

# Business Continuity Plan

## QP 17 605

### Publication 3

Classification		
Level		
0	Unclassified - Public information	X
1	Restricted - Invoke personnel only	
2	Confidential - Authorized users only	
3	Secret - Authorized users only	
4	Top Secret - Authorized users only	

Version				
Date	Versions	Author(s)	Validated (V) / Approved (A) by	Version
27/12/2017	Publ. 1	SV	IT dept.	Original version
17/07/2020	Publ. 2	SV	Security Committee	Addition of paragraph 5
25/06/2021	Publ. 3	SV	Security Committee	Review

Reviewed by				
Date	Versions	Name	Job title/Department	Purpose

## Table of contents

1 - Subject .....	3
2 - General presentation of the network .....	3
3 - Critical Chain.....	4
4 - Securing the Critical Chain.....	5
4.1 - Monitoring.....	5
4.2 - Data Centers.....	5
4.3 - Power Supply.....	6
4.4 - Air-Cooling Systems.....	6
4.5 - Environmental Risks .....	6
4.6 - Networks .....	7
4.7 - Servers .....	8
4.8 - Data Storage .....	9
4.9 - Data Backup.....	9
5 - Availability Objectives .....	10

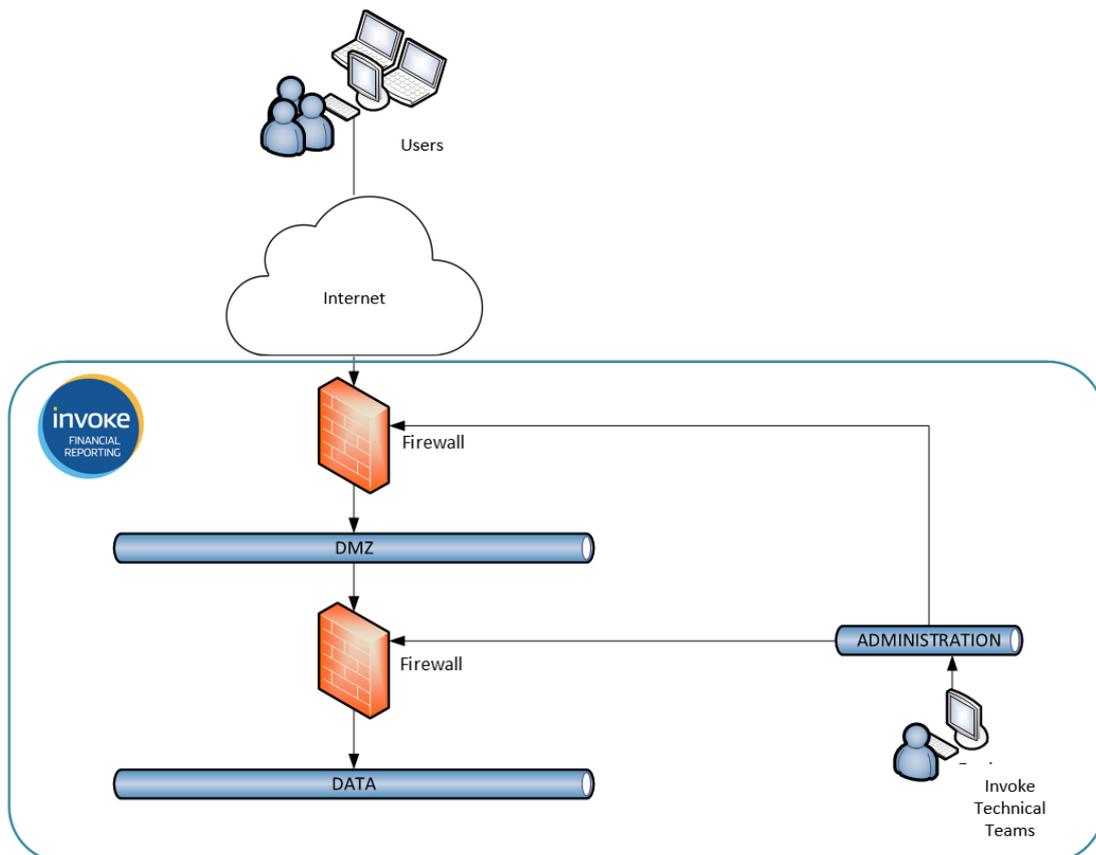
## 1 - Subject

The Invoke Business Plan (BCP) provides detailed information on policies and systems in place in the event of loss, damage or malfunction of its information system, with a particular focus on hosted services.

This document covers different critical elements of both internal and external networks. It also lists procedures implemented to lower downtime, which may impact Invoke clients.

## 2 - General presentation of the network

The network infrastructure used by Invoke for the provision of services is divided into several areas. These areas are separated by firewalls to ensure that servers and equipment are properly isolated.



The network used for hosted services is divided into 4 distinct areas, each isolated by firewalls. These firewalls act as a filter for the following exposed network services:

- **The Wide Area Network (WAN)** interconnects the infrastructure with the outside (Internet).
- **The Demilitarized (DMZ) network** is the only network accessible by the WAN network, and contains front-end servers that publish hosted applications.
- **The DATA network** hosts the database servers used by hosted applications.
- **The ADMINISTRATION network** contains the servers that administrate hosted applications, and is restricted to Invoke teams.

Invoke uses its own infrastructure to provide hosted services for its software solutions. Data centers and related equipment are thus the sole property of Invoke.

The IT department oversees all aspects of infrastructure operations and maintenance, and does not rely on outsourcing.

### **3 - Critical Chain**

All elements necessary to the provision of hosted services are part of the critical chain of the company, thus requiring a reinforced monitoring system and higher resilience against failures. In addition, Invoke has developed a specific architecture to ensure the highest possible availability.

Elements included in the critical chain are:

- Data centers
- Power sources
- Air cooling systems
- Environmental risks
- Networks
- Servers
- Data storage
- Data backup

## **4 - Securing the Critical Chain**

### **4.1 - Monitoring**

The IT team monitors all Invoke Information Systems in real time, to ensure proper functioning. This includes:

- Server rack power supply
- Server room temperature
- Air cooling systems
- Physical state of servers (disks, memory chips, CPU errors...)
- Logical state of servers (connectivity, service state...) and usage (CPU, memory, disk and network)
- Network devices (operation, port state, connectivity...)

Invoke's internal monitoring tool detects and notifies the supervision team of any anomaly immediately. The team then creates a new incident in the internal incident management tool. Any action carried out is recorded until the incident has been resolved.

### **4.2 - Data Centers**

Invoke operates two independent data centers. They are interconnected through multiple optic links, which enables data synchronization in real time. These two data centers are used simultaneously and the load is balanced between them. This system ensures that both data centers are running normally.

In addition, each data center uses less than 50% of its capacity. Should a failure occur on one data center, the other will be able to handle the entire load, thus ensuring SAAS continuity.

Invoke conducts load transfer tests annually to check for potential issues. Access to server rooms is restricted to members of the technical team, and requires both a key and a personal access badge. Lastly, a remote security company monitors data centers continuously. Should an alarm be triggered (intrusion, fire etc.), a security team will be dispatched immediately.

### **4.3 - Power Supply**

Two power paths -protected by UPS units, supply power to each server rack.

This dual power input protects equipment from any service disruption in the event of electrical maintenance or power outage. They also allow complete redundancy of the electrical path in case of failure from either an equipment or power supply unit. Lastly, the UPS units prevent server/equipment failure as a result of poor power quality, such as frequency or voltage variations.

The main Invoke data center is equipped with a backup generator. Should a power outage occur, this independent backup generator will turn on automatically and supply power to the building and servers for a minimum of 24 hours. The backup generator is able to restore normal power within a few seconds, during which the power of the infrastructure will rely on the UPS units. Tests are conducted every two months and Invoke is covered by a 24/7 maintenance contract.

### **4.4 - Air-Cooling Systems**

Each server room is equipped with two independent air-cooling systems. These systems run in active/active or active/passive mode, depending on their location. The server rooms are temperature controlled.

These air-cooling systems are covered by a maintenance agreement, and tested regularly. The monitoring tool notifies the supervision team of any change in temperature.

### **4.5 - Environmental Risks**

Invoke data centers are located in a low-risk area, and thus not impacted by natural disasters (flooding, earthquake etc.).

In the event of fire, an alert is sent to the remote security company immediately. The main data center is also equipped with an automatic fire suppression system.

These systems are checked periodically. The supervision team will be notified if any defect is identified.

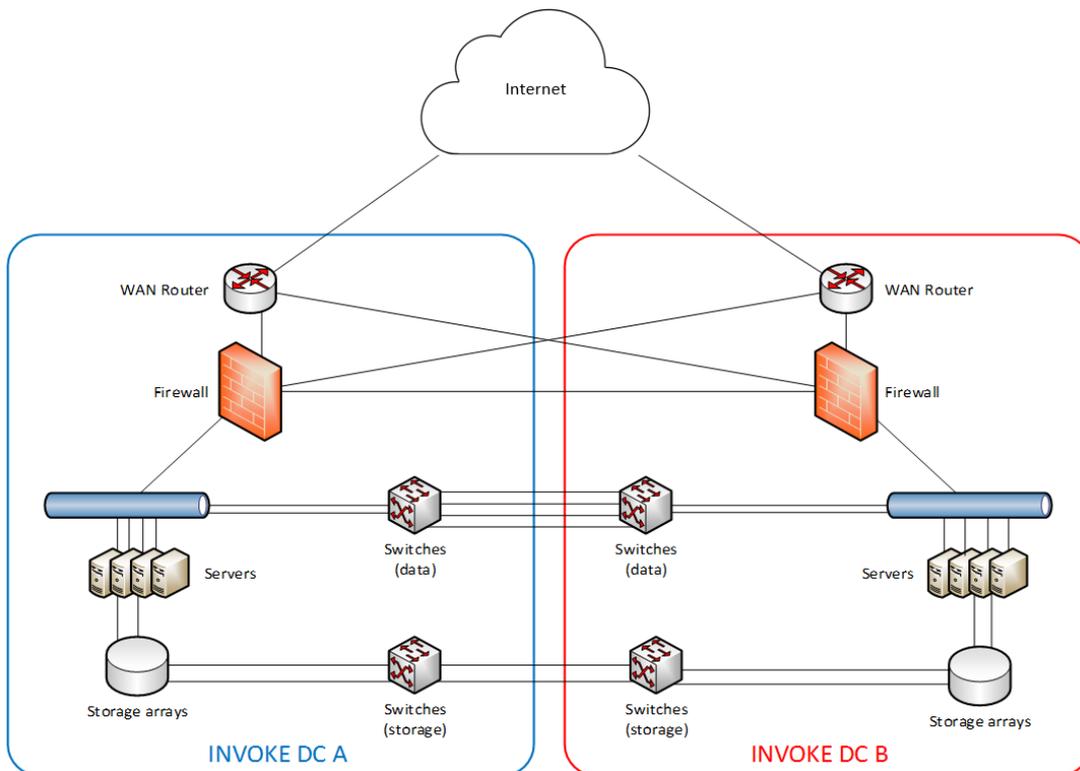
#### 4.6 - Networks

All networks used in the Invoke data centers are redundant. This layer of security improves service availability. Networks use dedicated optic links that run between the two data centers.

The networks are redundant, both in terms of media (6 dedicated optic links) and equipment (switches, firewalls, fabrics etc.). Redundancy prevents service interruption in the event of equipment/link failure.

There are 2 types of networks:

- Data networks: they establish communications between servers.
- Storage networks: they provide connectivity between servers and storage arrays.



There are different types of network equipment:

- **WAN routers:** Two main routers (active/passive) ensure the connection with the outside. Should one link fail, traffic is redirected to the second router within seconds.

- **Firewalls:** A firewall cluster (active/passive) isolates the different networks. Should a node in the cluster fail, the system will switch to the other node automatically and thus prevent a loss of connection.
- **Data switches:** Switch stacks enable communication between servers and data centers. The loss of one equipment is transparent since links between servers and switches are redundant.
- **Storage switches:** Fabrics enable connectivity between storage arrays and servers. The loss of one equipment is transparent due to the complete redundancy between servers, storage arrays and fabrics.

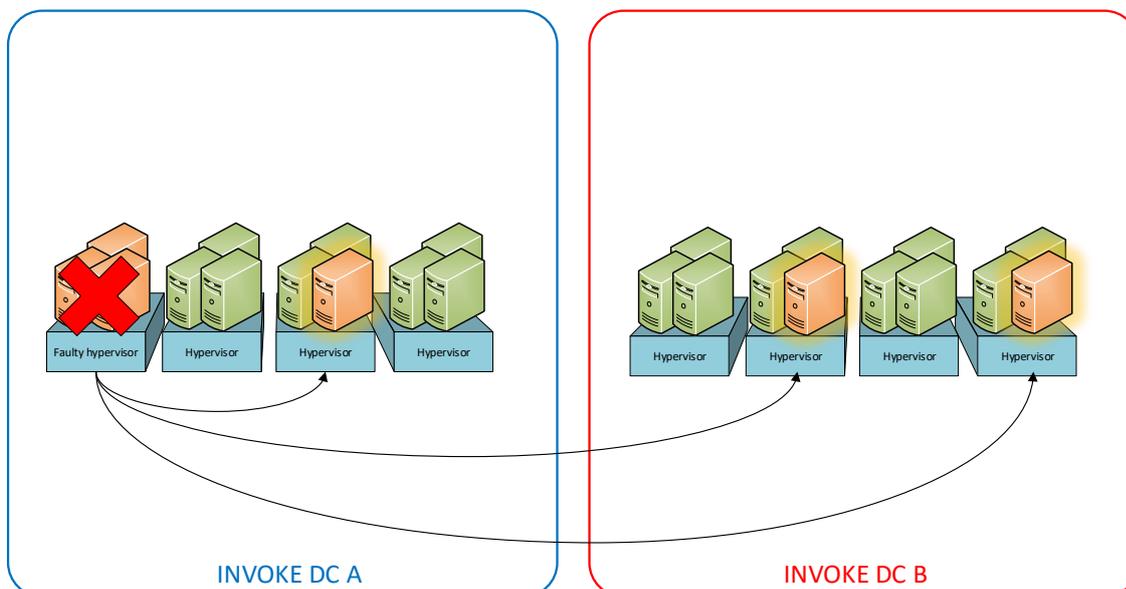
These networks are monitored continuously. Should a link fail, the supervision team will be notified immediately.

#### 4.7 - Servers

The servers providing Invoke hosted services rely on virtual machines. This technology allows high availability.

These virtual machines are portable, and may be moved to another server –whether this server is located in the same datacentre or not. Moving virtual machines will not impact services or create disruptions for end users.

Invoke has implemented a high availability system. This system restarts a virtual server on another host in the event of a loss of hypervisor host or data center. The supervision team is notified of such event but no human intervention is required.



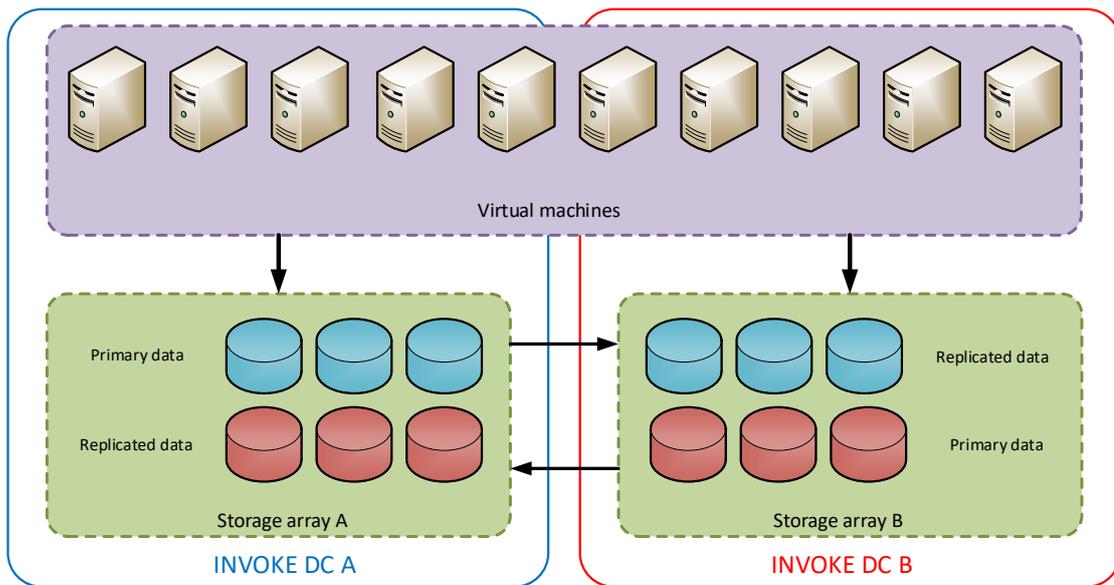
#### 4.8 - Data Storage

Data and applications are stored in storage arrays in each data center.

These arrays contain a large number of redundant disks and spare disks. Should active disks fail, spare disks will be integrated in the array immediately.

The monitoring tool notifies the supervision team of any failure immediately. Any action carried out is recorded until the incident has been resolved.

Lastly, both storage arrays are synchronized. They each contain a full copy of the data at any point in time. This system ensures that losing an array will not impact the services running at the time of the incident. Should an array fail, the remaining array will automatically and instantly remap the volumes on the servers (hosting the services).



This storage system is crucial and is therefore covered by a 'Mission critical 4 hours, 24/7' warranty from its vendor.

#### 4.9 - Data Backup

Hosted service data is stored in databases, which are checked and backed up on a daily basis. Backups are transferred to dedicated storage servers.

The replicated backups are stored on two different storage servers located in both data centers. Backups are kept for a minimum of ten days.

All actions carried out during the backup process are recorded. The monitoring team will receive a notification in the event of a failure.

## 5 - Availability Objectives

The elements presented above serve to meet the following business requirements:

Recovery Time Objective (RTO)	<b>4 hours</b>
Recovery Point Objective (RPO)	<b>24 hours</b>