
	N/A	Sub Programme 1.3: Knowledge Management
	N/A	Sub Programme 2.1: Medical Benefits
	N/A	Sub Programme 1.3: Projects Management Office
	N/A	Sub Programme 1.4: Communication Services
	N/A	Sub Programme 1.3:Quality Management
	N/A	Sub Programme 2.1: Military Pensions
	N/A	Sub Programme 1.1 Training
	N/A	Sub Programme 2.2: Manual Contributors
	N/A	Sub Programme 2.2: Additional Liabilities
	N/A	Sub Programme 2.2: Electronic Contributors
	24 Hours	Sub Programme 1.4: Communication Services
Intranet	24 Hours	Sub Programme 2.2: Business Support Services
	24 Hours	Sub Programme 1.3:Quality Management
	24 Hours	Sub Programme 2.1: Medical Benefits
MIS	24 Hours	Sub Programme 2.2: Special Projects
Oracle BI (Web based)	24 Hours	Sub Programme 2.2: Membership
Oracle BIEE	24 Hours	Sub Programme 2.2: Funeral Benefits

	24 Hours	Sub Programme 2.2: Pensioner Maintenance
	24 Hours	Sub Programme 2.2: Membership
	24 Hours	Sub Programme 2.2: Withdrawals
	24 Hours	Sub Programme 1.3: Applications
	24 Hours	Sub Programme 1.3:Management Information Services
	24 Hours	Sub Programme 1.3: Applications
	24 Hours	Sub Programme 1.2: Taxation
ODS – Tax Directives service	1 Hour	Sub Programme 2.2: Business Support Services
Oracle Portal	24 Hours	Sub Programme 2.3: CRM – Regional Offices
	24 Hours	Sub Programme 2.3: OSS – Indexing
	24 Hours	Sub Programme 2.2: Special Projects
	N/A	Sub Programme 2.3: Call Centre
	24 Hours	Sub Programme 2.3: C Centre
Pekwa	1 Hour	Sub Programme 2.2: Business Support Services
	24 Hours	Sub Programme 1.2: Debtors
	24 Hours	Sub Programme 1.2: Employee Benefits
	24 Hours	Sub Programme 1.2: Unclaimed and Re
	24 Hours	Sub Programme 2.3: OSS – Inbound
	24 Hours	Sub Programme 2.3: CRM – Regional Offices
	24 Hours	Sub Programme 1.2: Taxation
	24 Hours	Sub Programme 2.1: Injury on Duty
	24 Hours	Sub Programme 2.1: Medical Benefits
	24 Hours	Sub Programme 1.5: Legal Support
	24 Hours	Sub Programme 1.5: Forensic and Fraud Prevention
	24 Hours	Sub Programme 2.1: Military Pensions
	24 Hours	Sub Programme 2.2: Membership
	24 Hours	Sub Programme 1.1 Physical Security
	24 Hours	Sub Programme 2.2: Special Projects
	24 Hours	Sub Programme 2.2: Withdrawals
	24 Hours	Sub Programme 2.2: Funeral Benefits
	24 Hours	Sub Programme 1.3: Applications
	24 Hours	Sub Programme 2.2: Pensioner Maintenance
	24 Hours	Sub Programme 2.2: Funeral Benefits
	24 Hours	Sub Programme 2.2: Pensioner Maintenance
	24 Hours	Sub Programme 2.2: Manual Contributors
	24 Hours	Sub Programme 2.2: Additional Liabilities
	24 Hours	Sub Programme 2.2: Electronic Contributors
	N/A	Sub Programme 1.1 Human Resource Administration
PERSAL	N/A	Sub Programme 1.1 Training
	FTP	Sub Programme 2.2: Electronic Contributors
	24 Hours	Sub Programme 2.3: Travena C Centre
RightFax	24 Hours	Sub Programme 2.1: Special Pensions
	24 Hours	Sub Programme 2.3: Quality Assurance
	24 Hours	Sub Programme 2.2: Funeral Benefits
	24 Hours	Sub Programme 2.2: Pensioner Maintenance
	24 Hours	Sub Programme 1.3: Applications
	24 Hours	Sub Programme 1.2: Cash Flow Management
Safety Web	24 Hours	Sub Programme 1.3: Applications
	24 Hours	Sub Programme 2.2: Business Support Services
	24 Hours	Sub Programme 2.2: Additional Liabilities
	24 Hours	Sub Programme 2.2: Electronic Contributors
	24 Hours	Sub Programme 2.2: Manual Contributors
	24 Hours	Sub Programme 1.2: Taxation
SARS Services	24 Hours	Sub Programme 2.1: Taxation
	24 Hours	Sub Programme 2.2: Taxation

	24 Hours	Sub Programme 1.3: Applications
	24 Hours	Sub Programme 2.1: Medical Benefits
	24 Hours	Sub Programme 2.2: Business Support Services
	24 Hours	Sub Programme 1.3: Information Security
Share Point	24 Hours	Sub Programme 1.3: Projects Management Office
Shared Drive	24 Hours	Sub Programme 1.4: Strategy and Policy
	24 Hours	Sub Programme 1.2: Cash Flow Management
	1 Hour	Sub Programme 2.2: Business Support Services
	24 Hours	Sub Programme 2.3: OSS – Inbound
	24 Hours	Sub Programme 1.2: Investment Accounting
	24 Hours	Sub Programme 1.2: Debtors
	24 Hours	Sub Programme 1.2: Employee Benefits
	24 Hours	Sub Programme 1.4: Communication Services
	24 Hours	Sub Programme 1.3: Knowledge Management
	24 Hours	Sub Programme 1.3: Infrastructure
	24 Hours	Sub Programme 2.3: CRM – Regional Offices
	24 Hours	Sub Programme 1.2: Budgeting And Reporting
	24 Hours	Sub Programme 2.1: Special Pensions
	24 Hours	Sub Programme 1.5: Legal Support
	24 Hours	Sub Programme 2.1: Military Pensions
	24 Hours	Sub Programme 1.4 Monitoring and Evaluation
	24 Hours	Sub Programme 1.3: Projects Management Office
	24 Hours	Sub Programme 1.2: Taxation
	24 Hours	Sub Programme 2.3: OSS – Indexing
	24 Hours	Sub Programme 2.3: Quality Assurance
	24 Hours	Sub Programme 1.4: Strategy and Policy
	24 Hours	Sub Programme 1.2: Unclaimed and Re
	24 Hours	Sub Programme 2.2: Membership
	24 Hours	Sub Programme 2.2: Withdrawals
	24 Hours	Sub Programme 2.2: Special Projects
	24 Hours	Sub Programme 1.3:Quality Management
	24 Hours	Sub Programme 2.2: Funeral Benefits
	24 Hours	Sub Programme 2.2: Pensioner Maintenance
	24 Hours	Sub Programme 2.2: Electronic Contributors
	24 Hours	Sub Programme 2.2: Manual Contributors
	24 Hours	Sub Programme 2.2: Additional Liabilities
	24 Hours	Sub Programme 1.4: Communication Services
SMS Gateway	N/A	Sub Programme 2.2: Electronic Contributors
Transversal Systems (SANDF, SARS, SASSA and RTMC)	N/A	Sub Programme 2.2: Additional Liabilities

TABLE 6 - RPO OF APPLICATIONS

10 BC EXERCISES AND MAINTENANCE

The business continuity testing and resilience improvement is subject to continuous improvement through the methodology and practice of at least twice per annum.

10.1 METHODOLOGY

The methodology for testing increasing organisational resilience is depicted in Figure 7 - Period model

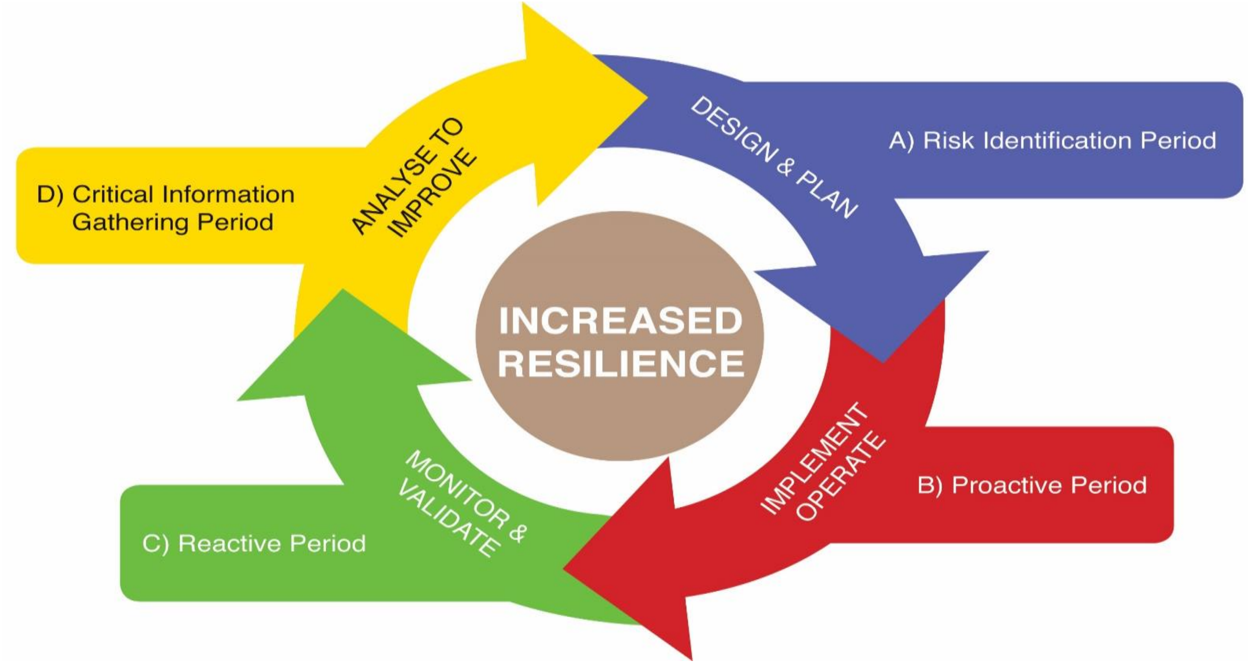

FIGURE 7 - PERIOD MODEL

- *Understanding the business period:* Strategic risks are identified in the exploitation cycle as opportunities for resilience. These could be in any area of concern, ie possible epidemics, man-made or natural disasters, system or service failures, etc. A full business impact analysis can be done at this stage to understand the business.
  - *Design and plan:* Mitigating strategies are planned, even if the incident has never occurred. Scenarios should be developed to come up with best strategies.
  - *Do and implement:* The strategies should be implemented as managed projects in the conservation cycle; this includes the project management principles of cost, quality and time.
- *Proactive period:* The resilience cycle should be accompanied by milestones and testing. This intersects with the business continuity life cycle where testing and maintenance take place.
- *Reactive period:* This period is concerned with reacting to an event, whether by practice or by specific incident. In this period, a disaster can be declared if the system can recover by resilient means.
  - *Act:* The incident or disaster occurs and the incident management plan is utilised as tested in the project. This will minimise loss and prove the elasticity of the engineered system, process or technology.
  - *Validate:* The reactive process may in itself be accompanied by reactive measures that may not be documented at all. The more mature GPAA, the more undocumented reactions with good outcomes will be experienced at this stage

- *Gathering information and evidence period:* The evidence-based approach makes information-gathering more complex, but leaves an audit trail for making informed decisions and corrections at a later date.
  - — *Evaluate:* The post-event reorganisation is likely to be slow and requires a robust evaluation process. This phase is one of identifying the lessons from the incident or disaster and will probably be placed in institutional memory. In the event of another disaster, institutional memory may cause a different, more mature reaction.
  - — *Analyse:* Reorganisation requires an immense amount of energy for analysing. This will, of course, vary with the intensity of the incident or disaster. The reorganisation process places a burden on emotion, human and financial resources.

10.2 DESKTOP SCENARIO

The purpose of a desktop scenario is to test the BCP without disrupting normal business and to ensure readiness should a disruption occur. The GPAA's approach to completing the BCP desktop scenarios is effected by:

- A surprise BCM incident announcement
- Planned Facilitation for the execution of the desktop scenario includes:
  - ➢ A set scenario for the reported incident,
  - ➢ Identification, notification and scheduling of appropriate personnel
  - ➢ A facilitated walk-through of the scenario, along with discussions on Business Continuity Plan actions and responsibilities
  - ➢ Capturing of desktop scenario notes, including issues and areas for changes/additions to the BCP documents,
  - ➢ Assignment of responsibilities for BCP update work,
  - ➢ Closing discussions.

Following the conclusion of the desktop scenario, the facilitator and participants should discuss issues and comments relevant to the status of the business continuity plans. The business process managers retain ownership and responsibility for ensuring that appropriate changes and updates to the Business Continuity Plans are implemented.

The desktop Scenario may take place in a business unit, on sub-programme or Programme level, eve at a regional office. An Ideal way for M&E to test the BCM plans for each business unit.

10.3 LIVE RECOVERY

The heavy reliance that GPAA business has on its ICT systems and infrastructure makes its recoverability and availability of paramount importance. To ensure live recoverability and reliability there shall be alternate Data Centres and Recovery Site/Work Area Recovery.

Live recovery shall be accomplished by replicating the Oracle Supercluster data over a Multiprotocol Label Switching (MPLS) link from the Hamilton Street Data Centre to the Gallo Manor data center in Sandton. The Mainframe component shall be replicated at the BCX site in Midrand.

The Work Area Recovery (WAR) shall be hosted by a service provider with a single 50Mbps internet link from Gallo Manor with WAR seats connecting directly over the open internet to ensure a live working environment. There shall be MPLS connection from the WAR to allow for seamless transfer of live services.

Both these replications shall be tested annually.

An alternate method of work area recovery shall be made available via the eleven mobile vans. Each van should accommodate about 20 users on either a satellite connection to Gallo Manor, or a VPN tunnel connection through the 3G network. This alternative should allow for about 260 connections nationally.

10.4 HYBRID

The GPAA shall conduct disaster recovery/live recovery exercises guided by various desktop scenarios where different business units in unity test the reliability of the replica data centers at the WAR Centre. The scope shall include testing the WAR Centre level full functionality of all the systems that enable them to conduct their daily activities.

A typical live recovery exercise shall focus on the ability of the server (host) level recovery to adequately ensure a complete recovery of the applications without any inconsistencies among various interdependent subcomponents. Post the exercise feedback by business units representatives shall include realistic readiness status and overall recovery time objective (RTO) for multiple applications at the WAR center.

Live recovery exercises to test the reliability of the replica data centres shall be conducted twice a year at the head office, and also the regional offices.

11 STRATEGIC BCM SCORECARD

Objective	Disastrous Risk	Business Area	Performance indicator	Baseline	Target 2018/19	Q1/Q2	Q3/Q4	Achievement 2018/19
To manage disruptive incidents without calling for recovery invocation	Inability to do business after a disruptive incident	Head Office	% of disruptive incidents and DR Tests managed without invocation	90%	91%	100%	98%	99%
To ensure recovery within the Maximum Tolerable time of Disruption (MTTD)	Inability to recover from a disruptive incident within the MTTD	Head Office and Provincial offices	% of disruptive incidents and DR tests managed within MTTD	95%	98%	90%	100%	95%
To ensure recovery of systems within the required RTO	Inability to recover from a disruptive incident within the required RTO	Head Office and Provincial offices	% of disruptive incidents and DR tests managed within RTO	95%	98%	85%	100%	92%
To ensure recovery of systems within the required RPO	Inability to recover from a disruptive incident within the required RPO	Head Office and Provincial offices	% of disruptive incidents and DR tests managed within RPO	95%	98%	75%	100%	83%
To ensure instil an enterprise wide BC culture	Recovery and incident management failing due to staff matters	Head Office and Provincial offices	Number of awareness and training sessions	1 at head office 0 at regional offices	2 at head office 8 at regional offices	1 at head office 3 at regional offices	1 at head office 5 at regional offices	2 at head office 8 at regional offices
To ensure risk practitioners are suitable certified in BCM	Risk practitioners cannot manage incidents in line with BCM standards	Head Office and Provincial offices	Number of certified BCM practitioners and auditors in GPAA	0 EXCO 1 MANCO 10 Operations	3 EXCO / RMC 10 MANCO / RISK 10 OPERATIONS	2 EXCO / RMC 4 MANCO / RISK 6 OPERATIONS	2 EXCO / RMC 6 MANCO / RISK 12 OPERATIONS	4 EXCO / RMC 10 MANCO / RISK 18 OPERATIONS

TABLE 7 - BCM SCORECARD