BOC Cloud Services – Business Continuity Management (BCM)

Table of contents

Acronyms

Acronym	Description
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
DRP	Disaster Recovery Plan
RTO	Recovery Time Objective
SLO	Service Level Objective

1 Introduction

BOC's cloud services are the operations model for many customers relying on the optimal reliability, performance, and security of for their BOC product accounts. To ensure these service quality attributes even in adverse situations, BOC has developed a Business Continuity Plan (BCP) specifically for the offered Cloud Services. This document shall provide an overview of the underlying strategy and the operational part of this BCP to interested parties.

2 Scope

The Business Continuity Plan described in this document has been put in place for the following services, covering all BOC products:

- Enterprise Accounts
- Starter Edition
- Partner Accounts
- Project Accounts
- Academy Accounts
- Premium Test Accounts
- Standard Test Accounts
- Community Editions
- Hotline Services
- Change Management
- Request Fulfilment

3 BIA

In order to identify criticality of the services in the scope and to establish a matrix between the services and the various assets required for providing these services, a business impact analysis is being performed on annual basis to adjust according to business requirements and changes in the way the services are provisioned.

4 Concept

The concept applied to establish managed business continuity is split in two parts. The first part deals with organizational aspects, the corporate facilities and corporate IT resources. The second part deals with the IT resources which are part of the BOC cloud services platform.

4.1 Corporate Organization, Facilities, and IT Resources

BOC has implemented a Business Continuity Plan focussing on situations that could directly affect the organization itself, i.e., the staff, the premises and the IT resources required for the execution of relevant business processes of BOC.

4.1.1 Staff

While BOC's overall BCP covers business processes of the whole organization, the staff related assets and processes required for a flawless business continuity of BOC Cloud Services are:

- Cloud Operations Staff
- Hotline Staff
- Incident Management Process
- Request Fulfilment Process

The Business Continuity Plan actions covered with respect to staff include:

- Knowledge documentation and transfer
- Key personnel identification
- Team splitting in health crisis
- Teleworking in health crisis
- Special management support for key personnel during crisis
- Hiring strategies and programmes

4.1.2 Facilities and IT Resources

BOC corporate facilities and IT resources required for the operations of BOC Cloud Services are:

- Central Firewall
- Directory Services
- DNS Service
- Domain Controller
- File Server
- Headquarter Office
- Mail Server
- Service Desk
- VPN Gateway

The Business Continuity Plan actions for facilities and IT resources are split into two categories: recovery actions that can be implemented on the primary site (activation of stand-by equipment, replacement of equipment, restore of configuration, restore of virtual servers, etc.) and those that require a relocation. Relocation plans exist for moving central services to the premises of BOC in Berlin, where the base infrastructure is available to allow for resuming the services in a timely manner. Three relocation scenarios are defined based on which assets from the primary site are available for restore (backup tapes only, backup

equipment with data, all infrastructure elements). Exercises cover failover tests of redundant equipment as well as restore tests on service level.

4.2 Cloud Platform IT Resources

Specifically for the cloud services, a dedicated Disaster Recovery Plan focusing on the SaaS Platform has been put in operation. At its core it builds on the availability of a second location that can be used to spawn services in a disaster case where the primary site is in an unrecoverable state. In order to make the secondary location available at any time, the relevant information required for service restore is continuously being replicated from the primary site to the disaster recovery site. This information includes:

- All configuration management assets, including the full inventory of deployed infrastructure and service on the primary site
- The directory services used for management of users and servers
- The software packages required for deploying SaaS accounts
- The backups of all databases

For a fast recovery process base infrastructure is permanently available on the disaster recovery site for all central services like firewall, reverse proxy, active directory, email, file services, configuration management, database and monitoring. A small number of servers is stand-by for actually running the workload.

In a disaster situation the operations team follows the instructions for establishing the services in the secondary location ordered by their priority which is derived from the BIA. Recovery procedures are described for all assets that are needed for the operation of the cloud services platform and the hosted services and accounts.

5 Tests and Training

To validate the feasibility of the planned recovery procedures and also to ensure that enough personnel is capable of performing these procedures, recovery tests are performed at least twice a year.

5.1 Test Plans

For the execution of such recovery tests, the DRP contains test plans describing the steps of the to be executed test. Some of the relevant steps are:

- Random selection of a production account
- Restore of the corresponding database
- Spin-up of the required machines in the disaster recovery environment
- Deployment of the application stack
- Testing of access to the recovered account
- Documentation
- Clean-up

5.2 Test Execution and Training

A planned recovery test is assigned to one of the team members who then executes the test plan using the procedures defined in the DRP, documenting any observed obstacles of uncertainties, and capturing the time spent for the various steps. The tests are documented in the corporate issue tracking system and reviewed by the head of the operations team.