The Cloud: new challenge for Business Continuity

What is the vision and experience of Orange Business Services for success in these projets?

The Duquesne Group

Business Services

orange™

Table of contents

A Dusquene Group White Paper prepared in partnership with Orange Business Services

#1 Introduction

The starting point for Business Continuity is the business activities of an enterprise. If the underlying resources upon which they depend fail or are struck by a disaster, these activities - the true “raison d’être” of the enterprise - can be severely disrupted or even entirely interrupted.

The management of Business Continuity takes into account all of the resources, both technical such as IT and non-technical such as offices and staff, that are necessary for the essential activities of the business lines. Its purpose is to protect, continue or resume these activities - whatever the nature of the failure or disaster and whatever resources may be affected - in a time frame and under conditions that are acceptable for the business lines.

Even so, it goes without saying that the enterprise information system is an increasingly indispensable resource for most business activities. That’s why for years, so many CIOs have implemented often costly measures – data center backup sites, contracts with specialist IT recovery companies, etc. - to cope with a major failure or disaster at their data centers.

And then the revolution of the Cloud arrived - a new IT paradigm which in our opinion represents a crucial challenge for Business Continuity.

Yet, in the ongoing “conversation” about the cloud, the need for business continuity has too often been neglected. The issue does appear from time to time when the services of a major cloud provider are disrupted or interrupted, for example, by a powerful strike of lightning on a cloud data center or a major technical failure. In 2018, all of the big “hyperscale” clouds suffered “outages” that were highly disruptive for the business of customers but seldom of long duration.

That being said, we must admit that very rare events - but with huge impact - eventually do come to pass. One day or another, a cloud data center will indeed suffer a major disaster - for natural, technical or human reasons - jeopardizing the business of its customers. It’s a bit like the great centennial flood of the river Seine in France: the question is not “if” but “when”.

Even so, the picture is not entirely dark. Thanks to technological progress, continuity and recovery solutions that are well adapted to cloud environments are now available.

In this context, the purpose of our white paper is to analyze the challenge of the Cloud for Business Continuity, fully taking into account the wide variety of needs and solutions for different customers.

To make our analysis as concrete as possible, we chose to develop it in partnership with Orange Business Services (OBS). We shared our visions of the market, used as examples some of its solutions and references, and even commented on its new multi-cloud strategy.

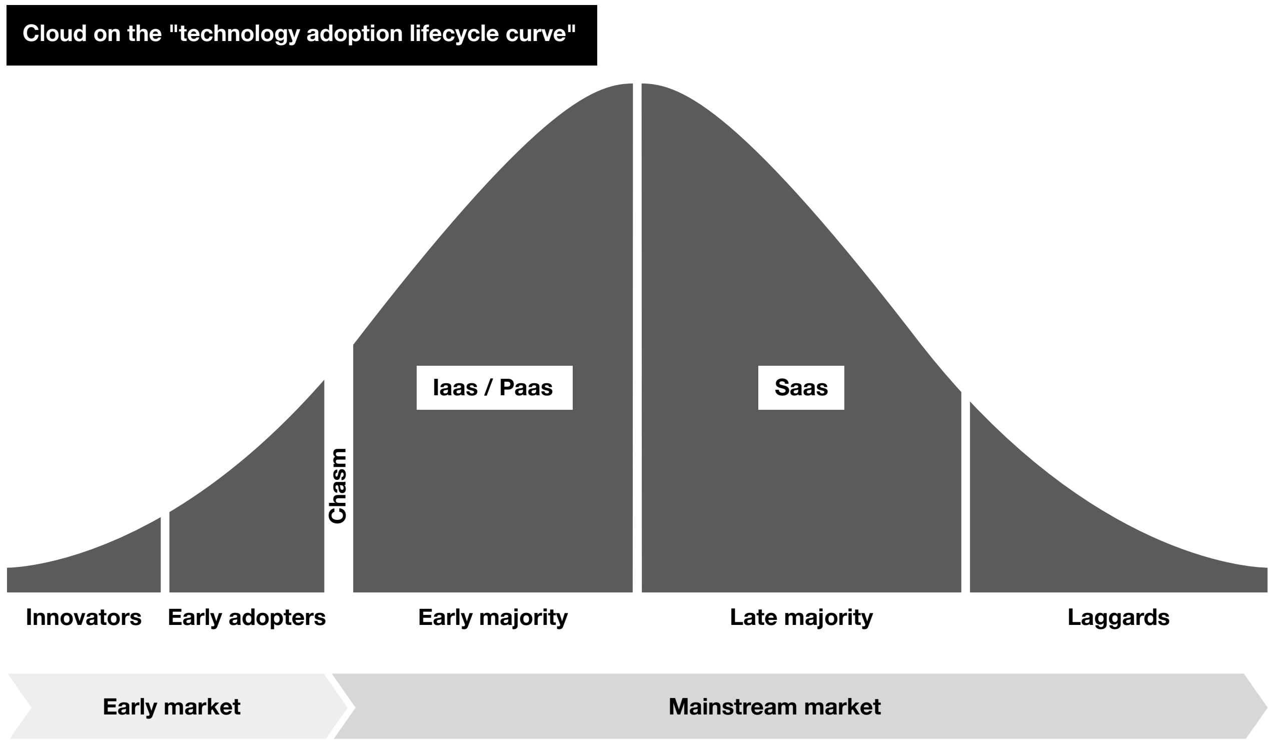
Nonetheless, our analysis accurately reflects our own independent vision of what we see as a crucial challenge for enterprises going forward: ensuring the continuity of their business activities in the era of the cloud.

#2 Evolution of the Cloud market: the requirement of continuity

With so many user organizations proclaiming a “cloud first” strategy, together with teutonic shifts in power and influence on the vendor side, it’s clear that cloud computing has gone mainstream.

As always in technology markets, this maturation leads to changes in “buyer values”, which translate into new customer expectations and requirements.

To get a better understanding of what this means in terms of market dynamics, we’ll start by positioning the cloud (IaaS/PaaS) on the widely accepted technology adoption lifecycle curve of Geoffrey Moore.



Before exploring the implications, two points should be made:

- “Cloud” (IaaS / Paas) includes “public” and “private”. Contrary to the predictions of a good many IT pundits, private cloud has shown considerable tenacity and continues its progression with double digit growth.
- Cloud adoption by numerous mainstream users does not imply that their applications run primarily in the cloud. Diane Greene, formerly responsible for Google Cloud Platform, estimates that only about 10% of business processing is done in public clouds. IBM gives an estimate of 20%, both public and private. The cloud paradigm has conquered “mainstream market” mindshare, but it still represents a small - but growing - share of enterprise computing.

Let’s return now to our analysis. The life cycle of technology adoption is a normal bell curve divided into five phases defined by customer types: visionaries, early adopters, early majority, late majority and laggards. The most critical moment of the cycle is the transition (the “chasm”) between early adopters and the early majority, because the “buyer values” are very different.

• Early adopters are typically technically motivated, tolerant of a new technology’s inevitable sometime failures and focused on the problems they want to solve. In the early years of the cloud, it’s not surprising that developers – often but not always in start-ups - drove adoption.

• The buyer values of mainstream customers are more pragmatic than technical, generally focused on “what does it mean for my enterprise?” Their concerns include: take-up in their own business sector, corporate sourcing policies, end to end services as needed, integration with existing investments, security and compliance, manageability and, of course, the reliability and resilience needed to support essential business activities. In the case of the cloud, these are and remain typical CIO level concerns.

It is clear that, over the last several years, the cloud has “crossed the chasm”, moving from the “techy” early adopter phase and into the pragmatic mainstream where CIO level concerns come to the fore.

In our opinion, the continuity of applications that are “critical” for essential business activities is one of the most important requirements… and these applications are increasingly deployed in cloud environments. As a result, companies can no longer accept theoretical availability levels (as in most public cloud SLAs). In case of failure or disaster, the enterprise must be able to restore these applications within time constraints and under conditions that are acceptable for the business lines.

Bottom line: **as cloud services become increasingly prevalent, the demand of customers for the continuity of business critical applications in the cloud accelerates.**

Orange Business Services has been prescient in anticipating and reacting to this requirement. The company has invested heavily in a broad portfolio of solutions, with leading technology partners, to meet the different requirements of its customers for the continuity of cloud services.

To establish the context for these solutions, we will first briefly outline the fundamentals of business continuity management.

“ Evolution of the Cloud market: the requirement for continuity

- Cloud computing has entered the “mainstream“ of the IT market.
- Applications that are “critical” for essential business activities are increasingly deployed in cloud environments.
- In case of failure or disaster, the enterprise must be able to restore these applications within time constraints and under conditions that are acceptable for the business lines.
- As cloud services become increasingly prevalent, the demand of customers for the continuity of business critical applications in the cloud accelerates.

#3 ISO 22301: the framework for Business Continuity

ISO22301, the international normative reference in the matter, defines business continuity as the "capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident."

Indeed, the purpose and focus of the standard is the continuity of the business activities of an organization. These activities rely on both technical resources (cloud services, applications, etc.) and non-technical resources (HR, offices, etc.). If these resources are struck by a failure or a disaster ("a disruptive incident", in the language of the standard), the essential activities of the business lines can be disrupted or even interrupted.

The figure below presents in a simplified way the main components of what is commonly called an enterprise Business Continuity Plan (BCP), in line with ISO 22301 requirements. We will briefly explain each component with, in some cases, a comment on aspects relevant to the cloud.

Risk assessment	**Business Impact Analysis (BIA)**
Business Conituity Strategy IT and non IT	
Crisis Management Structure	**Business Continuity Plans**
Tests & exercices	**Training & Awareness**

Policy - Governance - Controls - Improvements

Three "upstream study" components are positioned in the upper part of the figure:

- **The Business Impact Analysis (BIA),** as Emmanuel Besluau, a leading expert in the field, writes, is "at the heart of modern approaches to managing continuity. It focuses on the business activities of the company and provides answers to questions such as: "what activities must be continued or restored in the event of a disaster?" ... "in what time frame?" ... "with what resources?" Emmanuel Besluau adds, "in other words, the BIA is an essential starting point."

  Two requirements - identified during the BIA for each business line activity - are crucial:
  - Maximum Tolerable Period of Disruption (MTPD)
  - Maximum Tolerable Loss of Data

  It is sometimes said that business lines require 100% continuity for all their activities. This affirmation is false. The requirements of different organizations and of their business lines are different. Moreover, there is always a hierarchy of temporal priorities among business activities, even if the trend today is towards shorter and shorter MTPDs.

In the cloud, the starting point remains the requirements of the business lines

Taken together, these two requirements - maximum acceptable interruption and maximum tolerable data loss - express both the business vision of the "criticality" of an activity and business line requirements for continuation or recovery in the event of a failure or disaster. They are at the heart of the problem of choosing appropriate cloud based business continuity solutions. We will come back to this later.

- **Risk Assessment** focuses on the resources (IT, HR, offices ...) upon which these activities rely. The assessment involves systematically identifying, analyzing and evaluating the risks to which these resources are exposed and determining the risk scenarios to be taken into account. However, it is in the "state of the art" (and often among the requirements of regulators) to take into account "extreme shock" scenarios, such as the complete loss of the HQ building or a long interruption of the information system. Moreover, this assessment is also an opportunity to see if it is possible to reduce proactively the probability or potential consequences of the various risks.

- **Business Continuity Strategy** is a crucial step. According to the standard, "determination and selection of strategy shall be based on the outputs from the business impact analysis and risk assessment." Various combinations of solutions for the continuity or the resumption of essential activities may be possible, various criteria of evaluation (technical, economic, organizational ...) may come into play, but the organization must decide! Often, the final decision belongs to Top Management.

Based on its business continuity strategy, the organization can move on to developing, documenting and implementing "operational" measures to ensure that it can cope with various failures or disasters, if and when the time comes.

- **The Crisis Management Structure** maintains, first and foremost, the decision-making capacity of an organization in an abnormal situation. The center of the structure is the crisis cell, whose composition depends on the structure of the organization and the nature and gravity of the incident. It is set up quickly to "take things in hand" in decision-making, management of priorities and communication. It launches and provides overall supervision for the various individual business continuity plans and procedures that were prepared in advance ... and deals with issues and problems that were not foreseen.

- **Business Continuity Plans** (detailed plans for various organizational units) prepared in advance collectively represent what one might call a "tool box" for the crisis cell, launched according to the circumstances to continue or resume business activities and restore or provide resources (IT, offices, HR, ...) that are necessary. Most IT oriented business continuity plans rely on technical solutions, especially those designed to protect data (for example by replicating it to a recovery site) and to restore applications for the activities that are business line priorities.

The cloud for a "recovery site"

The use of the cloud for a recovery site has many advantages. The establishment and management of a physical recovery site is a cumbersome and expensive option, especially in terms of investment (CapEx) for resources that are often seldom used. A cloud recovery site takes advantage of shared resources and makes it possible to pay only the resources actually consumed (OpEx).

- **Training & Awareness** are basic requirements of the standard, which attaches great importance to the skills of the people who are responsible for various business continuity measures. In addition to training in technical tools, ISO 22301 certification training courses can be considered. Even if the intention is not certification of the organization, the certification of some key players in business continuity management reflects a serious approach. In addition, the standard requires regular awareness sessions for all staff, especially concerning their own roles in the event of a failure or disaster.

When a major failure or disaster comes, the effectiveness of the overall enterprise Business Continuity Plan will depend on the skill and preparedness of people who have to deal with it.

- **Tests & Exercises** of continuity measures and plans are among the basic requirements of the standard. It is almost certain that a plan that is not tested regularly and, consequently, not kept up to date, will prove to be defective when the failure or disaster arrives.

  Two clarifications of the standard here are particularly relevant. It requires tests that "taken together over time validate the whole of its business continuity arrangements" and "minimize the risk of disruption of operations".

The advantage of the cloud for tests

A major benefit of modern solutions for recovery in the cloud is to facilitate testing. Most cloud based recovery tools enable more frequent and granular tests, with resources paid for on a usage basis (OpEx) and above all without disrupting operations. We will return to this point.

At the bottom of the diagram, we find other requirements of the standard - Business Continuity Policy, Governance, Controls and Continuous Improvement - which make it possible to ensure (beyond simple tests of measures in place) that the overall Business Continuity Plan of the organization can remain effective over time, evolve in line with the needs of the organization and be improved continuously.

Now, based on the proven best practices of ISO 22301, we are ready to get to the heart of our subject and address the issue of choosing solutions for continuity and recovery in the cloud.

ISO 22301: the framework for Business Continuity

- The purpose and focus of ISO 22301 - the international normative reference for business continuity planning - is the continuity of the business activities of an organization.
- The BIA provides answers to questions such as: "what activities must be continued or restored in the event of a disaster?"... "in what time frame?" ... "with what resources?"
- Two requirements - identified during the BIA for each business line activity - are crucial: maximum acceptable interruption and maximum tolerable loss of data.
- On the IT side of business continuity planning, the use of the cloud for a recovery site has many advantages: mutualisation of resources, usage based payment (OpEx)…

#4 How to choose a solution for continuity and recovery in the cloud

For the CIO, the choice of a solution (and also the choice of the supplier or provider) is often complex, because it may need to take into account many factors.

Before discussing the criteria, we should remember that the choice of business continuity solutions comes in the "downstream" part of the work according to ISO 22301. We assume here that a minimum of reflection "upstream" was done in advance at least on the IT part, particularly in terms of BIA and Continuity Strategy. Depending on the size and structure of the organization, this reflection is not necessarily completely structured, but we need at least a clear vision of the continuity requirements of the business lines.

Under this hypothesis, we will highlight some major criteria for choosing solutions. We will also mention as examples some offerings from Orange Business Services (OBS), but the logic remains valid regardless of the supplier.

We will start with three major criteria:

- **The "criticality" of applications and data to be protected**

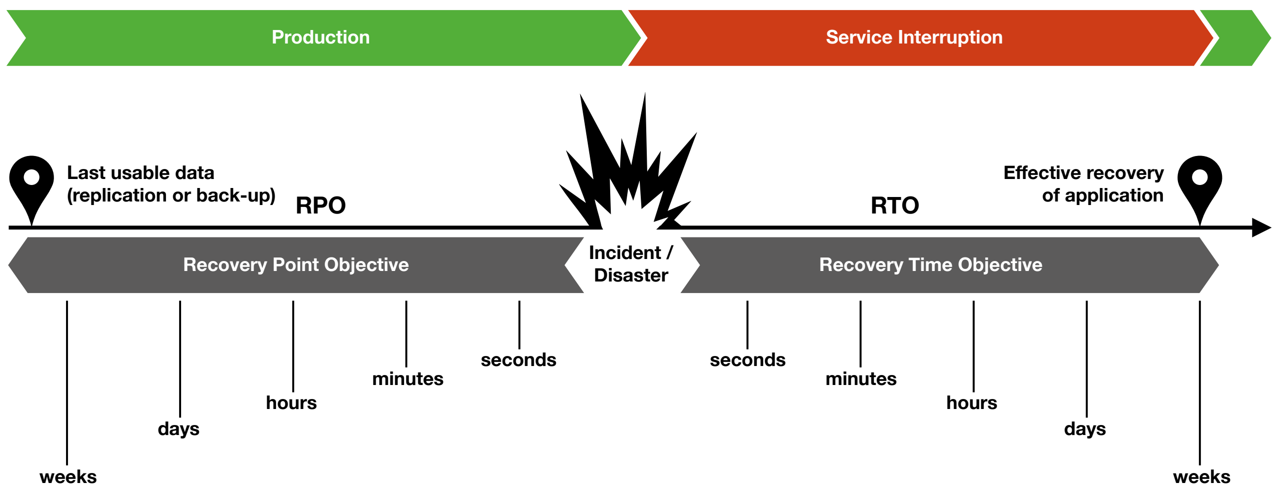
  This criterion is by far the most structural. The purpose of business continuity planning is to protect, continue or resume business activities in case of failure or disaster. As noted earlier, two business requirements are identified during the BIA for each priority activity:

  - Maximum Tolerable Period of Disruption (MTPD)
  - Maximum Tolerable Loss of Data

  During the work on the Continuity Strategy, these requirements are confronted with technical and budgetary realities, for possible adjustments or validations. Then the enterprise can translate the finalized business requirements into technical parameters for solutions:

  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)

Illustration of RPO and RTO



According to ISO 22301, the RPO corresponds to “the point to which information used by an activity must be restored to enable the activity to operate on resumption”. The meaning of the RPO is generally clear for all, because its value is a function of the latest data presumed to be available for recovery from a failure or disaster.

Some confusion however remains about the true meaning of the RTO. In the diagram above, the representation of the RTO is in line with ISO 22301 which defines it as the “period of time following an incident within which (a) product or service must be resumed, or (an) activity must be resumed, or resources must be recovered”. The RTO (which is an objective, even a commitment, but never a certainty) starts with the incident (or its detection) and runs until the applications for the business lines are restored.

The ability to meet a defined RTO depends on multiple factors: not only the technical recovery tool (for example that of Zerto, an OBS technology partner, whose intrinsic performance is measured in minutes) but also organizational procedures and structures in place to manage an abnormal situation. In this context, the “software editor RTO” of a technical tool is only one of the components - often the shortest - of the overall RTO:

- Following the detection of a failure or disaster, the RTO includes the time needed for escalation, analysis and decision. The occurrence of a “disruptive incident” does not necessarily imply a decision to fail-over to the recovery site. If the down time for repair is acceptable under the circumstances, the company may prefer to wait rather than fail-over.

- If the decision to fail-over is made, the “software editor RTO” begins with the activation of the tool and ends (usually) with the reestablishment of the VMs on the recovery site.

- Then, the VMs need to be activated and the applications restored, without forgetting to verify (and possibly correct) application consistency and of course to redirect user network access to the recovery site.

In addition, restoration of applications does not necessarily allow immediate resumption of business activities, which is why the standard specifies that the RTO must be inferior to the MTPD. With the support of IT, the business lines may need to carry out functional controls, analyze the impact of a possible loss of data and, if necessary, do catch-up work before they can resume normal activities.

Despite these caveats on the RTO, the “criticality” of applications and data (RTO, RPO) is the basis for a useful typology (in the table below) of continuity and recovery solutions.

Level	Nature of the solution	RTO et RPO	OBS solutions and technology partner tools
0 – Cold	Backups of data (or copies) externalized outside company site	RTO: undefined RPO: function of the last usable backup	Flexible Recovery (OBS) with the partner tool Veeam Repository as a Service
1 - Warm	Preparations in place to rebuild the Information System on the recovery site and restart from backups	RTO : defined, non-zero RPO: function of the last usable backup	Partner solution Nuabee
2 – Hot	Up-to-date protection environment on the recovery site (continuous data replication) with VMs ready to be reestablished	RTO and RPO defined but not zero	Flexible Recovery Advanced (OBS) (available soon) with the partner tool Zerto IT Resilience Platform
3 – HA	High Availability (HA): 2 synchronous active sites (hence close, <40km. of separation)	RTO and RPO at zero (in principle), with seamless user fail-over… but shared risks (distance) in the event of a regional disaster	OBS customer project with a catalog of software solutions such as SQL Server AlwaysOn of Microsoft
4 – Vital	HA on 2 nearby active sites PLUS Hot recovery on a 3rd passive site, at > 100 km. distance	- RTO and RPO at zero (in principle) with seamless user fail-over for both active HA sites - RTO and RPO defined but not zero for the 3rd passive site	Flexible Resilience (OBS): OBS customer project with a catalog of software solutions such as SQL Server AlwaysOn of Microsoft PLUS Zerto IT Resilience Platform

This typology - based on the “criticality” of applications and data to be protected - allows us to identify the relevant categories of solutions for further analysis.

- **The capability of the solution to facilitate testing**

This criterion is also very important, because good test campaigns provide the company with the assurance that in the event of a failure or disaster, its measures of protection for business activities will work as intended. Tests make it possible to detect and correct possible inconsistencies between the nominal site and the recovery site (for example, following the launch of a new application) and also to verify the effectiveness of the procedures and the skills of the people who need to be involved.

Modern continuity technologies can deliver significant benefits leveraging virtualization and the cloud. These technologies typically create a cloud “sandbox” dedicated to testing. Normal IT Production continues in parallel with the tests and in fact remains protected. If a disaster or failure occurs while tests are underway, the RPO and the RTO should not be degraded.

Moreover the fail-over perimeter can be easily delimited, both for tests and for real fail-over. This has other advantages, especially if the protection only covers part of the information system. Tests can be done for a restricted perimeter, without impacting IT Production or its protection, and involving a limited number of people. The tests can thus be split up, multiplied and conducted in working hours, hence more frequently and with greater effectiveness in building skills since they can involve all necessary IT and business line staff.

Finally, with payment by usage (OpEx), the costs of testing are reduced. The additional resources used in the cloud for testing are billed only when they are provisioned for the test, and at the list prices of cloud platforms.

- **End to end support services**

Customer needs for support services in the choice, implementation or management of cloud based business continuity solutions are different, depending on their size, their organization, their existing information system and especially their in-house skills.

With recovery solutions, OBS commits to the provision of a solution with a modern technical tool and a cloud recovery platform, with VM based pricing: a simple, “off the shelf” approach that meets the requirements of many customers, especially large corporate groups.

However, other customers (especially SMEs and mid-size companies, but not only) may need more support. This is why OBS offers an end to end range of services “à la carte”. Services for recovery solutions are summarized in the table below:

Study	Configuration	Tests	Update	Fail-over	Fail-back
Identify priority business activities, define their continuity requirements, identify underlying resources (BIA)	Deploy the protection tools on the nominal site	Organize the test(s)	Adjust the configuration to correct any gaps	Ensure the appropriate organization for managing fail-over	Test the correct operation of the nominal platform
Evaluate the criticality of applications and data for these business activities (BIA)	Configure the recovery environment on the recovery site	Test the smooth functioning of the recovery solution	Review / revise processes for joint update of the Information System on nominal and recovery sites	Define the procedures (decision makers / personnel / actions)	Organize the fail-back
Identify the Information System components needed for these applications	Configure the test environment on the recovery site	Determine the pitfalls of restarting applications	Update the recovery site as the Information System evolves	Set up a 24/24, 365/365 organization	Restart servers and applications
Choose the desired level of protection for these Information System components	Configure the necessary network links	Check application consistency		If needed, fail-over : -Restart servers and applications -Check functioning and application consistency	Check functioning and application consistency
Qualify the technical solution(s)	Configure application protection	Compare results to defined RPO / RTO			
	Initiate data replication	Analyze reasons for divergences			

The table summarizes the end to end support services offered by OBS for its cloud recovery offerings. However, we have also included in our typology High Availability (HA) solutions, which are usually delivered in the context of larger projects - deployment, migration or even application development – which require other services.

In any case, the supplier’s capability to provide end to end services that meet the needs of the individual customer is a major factor in the choice of a solution.

- **Other potentially relevant criteria**

So far we have highlighted three major criteria for the choice of a cloud based business continuity solution: the “criticality” of applications and data to be protected, the capability to facilitate testing, and a wide range of support services.

Of course, other factors come into play. For example:

- **The cloud technical environment (VMware, OpenStack, AWS, Azure…)**

Previously this factor was crucial. However, modern continuity tools are becoming “cloud agnostic”. In addition, more and more cloud services providers - including OBS - are also positioning themselves as “multi-cloud”, a change that we will discuss in chapter 6.

- **The existing IT infrastructure of the customer**

The solutions discussed in this white paper are mainly relevant for industry standard x86 architectures. Many customers, however, also continue to use “legacy” systems (mainframes, IBM i, proprietary UNIX systems). In a DRaaS context, it may be necessary to combine a standard x86 solution with specific solutions for these systems.

- **The intention to avoid dependence on a single public cloud provider**

Some customers require that the recovery site for cloud-based applications be hosted in a cloud from another provider, either to avoid “vendor lock-in” or to guard against a major failure on multiple platforms of the same provider. An example of this type of failure is the famous 2017 AWS outage in the US-EAST-1 region, which interrupted the service of all AZs (“Availability Zones”) in the region and caused massive business disruption for many customers.

- **The geographical location**

For regulatory or prudential reasons, some companies require that the data center of the recovery site be located in their own country, including (but not only) in the Finance sector. In the case of European customers, location in another country of the European Union is sometimes acceptable.

In the next chapter, we will present some customer examples, in order to illustrate how and why they chose their business continuity solutions with Orange Business Services.

How to choose a solution for continuity and recovery in the Cloud?

- On the basis of business line requirements, two technical parameters can be defined:
  - RTO: time between the beginning of a failure or disaster and the effective recovery of the application
  - RPO: function of the latest data usable for recovery from a failure or disaster.
- First major criterion: the "criticality" (RTO, RPO) of applications and data to be protected.
- With this first structural criterion, solutions based on different technologies can be categorized: Cold, Warm, Hot, HA (High Availability) and Vital (HA + Hot recovery).
- Second major criterion: the capability to facilitate tests of recovery in the cloud, with usage based payment (OpEx) and no impact on IT Production in parallel.
- Third major criterion: support services "à la carte" in the choice, implementation or management of the solution.
- Other potentially relevant criteria : geographical localisation, technical environments, avoidance of dependance on a single supplier etc.

#5 Orange Business Services, its customers and responses for their projects

In this chapter, we review a selection of customers who chose cloud based business continuity solutions with Orange Business Services (OBS). These are real customers but, with its usual concern for discretion, OBS has asked us to present them anonymously.

The examples will be presented following the logic of the previous chapter: in an ascending sequence of "criticality" of the applications and data to be protected for the business, while evoking other factors that mattered in customer choices.

- **A public social housing organization: Level 0 Criticality "Cold"**

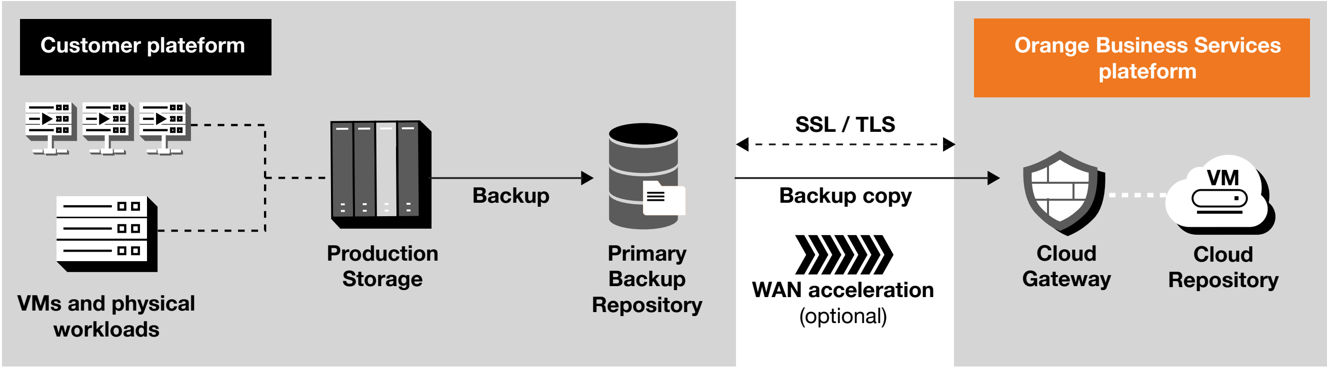
"Externalize backups" - or more precisely send copies off site - is a golden rule of business continuity and the most basic level of protection. An organization that has lost its servers following an "extreme shock" may be able to rebuild its information system and survive. If the data has been definitively lost, it's another story.

Consider the example of a social housing organization which wanted to externalize its backups as a first level of security. Its activity is to develop and manage social housing, but also increasingly to offer a real quality of service to the tenants. In this context, a major loss of data from tenants was unacceptable.

For this customer, OBS implemented the cloud backup functions of Flexible Recovery, leveraging "Repository as a Service" and "Cloud Connect" technologies from its partner Veeam, a recognized leader in backup management.

The general architecture of the technical solution is presented in the following diagram:

General Architecture : Veeam back up solution



This client already had a Veeam backup solution in place at its production site and was already used to the "Veeam experience", with little or no further learning needed of the solution. Flexible Recovery - leveraging other technologies from Veeam - made it possible to extend the existing backup infrastructure to the cloud and protect the data in a high security OBS data center.

An organization with a delegation of public service : Level 1 Criticality "Warm"

Many small and mid size organizations can't meet their business requirements simply by backing up data to the cloud. They need a real recovery solution, despite limited IT expertise and tight budgets. For them, a "Warm" solution may offer a good cost / risk balance.

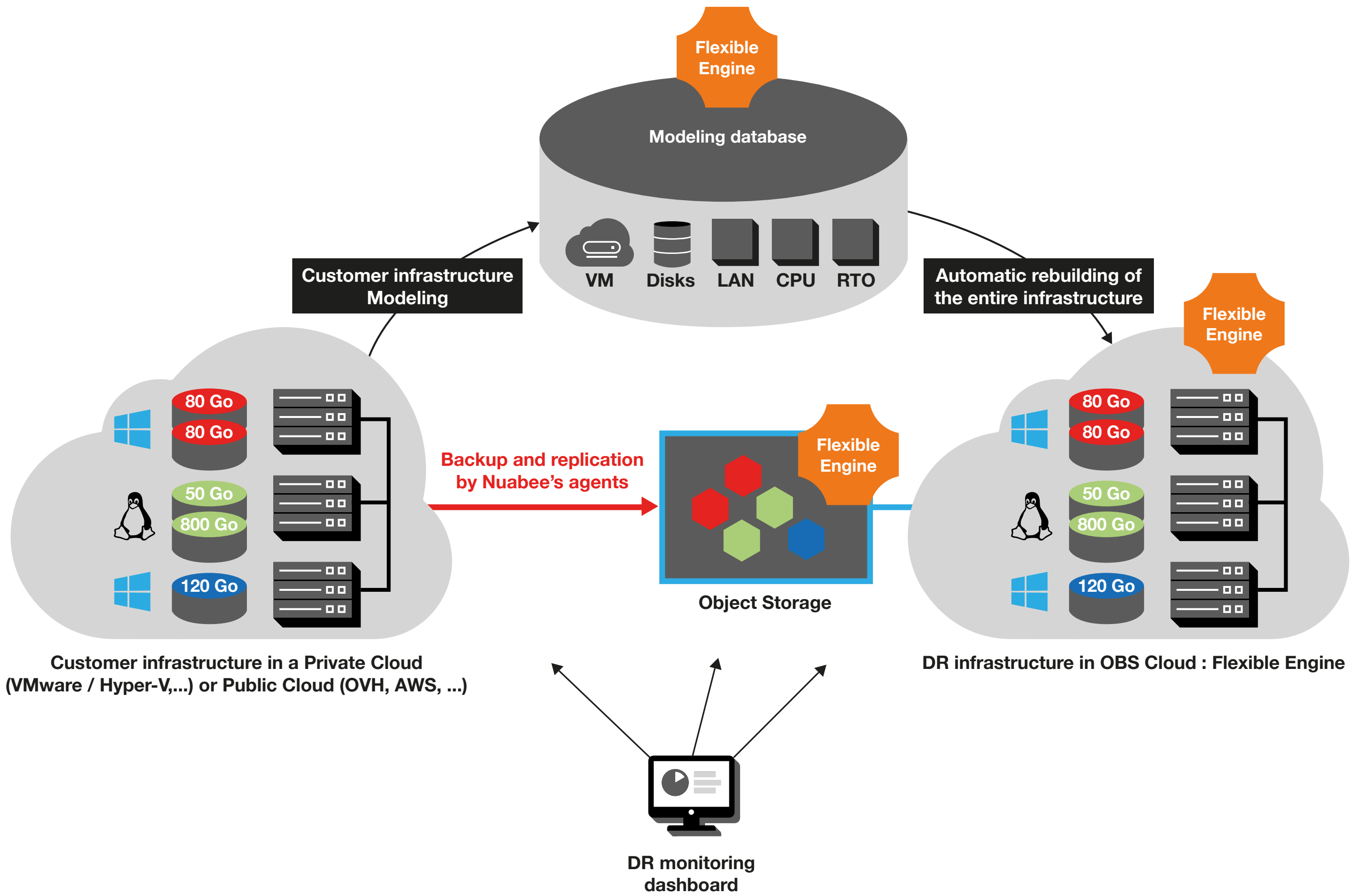
The customer here is an intermediate size organization with a "delegation of public service", in charge of receiving and implementing requests for blocking telephone marketing solicitations for individuals and companies. The information system runs in a VMware vCenter dedicated cloud hosted by OVH in France, with about 35 Linux VMs (Debian) and 3 ESXi hypervisors.

The customer can tolerate an interruption of several hours and the loss of a day of data… but the continuity of public service must be ensured! OBS proposed the solution of its partner Nuabee, with the nominal site on OVH and the recovery site on Flexible Engine, its OpenStack platform. To explain some key factors in their choice, we will simply quote the customer:

"When it was decided that a recovery plan was needed, "which operator?" was a major question. In order to ensure that we would not be vulnerable in the event of a failure of the original operator, we decided to find an alternative operator and that it had to meet quality criteria compatible with the status of public service delegation and also had to host the data in France. The other choice was to keep a VMware vCenter environment or opt for a different environment. Implementing a recovery site on identical infrastructure is simpler but makes us vulnerable to a failure or attack on that platform. Our decision was for a different solution..."

The diagram below shows the general architecture of the solution:

Nuabee's solution general architecture, partner of Orange Business Services



The principles of operation are clearly indicated on the diagram. In addition, we should note that, in the case of this customer, the solution is fully managed by Nuabee: implementation, testing, monitoring of data transfers, fail-over (if necessary) to the recovery site on Flexible Engine and fail-back to the nominal site on OVH when appropriate.

- Implementation

  - The nominal site infrastructure is modeled in a database stored in Orange's Flexible Engine (OpenStack)
  - An empty "tenant" is reserved in Flexible Engine for recovery and for testing
  - Nuabee agents are installed in the VMs (Linux or Winsows) of the nominal site
  - A complete copy of the data is transmitted to Flexible Engine and kept in the form of "object storage". This is a key point: the use of object storage is about 10 to 20 times less expensive than traditional block storage.

- Normal operations

  - Once or twice a day, agents transmit data associated with protected VMs (only blocks that have changed since the last time) from the nominal site to Flexible Engine object storage.
  - If there is a change in the infrastructure: for example, when adding a VM to be protected, an agent must be installed on this VM and the modeling database updated correspondingly.
  - For tests: protected VMs are automatically rebuilt from the modeling database, in the tenant space provided on the recovery site and tested with a snapshot of the data. Testing disturbs neither IT Production nor its protection.

- Fail-over in case of failure or disaster

  - The RTO (in this case 4H) starts running when the incident is reported to the service technicians.
  - Given its very low cost, the automatic reconstruction of the infrastructure can be launched on the recovery site without necessarily waiting for a fail-over decision: recovery of VMs (with agents) and creation of block storage from data backups in object storage.
  - If the decision is made, Production fails-over to the recovery site on Flexible Engine.
  - Network access is switched to the recovery site and applications are restored
  - After dealing with the issue of potentially lost data, the business lines can resume their activities on the recovery site.

- Fail-back: return to the nominal site relies on the same mechanisms, generally in a much calmer moment than the situation which required a fail-over.

With automated mechanisms that take advantage of cloud functionalities and inexpensive object storage, Nuabee stands out for ease of use, a good cost / risk balance and its ability to handle a wide variety of information system configurations.

With the solution of its partner Nuabee, OBS can offer a well-targeted response to the expectations of a large number of small and intermediate size customers.

A European Technological Agency: Level 2 Criticality "Hot"

Remaining in our logic of ascending "criticality", we now consider "Hot" recovery solutions that maintain an up-to-date protection environment, through continuous data replication with VMs ready to be re-established.

The customer we have chosen here is an intergovernmental agency coordinating spatial exploration projects carried out jointly by some 20 European countries. With a budget of 5.720 million euros in 2019, the agency employs about 2.250 people in a dozen locations in different contributing countries, each with a specific area of intervention.

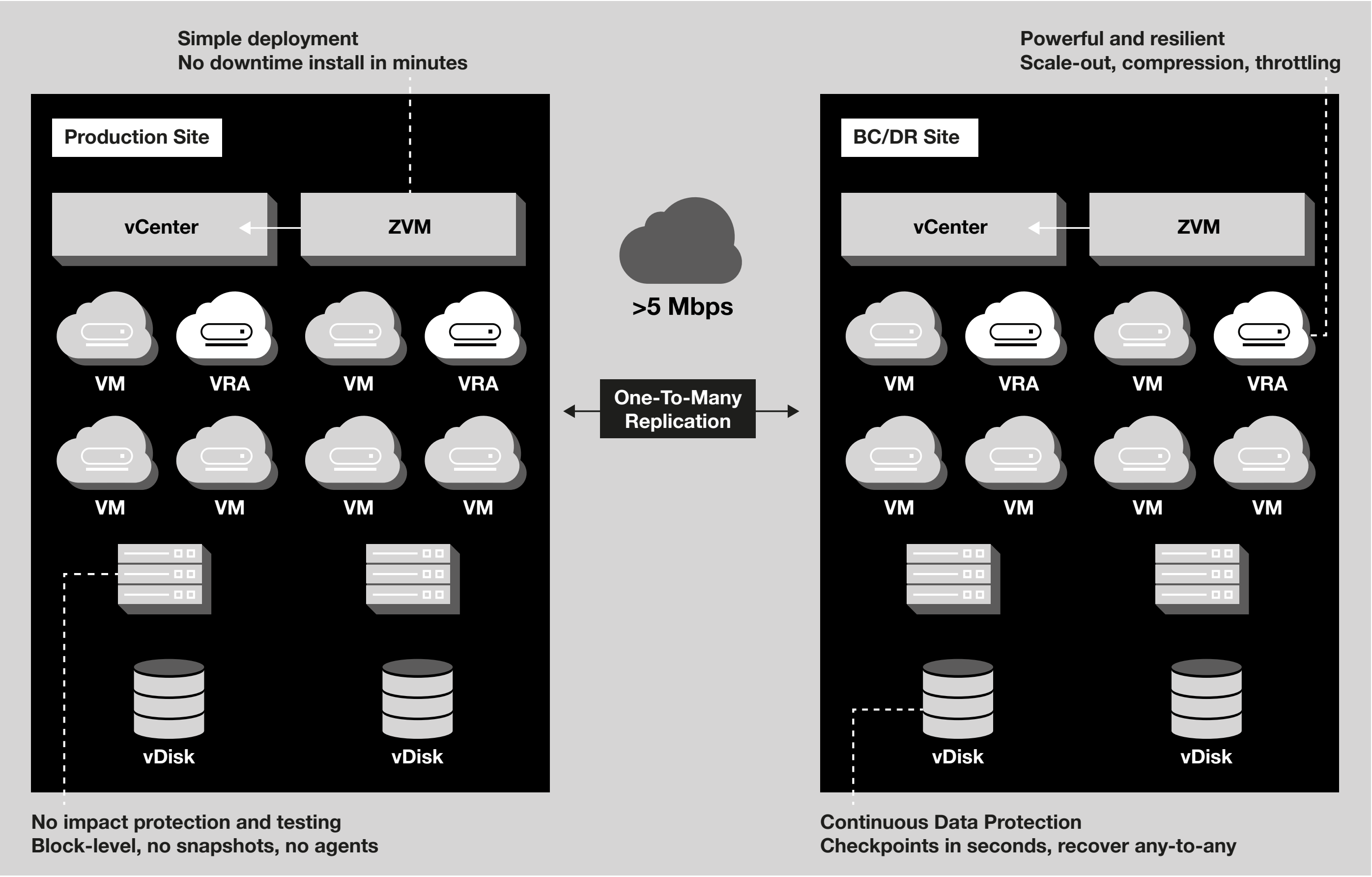
This award winning reference is so well known that we will make an exception to our rule of anonymous presentation. Connected readers can discover a two-minute video in which the customer IT managers explain their choice of private clouds and their need for an effective and rapid recovery solution. (watch the video).

In addition to the critical nature of applications and data in the private clouds in Italy and Germany, the issue of tests was crucial. In fact, the agency already had a recovery solution, but it could be tested only in "all or nothing" mode. It was not possible to test only one part of the workloads without affecting the others. In consequence, the existing solution was not tested frequently and there was real doubt about its effectiveness. It was crucial for the agency to be able to test recovery without disrupting production, while improving the flexibility and granularity of testing.

To meet these expectations, OBS implemented a recovery solution built on the IT Resilence Platform of Zerto, a technology leader and OBS partner. Since the applications and data in the two VMware clouds are completely unrelated and separate, the solution was set up in a "crossed Active-Passive" configuration, with each of the two sites serving as a recovery site for the other.

The general architecture of the solution with the Zerto IT Resilience Platform is presented on the following diagram:

General architecture: Zerto it resilience platform



The diagram presents the architecture for VMware cloud environments. Without getting into detail, we should mention two key components: the ZVM and the VRA.

- The ZVM (Zerto Virtual Manager) connects directly to the virtual management console (here, VMWare VCenter), providing visibility across the entire infrastructure. ZVM is the nerve center of the solution, managing the replication of the entire VSphere domain.
- The VRA (Virtual Replication Appliance) is a software module that is automatically deployed on physical hosts. The VRA continuously replicates data from user-selected virtual machines, compressing them and sending them to the remote site over WAN links.

The technical strengths of the platform are indicated on the diagram provided by Zerto, so we won't repeat them here. However, we will briefly summarize some key benefits of Orange's solution that were especially pertinent for the agency:

- Simplicity and flexibility for testing: this was a major requirement of this client and many others.
- Ease of implementation and use: this point is widely recognized in the market and highly appreciated by customers.
- Services: OBS not only implemented the solution but also remains responsible for the tests and, if necessary, for fail-over.
- OpEx pricing: after a one time implementation fee, the solution is priced as a monthly cost, adjusted for the number of protected virtual machines.

To conclude, it should be noted that OBS is not limited to the configuration of private-private cloud recovery, as in this example. With Flexible Computing Advanced; Flexible Computing Premium and Flexible Engine, Orange also has numerous references, in France, Europe and Asia-Pacific, with public-public cloud configurations.

In addition, OBS will also launch an offer of "Disaster Recovery As a Service" called **Flexible Recovery Advanced.** This offer responds to the market's expectations in terms of a private to public cloud recovery solution: no obligation to modify the private cloud and no need to invest in a shared cloud dedicated to recovery, together with a choice of customer support services and usage based pricing (OpEx) for customer cost optimization.

- **An international paramedical group: Level 3 of Criticality "HA"**

Moving beyond hot recovery, some companies and large organizations are even more demanding for the availability of their applications and data in the cloud. They require continuity of service without any interruption, be it to repair a technical failure in two hours or to mount a new version of software into Production or even to manage a data center disaster.

According to our typology by criticality, we put into the HA category (High Availability) solutions with 2 synchronous Active sites, hence separated by <40 km. With in principle RTO and RPO at zero, they allow transparent fail-over of users from one site to another, subject to certain shared risks in case of a regional disaster

The customer example here is a large paramedical company, which federates nearly 1,400 specialist stores in France and abroad. In addition to its technical expertise, the quality of in-store reception and personalized service to individual customers is at the heart of the brand's value proposition. The operation of the member stores depends on its main business application. If the application went down, the "customer experience" that the group wants to ensure would inevitably be degraded.

Moreover, as a company in a paramedical sector, it processes and stores very large flows of sensitive data such as scans of prescriptions and insurance documents, price quotes, invoices...

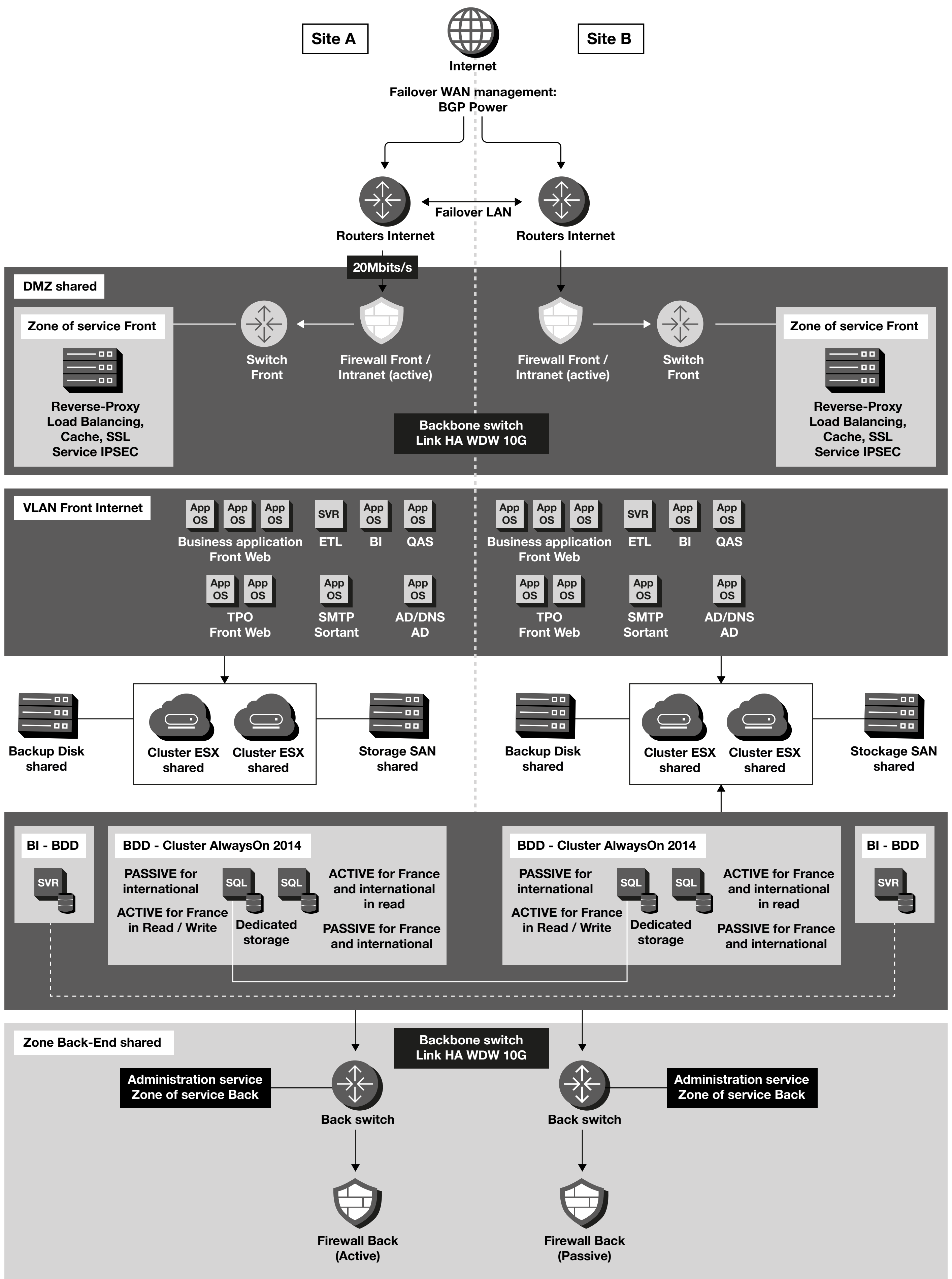
As a result, this group cannot tolerate any interruption of service or loss of data and we consider that these requirements place it at level 3 of criticality - High Availability (HA).

To meet the expectations of this customer, OBS implemented a cloud hosting solution with the following fundmental characteristics:

- Deployment on two Active-Active managed cloud platforms in the Paris region
- 24/7 high availability of the solution
- No service interruption: transparent user fail-over (one site to the other) if needed
- No loss of data in the event of a data center failure or disaster
- Added value services in addition to managed services

To make this a bit more concrete, the technical architecture of the solution - on both sites A and B - is presented on the following diagram:

« Always On » High Avaibility Architecture of Orange Business Services



We do not intend to examine in detail this (admittedly) somewhat complex architecture, but simply highlight some major technical aspects.

First, in the lower part of the schema, we see the keystone of the HA solution - a Microsoft SQL Server AlwaysOn data base cluster, deployed across both data centers with two nodes per site. In the event of a data center failure or disaster, the AlwaysOn cluster allows immediate fail-over to another node.

Given the critical role of the AlwaysOn cluster for high availability ensured by the two sites, the contract between OBS and the customer provides for a 1-hour RTO (as an exception) in the event of a data base cluster failure.

In this example, the customer has chosen a certain specialization of the data base back-ends of the two sites between France and International (including DOM-TOM). On the one hand, a read-only transaction (80% of volumes) can indifferently use either site. On the other hand, France transactional updates are normally processed on the back-end of site A and International updates on site B. However, all updates are immediately sent by "log shipping" from the first site to the other to synchronize the database.

Second, in moving up the diagram we can notice that all technical elements are present on both site A and site B and, in the "VLAN Front Internet" the same business applications are deployed on both sides, not to mention Active Directory which is essential software in Microsoft environments.

Finally, at the top of the diagram, we see the "load balancing" elements that ensure both the distribution of user workloads between the sites and the transparent fail-over of users from one data center to the other in the event of a failure or disaster.

In summary, with the HA AlwaysOn solution, Orange Business Services was able to meet the requirments of this paramedical group for uninterrupted continuity ... which the group deems essential for the quality of the "customer experience" it wants to provide in all the member stores all over the world.

- **A French bank: Level 4 of Criticality "Vital"**

To round out this chapter on customers and the answers to their expectations for continuity in the cloud, we will now consider the highest criticality level in our typology.

Although the HA solutions previously discussed - with two Active-Active systems fairly close (<40 km.) - generally provide a strong assurance of uninterrupted continuity, they nevertheless remain exposed to certain shared risks in the event of a regional disaster. In sectors such as Finance and some levels of public administration, this is not acceptable.

In this most demanding level of our criticality typology, we put HA configurations with two separate but nearby Active sites with, in addition, Hot recovery on a 3rd Passive site located at > 100 km avoiding the risks of a regional disaster shared by the two Active sites.

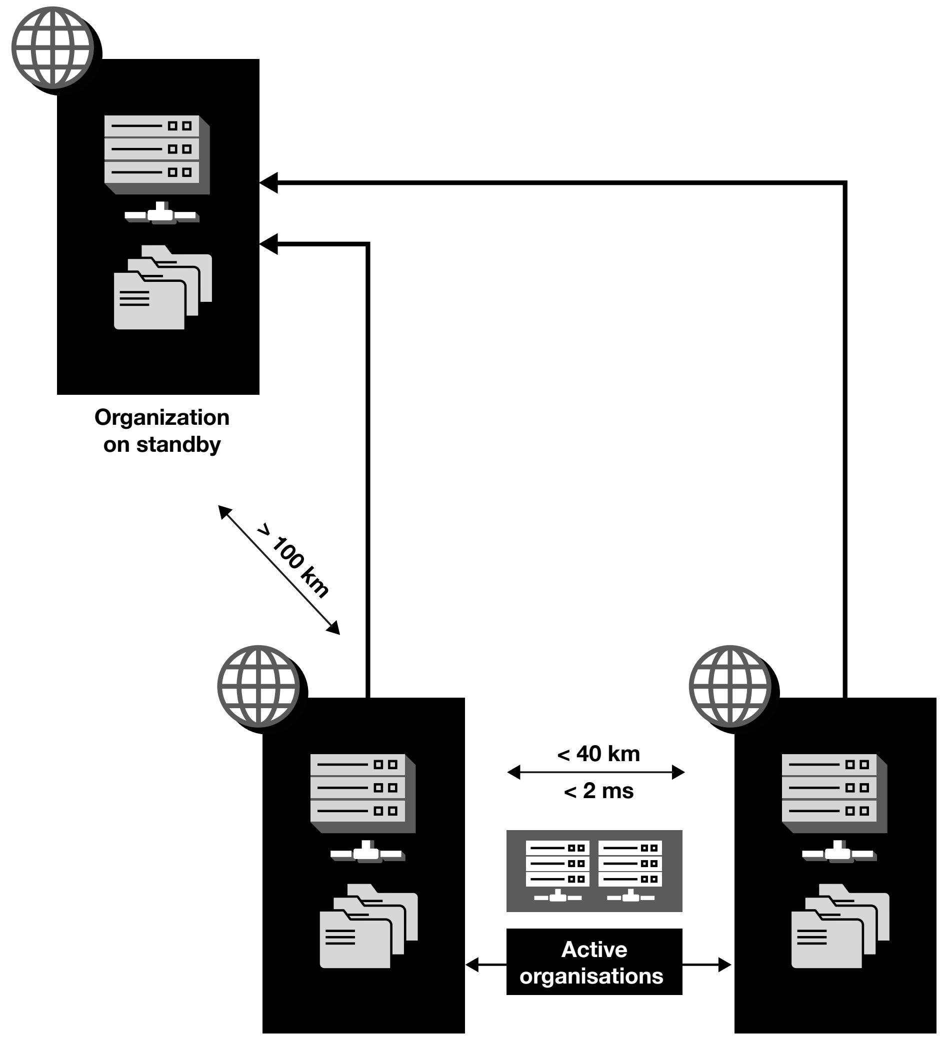
Here we take as an example a French bank widely implanted throughout the national territory with 17,000 points of contact, serving more than 10 million individuals but also businesses, professionals, social economy organizations and local public sector administrations. For both prudential and regulatory reasons, in 2014 - as part of an IT infrastructure renovation program that was already underway - it decided on a private cloud architecture, together with continuity and recovery solutions at the "Vital" level.

This mission was entrusted to Orange Business Service, which implemented three private clouds for the bank - with two nearby Active-Active sites and a third Passive recovery site located at > 100 km. - using technologies from VMware, Cisco, EMC and VCE.

This innovative private cloud project was priced in CapEx. Recently, however, OBS has launched an offering with a similar general architecture - also at the Vital level - in public clouds. Among the advantages of this new offering - named Flexible Resilience - is "Full OpEx" pricing. After one time fees for installation in Orange's public clouds, the solution is paid on a usage basis, depending on the number of VMs.

It is presented on the following diagram:

General Architecture of Flexible Resilience of Orange Business Services



As comments on the figure, we will simply highlight two points:

- The detailed HA technical architecture of the two nearby Active systems is very similar to what was presented in the previous HA section.
- The Hot recovery of the two active sites to the 3rd passive site at > 100 km. is ensured with Zerto technologies.

With Flexible Resilience, Orange Business Services can offer a well-targeted response to customers who want to take advantage of the public cloud and OpEx pricing, while at the same time being extremely demanding on the continuity of their applications and data in the cloud.

“ Orange Business Services, its customers and responses for their projects

- **Example criticality “Cold”:** implementation of cloud back-up functions of **Flexible Recovery,** based on Veeam technologies.
- **Example criticality “Warm”:** **the solution Nuabee,** for a nominal site on the OVH public cloud with a recovery site on **Flexible Engine** of OBS, implemented and managed by the partner.
- **Example criticality “Hot”:** implementation and management of a recovery solution (“crossed Active-Passive”) between two private clouds in Germany and Italy based on Zerto technologies. A similar offering **Flexible Recovery Advanced** – from private clouds to the public cloud **Flexible Computing Advanced** – will soon be available.
- **Example criticality “HA”:** implementation and management of a solution with two Active-Active sites on **Flexible Computing Premium,** leveraging in particular the Microsoft technology SQL Server AlwaysOn.
- **Example criticality “Vital”:** implementation (with CapEx) of a configuration with three private clouds - 2 nearby sites Active-Active with a 3rd Passive recovery site at a distance >100 km – leveraging technologies from VMware, Cisco, EMC and VCE. A similar offering **Flexible Resilience** – with OBS public clouds and payment in OpEx – is now also available.

#6 New challenges of multi-cloud environments

Over the last several years, Orange Business Services has developed a large portfolio of cloud based business continuity solutions with leading technology partners. As we have seen, this portfolio has enabled it to respond to many different needs of its customers, from small companies to large groups, in France and internationally.

However, the market is constantly evolving and new challenges are emerging. In this chapter we will discuss the new perspectives that are opening with the emergence of “multi-cloud”.

- **Multi-cloud : the new reality of the market**

According to conventional wisdom two or three years ago, most users would move all or part of their information systems into a single large public cloud, with only a few “hyperscales” dominating the entire market.

In fact, things didn’t turn out that way. While some companies opted to go “all in” with a single large cloud provider, most - as many studies show - use multiple partners and expect to use more in the future. The hyperscales have indeed developed rapidly but they work more and more in partnership with all kinds of players. In addition, a dynamic ecosystem of “cloud agnostic” software and services is taking shape.

- **Orange Business Services adopts a multi-cloud services strategy**

Having taken full measure of this new market reality, OBS announced on September 18, 2018 its ambition to become a world leader in multi-cloud services: “Orange Business Services chooses to be agnostic in cloud technologies”, positioning itself as an integrator and operator in a multi-cloud environment, whether public or private.

None of this suggests that the company will stop investing in its VMware and OpenStack cloud infrastructures, which are strategic assets for a multi-cloud services provider. It does however clearly mean that OBS is equally capable of providing services around the clouds of other players. OBS has signed agreements with hyperscales such as AWS and Microsoft and has already certified some of its engineers with Google.

This shift to multi-cloud is a game changer for the company’s activity of business continuity in the cloud. Previously focused primarily on its own platforms, the OBS “addressable market” has been greatly enlarged, especially since many of current cloud customers also use platforms from other providers. These customers will be able, if they so wish, to draw upon OBS expertise for the implementation (or even management) of business continuity solutions with a consistent approach for their multi-cloud environments.

- **Three major challenges**

To capitalize on this opportunity to better serve customers, Orange Business Services faces many challenges. Here we will only mention three.

- **Build new technical skills: hyperscales and open source platforms**

For a technology oriented services company, the complete technical mastery of the environments in which its teams will work is an absolute prerequisite.

OBS has already trained a number of engineers on the technologies of Microsoft Azure, AWS and Google Cloud Platform. It's a good start. However, the hyperscales are very rich environments that evolve quickly, and these investments in technical skills have to be sustained over time.

In business continuity solutions, OBS technology partners are already (more or less) cloud agnostic. In the case of "classic" applications, the implementation work will be similar to what OBS already does in VMware and OpenStack clouds, with some additional skills required. On the other hand, if the application uses proprietary hyperscale services (for example "serverless"), the work will be more complex. Simply replicating VMs (as Zerto does) on another cloud will not be enough, because these proprietary services must also be planned and configured as standby on the recovery site.

In addition, we shouldn't forget the specific expertise needed for open source platforms such as Cloud Foundry or OpenShift, not to mention the duo Kubernetes-Docker (containers) which has been chosen by many large groups. All of this adds another layer of complexity for the implementation of continuity and recovery solutions.

The training programs of OBS engineers are going to be loaded!

- **Prepare for the arrival of "Edge Computing"**

If the cloud paradigm has entered the mainstream of the market, a new model - more decentralized but complementary - is now emerging: "Edge Computing". You can't do everything in a centralized cloud. The basic problem is simply the speed of light!

New categories of applications - such as IoT (Internet of Things) systems or augmented reality applications - require very low network latency that is incompatible with processing in a large public cloud several hundred kilometers away. Intelligence must be brought as close as possible to the point of data capture.

Here again, continuity of service will be a vital necessity, both for large IOT connected infrastructures (cities, highways, power grids ...) and for companies in sectors such as Industry and Retail.

OBS has invested for years in connected objects and, in addition, operates large capillary telecommunications networks. With some other operators like Telefónica and AT&T Business, the company is well positioned to take advantage of this evolution, but it will have to integrate continuity of service (and of course security) into the design of these new "Edge" systems.

- **Make its strengths better known, build differentiation especially with Business Continuity**

Orange Business Services does not yet have the "brand visibility" that it should have in the IT market. With its shift to multi-cloud services, OBS has made the necessary decision, but this market is already crowded and differentiation is essential.

Even so, the company has been prescient in developing distinctive skills and experience in business continuity for the cloud, with a broad portfolio of solutions to respond to that expectation and requirement of mainstream customers, well before the arrival of multi-cloud.

Admittedly, OBS has other potential areas of differentiation to pursue, but in our opinion the time has come to promote aggressively this distinctive expertise – business continuity in the cloud - throughout the market.

New challenges of multi-cloud environments

- "Multi-cloud" is the new reality of the market, in terms of the choices of a very large number of customers as well as the strategies of providers of cloud services.
- In choosing to be "agnostic in cloud technologies", positioning itself as an integrator and operator in a multi-cloud environment whether public or private, Orange Business Services has made the necessary decision.
- Nothing suggests that the company will stop investing in its own cloud infrastructures, but OBS is also capable of supplying services in the cloud environments of other players.
- First challenge: Continue the development of new technical skills (hyperscales and open source cloud platforms).
- Second challenge: Prepare for the arrival of "Edge Computing".
- Third challenge: Make its strengths better known, build differentiation especially with Business Continuity.

#7 Concluding remarks

On July 3, 2018, Orange Business Services and Zerto won the “Best Cloud Customer Case” Trophy from EuroCloud France. The trophy was awarded for a business continuity solution implemented for the European Space Agency (ESA) between two private clouds in Italy and Germany.

This EuroCloud award illustrates, on the one hand, the growing importance of continuity in the cloud and, on the other hand, a beginning of recognition by the market of the distinctive skills and experience of OBS in this domain.

Given its culture as an operator of critical infrastructure, continuity and recovery - in the event of failure or disaster - are natural subjects for the company, as they are for the operators of electricity, gas or transportation networks. The life of the economy and the lives of everyone rely on these infrastructures and their services. So it’s not surprising that OBS approached the cloud market with the same culture of reliability, together with considerable investments made over the last few years.

Working with leading technology partners, OBS has brought to the market a broad portfolio of solutions for business continuity in the cloud, most of which are industrialized (“off the shelf”) offerings. Its ambition is to meet a variety of different needs of customers, from SMEs to large corporate groups, in France and around the world.

On behalf of OBS, we will conclude with the company’s commitment: Orange Business Services places itself at the service of its customers, so that they can find the right answers for their projects as they face a crucial challenge: ensuring the continuity of their business activities in the era of the cloud.

#8 About

Duquesne Group is a well known French analyst and consulting firm in information technology and business organization. Its partners are highly qualified senior professionals, with long experience in global consulting firms and leading technology market research organizations.

They combine a high level of technology skills with a business focused approach, and adhere to shared professional value of independence, service to clients and civic responsibility.

Their principal domains of expertise are Business Continuity and Information Security, together with the evolution of digital technologies in the era of the Cloud.

Their detailed analyses and blogs are freely available on the Web sites www.DuquesneGroup.com (French) and www.DuquesneAdvisory.com (English). They have also published various articles in the business and IT press and, in addition, one of the firm’s partners is the author of the leading reference book on Business Continuity in the French speaking world.

Duquesne Group is also a provider of training for professional development and ISO certification. In partnership with PECB, an international certification body, the firm provides training services in:

- ISO 22301 : Business Continuity
- ISO 27001 : Information Security
- ISO 31000 : Risk Management

While the firm is based in Paris, its culture is Franco-American, and it serves clients of all sizes and sectors in France, Europe and around the world.