

RISK COMMITTEE SUBMISSION - BUSINESS CONTINUITY

**Date:** Tuesday, 09 July 2019 **Tel:** 012 319 1197

**Contact Person:** Dr Ferguson **Fax:** 012 319 3578

**Division:** Strategy, Policy and BCM **Email:** ferguson.clifford@gpaa.gov.za

**Room No:** D205

**Ms. A. BADIMO**

**CHAIRPERSON**

**RISK COMMITTEE**

**GPAA**

Herewith the BC report in the month of March 2019, Q4, as presented to the Risk Committee of the GPAA. The BC Committee overseas three important components of Business continuity namely:

* The business continuity lifecycle;
* DR and BC Testing and
* Oversight of four sub-committees namely: The Damage Assessment Committee, the SHERQ committee, the Business Recovery Committee and the Technology recovery committee that seeks to conform to international disaster recovery (DR) standards.

**Disaster Recovery risk mitigation**

To mitigate the systems recovery risk of core business the GPAA has the following DR solutions in place**:**

1. The contract for the Work Area Recovery site of GPAA has been re-introduced at Continuity South Africa (CSA) as on 1 May 2019 through a renewed order sanctioned by SITA. The contract renewal was delayed due to a legal opinion that was required.
2. Mainframe DR site with direct replication is at IBM Randburg, renewed in 2018.
3. Oracle and Open Infrastructure DR site with direct replication is at MTN Galo Manor, Sandton
4. Tape drive back-up 3rd level DR.
5. A Mobile van solution, to accommodate about 25 users linked via 4G to either of the data centres, primary at 34 Hamilton Street, or secondary at Galo Manor. The solution allows for work area recovery at school halls, hotels or even a tent. The solution was tested in Worcester
6. Call centre overflow to regional offices via the redundant wide area network.
7. A call centre to be built at 40 Church Street, of about 60 seats. Shared capacity with National Treasury. A project manager has been appointed and will be working directly with National Treasury ICT and Facilities management for the build.

**Business Continuity risk mitigation**

The risk of not being able to continue with business after a hazardous or disastrous event, is mitigated by four separate sub-committees of the BC Committee. The SHERQ committee for the people and infrastructure management, Damage Assessment Committee, for ad-hoc damage assessment. The Business Recovery committee, determines work area, workflow and process commitments while the Systems Recovery committee ensures ICT and systems recovery though DR management. It has been decided to re-appoint and retrain the committees to ensure effective compliance with the OHS Act and ISO 22301.

The BC activities for the past year are tabulated in Table 1- BC Activity

.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Description** | **2018/19 (Q4)** | **2019/20 (Q1)** | **2019/20 (Q2)** | **2019/20 (Q3)** |
| **Business Continuity (BC) Training** | Five ISO 22301 Lead auditors to be trained  SHERQ – OHS training Fire, First Aid and Evacuation | BC ISO 22301 certification for branch managers  BC Awareness week | ISO Lead auditor training |  |
| **Determined scenario (BC)** | Cape Town Water & Sanitation Scenario | Scenario developed CSA test – 19 June 2019 | Regional Office test KZN – 7August 2019 | Scenario developed CSA test – 24 October 2019 |
| **BC Documentation produced** | BC Programme plan 2019-2021  ToR BCC review  Business Recovery committee appointment | Business unit DR Plans by 30 June 2019 |  |  |
| **Conduct  BC & DR test** | 26-27 February 2019 Worcester, WC  Evacuation test | Scenario developed CSA test  Evacuation test – 17 June 2019 | Regional Office test KZN  Evacuation test – 6 August 2019 | Scenario developed CSA test  Evacuation test – 23 October 2019 |
| **Report BC test results** | Audit finding resolutions February 2018 test | M&E and audit report | M&E and audit report | M&E and audit report |

Table 1- BC Activity

**Vacancy**

The vacancy still exists for the BC manager.

**Business Continuity Risk Register**

It is recommended that the GPAA BIA identified risks be listed in the Barn-Owl system to ensure that these are monitored and mitigated significantly, see Table 2 - BIA Risks.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Risk / Incident Topic** | **Recommendation – Brief Commentary** | **Exposure to:** | **P** | **I** | **RATING** | **Ownership** |
| 1 | **BCM Programme** | Access and URL details for logon to systems – if users are not at their own workstations with pre-loaded links and software, the access details are unknown and as a result user could not access remote systems. These details need to be incorporated into their BCP’s | Unable to access systems | 1 | 3 | 3 | Business Support Services / Information Security |
| 2 | Need pre-prepared media scripts for scenarios as well as scripts for Call Centre | Poor Media Communications | 3 | 3 | 9 | Communication Services |
| 3 | No formal invocation process involving the Communications team in the event of an incident | Poor Communications | 2 | 3 | 6 | Communication Services |
| 4 | No Recovery Site Work Are Recovery | Unable to Recover | 1 | 4 | 4 | ICT Business Unit |
| 5 | Business Continuity Management | The inability to manage and /or recover business critical operations within an acceptable time frame and thus negatively affect GPAA’s wellbeing, and possibly its continued existence. | 1 | 4 | 4 | Business Continuity Committee |
| In the event of an incident that affects the normal operation of critical business functions, for any reason, there is no strategy or plans in place to ensure the business can still function. |
| Corporate Governance standards, such as King IV in South Africa, recommend that companies have a tested Business Continuity Management programme in place as part of Enterprise Risk Management. |
| 6 | Off-site Work Area | Loss of workspace for staff to operate from | 2 | 4 | 8 | Information Security |
|
| 7 | Incident/Crisis Management | The inability to manage crises to ensure the best possible outcome for GPAA. | 1 | 4 | 4 | Business Continuity Committee |
| Incident/Crisis Management is a vital aspect of Business Continuity. |
| Not all incidents are operationally related; however, each incident must be managed and addressed timeously to ensure minimum negative impact on an organisation. |
| Note: Effective and rapid management of a crisis is the significant factor in protecting an organisation’s brand from financial and reputational damage. |
| It is recommended that an Incident/Crisis Management structure be implemented and integrated within this BCM programme to ensure incidents are managed and, if required, recovery invoked to ensure minimal negative impact to GPAA |
| 8 | Validity of Recovery Times | Inability to provide core services within acceptable time frames | 1 | 2 | 2 | ICT BU |
| The RTO’s provided by business have not been tested and thus are inaccurate indications of the acceptable downtime for the critical business processes. Testing of processes and their respective RTOs to prove their validity. |
| 9 | **Power** | No Second Generator | Loss of Failover power | 3 | 4 | 12 | Facilities Management |
| 10 | No alerts or alarms for UPS system as well as no history of testing of the batteries - no maintenance history available | Loss of UPS | 3 | 4 | 12 | Facilities Management |
| Automated systems need to be implemented as well as a full maintenance schedule enforced |
| 11 | The integrity of the Electrical reticulation and infrastructure is somewhat unknown and not documented. | Ineffective Maintenance | 2 | 3 | 6 | Facilities Management |
| 12 | Management of Power, AC and Access controlled by Infrastructure with uncertain maintenance and repair SLAs | Loss of facilities in an incident and the inability to repair and maintain this infrastructure within acceptable time frames | 3 | 3 | 9 | Facilities Management / ICT BU |
| The Management of Power, AC and Access are controlled by Infrastructure and yet the dependency ICT has on this is critical – closer interaction and the mutual agreement of SLAs need to be enforced as well as documented maintenance and testing implemented. |
| 13 | The amount of onsite diesel for the generators is unknown and as such the duration the generators can run in an incident is also unknown. It is also unclear where the additional fuel will be sourced and how much will be made available | Loss of fuel to operate the standby power units | 2 | 3 | 6 | Facilities Management |
| Sufficient diesel for the generator should be available as well as a published plan on where and how additional fuel can be provided |
| 14 |  | Five of the regions do not have generator or UPS power and as such cannot conduct their business when the city power is unavailable. SLA’s with Landlords should ensure the provision of this facility | Loss of service | 3 | 3 | 9 | Facilities management |
| 15 | **Building Evacuation** | Are assembly points adequate for an evacuation involving Hazmat - there are none outside the premises. Look at alternatives | Inefficient Evacuation | 3 | 2 | 6 | Employee Wellness / Facilities Management |
| 16 | Emergency Exits and Access - emergency exits and access routes must be clear of obstacles such as rubbish, packaging, boxes, old computers and the like. Access routes for emergency vehicles to get to the generator and transformers are blocked by staff vehicles. | Injury and the inability to evacuate timeously | 4 | 4 | 16 | Facilities Management / Physical Security |
| Clear emergency passages and routes of hindering blockages | OSS |
| 17 | Stores Area F 01 -Emergency exit keys are kept in the office of supervisor and would not necessarily be available in the event of an evacuation | Inefficient Evacuation | 2 | 3 | 6 | Facilities Management / Physical Security |
| 18 | How do we know who is in the building still and unaccounted members - how do we track where they are – an automated roll call off biometrics must be developed | Loss of People | 4 | 3 | 12 | ICT / Physical Security / Human Resources |
|
| 19 | Effective emergency communication methods need to be implemented – this can be via IP Phones or via a traditional Loudhailer system. Intercom system to be installed as a backup to the IP phone system so that it can be used in an emergency | Poor Communications | 3 | 4 | 12 | Facilities Management / Employee Wellness / Physical Security / ICT |
| 20 | **Physical Security** | The City Power transformer rooms are unlocked and unauthorized access to these is easily possible which could lead to sabotage rendering the building without power. | Sabotage or Damage | 1 | 3 | 3 | Facilities Management / Physical Security |
| 21 | DB Box’s left open and unlocked in corridors | Loss of Power | 2 | 3 | 6 | Facilities Management / Physical Security |
| 22 | Stores Area F 01 -Computer network room was not locked | Interference and loss of systems | 2 | 3 | 6 | Facilities Management / Physical Security /ICT |
| 23 | **Hamilton Street Data Centre** | There is no environmental monitoring which can be measured and monitored remotely evident – air conditioners and server room limits will not be monitored if there are no people involved. | Loss of Systems | 3 | 4 | 12 | Facilities Management |
| 24 | Air conditioners do not have an alarm / SMS alerting system to notify of temperature fluctuations – establish the remote and automatic environmental monitoring system | Loss of Cooling | 4 | 4 | 16 | Facilities Management / ICT |
| 25 | Gas Bottle and storage Area **- w**ater sprinkler in gas room – not known if it works - request maintenance records and conduct tests. | Loss of Facilities | 2 | 3 | 6 | Facilities Management / ICT |
| Not known if gas bottles are functional or full – no records of tests conducted are available – ensure the regular testing and maintenance of these assets. |
| 26 | Emergency Exit – this passage is in need of clearing as there are boxes of paper and other items such as old furniture and computers lying around – this is fire risk as well as an evacuation hazard. | Inefficient Evacuation | 4 | 3 | 12 | Facilities Management / ICT |
| The door lock needs correct access control as it currently has a bolt locking mechanism. |
| 27 | Environmental Issues | Loss of Network | 3 | 4 | 12 | Facilities Management |
| Air-conditioning insufficient for two servers / cabinets – overheating possibility. Correct cooling should be ensured in each room |
| Cable for outside air-conditioner unit runs through open window |
| No dust extractors or environmental controls / alarms – including no fire detectors, fire suppressants |
| Insufficient lighting in rooms |
| No sunshield or tinting on glass – exposure to damage from sun as well as possible overheating |
| 28 | **EOH and Outsourced Recovery Sites** | MPLS is owned by MTN – Open tender process underway | WAN Disruption | 1 | 4 | 4 | ICT |
| 29 | Some of the devices at Gallo Manor are single points of failure with respect to the WAN and connectivity from the regions and Head Office | WAN Disruption | 1 | 4 | 4 | ICT |
| 30 | Total reliance on external vendor and this contract is not being renewed, this leaves the organisation vulnerable to no ICT support both from an IP view as well as the vast outsourced hardware at the various sites managed by EOH – Open tender process underway | Loss of ICT Support | 1 | 4 | 4 | ICT |
|
| 31 | **Key Supplier Dependency** | Key product supply disruption in the event of key suppliers’ failure to honour their obligation to provide GPAA with product due to disasters affecting their own sites. | 2 | 4 | 8 | ICT / Supply Chain Management |
| GPAA has a dependency on key suppliers– advice from the BCI’s BCM Good Practice Guidelines on selecting appropriate tactical recovery options for the loss of suppliers include: |
| ·    Dual or multi-sourcing of supplies |
| ·    Identification and pre-acceptance of alternative suppliers |
| ·    Contractual obligations on the supplier to implement BCM |
| ·    Inspection of the supplier’s BCM capability, which should include evidence of successful exercises |
| ·    Holding spare or buffer inventories |
| ·    Significant penalty clause on supply contracts. |
| 32 | Dependency on hard copy documentation – no payments are made on any electronic documents, this opens the door to potential fraud as the controls around hard copy are more difficult to manage than a proper workflow process | Inability to provide a service | 2 | 4 | 8 | ICT / EB Operations and Finance / Civil and Military Pensions |
| 33 | The risk of losing data due to the scanning of archives only being done at the end of the document cycle is much higher – the original source documents may be lost or destroyed at any point during this process. Physical files will be a single point of failure as there is a huge dependency on these in the day to day activities | Inability to provide a service | 2 | 3 | 6 | OSS / ICT / EB Operations and Finance / Civil and Military Pensions |
| 34 | Supply Chain Management - procurement documents are filed and not scanned electronically | Loss of Information | 3 | 3 | 9 | Supply Chain Management / ICT |
| 35 | Call centre is not redundant and goes down for odd reasons.  Call routing not working | No client access to GPAA via call centre | 3 | 4 | 12 | ICT / MTN |
| 36 | Filing Room – Cabinets are filled with un-scanned tender documents which would be lost in the event of their being damaged. | Loss of Information | 3 | 3 | 9 | Supply Chain Management / ICT |
| A workflow and document scanning process should digitise hard copy files and documents |
| 37 | HR files are hard copies and not scanned | Loss of Information | 3 | 4 | 12 | HR / ICT |
| 38 | Forensic documentation is stored in a normal office on the ground floor and not in a safe – this creates a vulnerability to theft, sabotage or fire / water damage. This documentation is very important to the forensic teams and if it is unavailable it would be a severe blow to their on-going investigations. | Loss of Documentation | 2 | 3 | 6 | Forensic and Fraud Prevention / ICT |
| 39 | Local Data Loss | Loss of User data | 4 | 3 | 12 | ICT |
| Data which resides on local hard drives is often not backed up and will be difficult to reproduce. |
| Implement policies and procedures for saving of local data on the network or alternate methods of backup up the locally stored files on users laptops |
| 40 | **Fire Risks** | The only effective fire suppressants are in the data centre, many other areas have no protection other than hand held cylinders. Stores Area F 01 -No fire suppressants are installed in the computer store room and entire store area (including offices). Where appropriate correct fire suppressant should be installed. | Loss of assets and equipment | 2 | 3 | 12 | Facilities Management / ICT |
| Some of the hand held extinguishers have passed their service dates and need to be maintained and serviced. |
| 41 | There are a number of unrated wooden doors which will not offer any protection in the event of a fire – doors to computer facilities should be fire rated | Loss of ICT Systems | 3 | 4 | 12 | Facilities Management |
| 42 | **Regional Risks** | In some of the region’s the building cannot be accessed from outside by disabled members | Poor Public Image | 3 | 1 | 3 | Supply Chain Management / Facilities Management |
| 43 | Security – sometimes staff members are threatened by hostile clients and can enter building (main security access) without being checked properly for weapons. Office has been held hostage by unhappy Special Pensions clients for applications which are not valid - better security is needed at the entrance - metal detectors and handheld units | Safety of Staff | 3 | 3 | 9 | Physical Security |
| 44 | No automatic fire suppressant in any of the regional offices visited and very few had fire detectors installed | Fire Damage | 4 | 4 | 16 | Supply Chain Management / Facilities Management |
| 45 | No evacuation tests done yet in most regions | Inefficient Recovery | 3 | 4 | 12 | Employee Wellness / Physical Security |

Table 2 - BIA Risks

**Conclusion**

The GPAA will ensure compliance as far as Business Continuity is concerned with KING IV, GPG 2018 and ISO 22301, as listed in the BC Policy.

**Submitted**

**DR CS FERGUSON**

**DIRECTOR – STRATEGY, POLICY and BCM**

**DATE: Thursday, 25 April 2019**

**Supported / Not supported**

**MR E. KGOSIEMANG**

**ACTING CHIEF RISK OFFICER - GPAA**

**DATE:**

**Noted**

**MS. A .BADIMO**

**RISK COMMITTEE CHAIRPERSON - GPAA**

**DATE:**