Business

Service Description – Service Quality Commitments
Managed Applications

Table of Contents

Liste des figures

Liste des tableaux

1 Purpose of the document

The purpose of this service description is to define the conditions under which the Service Provider provides the "Managed Applications" service (hereinafter the "Service") to the Customer.

This description is attached to the Specific Conditions for Integration, Maintenance and Related Services.

2 Overview of the Service

2.1 Overall description

The service Managed Applications provide to Customer the following management levels:

1. **Governance and advisory services**: governance to drive the project and additional guidance and advisory services.
2. **Managed OS:** Operating system management including tasks related to the server and supplementary upgrading activities,
3. **Managed database:** This service provides the Customer with complete database management, including tasks connected with the server and optimisation and upgrading activities.
4. **Managed middleware** including all software offered in the catalogue by the components:
    - Web server
    - Proxy server
    - Application server
    - File server
    - DDI
    - Source Code Manager
5. **Managed Service for Kubernetes®:** As part of this service, the Provider manages Kubernetes® clusters hosted on the Public Cloud IaaS Cloud Avenue infrastructure (The Provider).
6. **Managed application:** Customer business application management (e-business web, ERP, CRM, Finance, HR, etc.) based on Customer procedures except SAP.
7. **Managed Hyperscaler Native Services**: monitoring and operation of cloud native services and hyperscaler PaaS services (Azure, AWS, GCP, FE).
8. **Managed Big Data:** Installation, monitoring and operation of Big Data solutions managed by the Service Provider, including the Log as a Service (LaaS) solution for end-to-end log analysis, which supports in-depth research, analysis and visualization of logs generated by different machines.
9. **Managed Computer Vision:** a solution that uses Artificial Intelligence techniques to enable customers to extract data from their video equipment (cameras) through alerts and dedicated dashboards.
10. **Managed RDS:** management of the Customer's RDS (Remote Desktop Service), enabling users to access Windows applications remotely, hosted on a Public Cloud IaaS infrastructure provided by the Service Provider or Partners (AWS, Azure, GCP).
11. **Managed AD:** the Managed AD Service is a service provided by the Service Provider, which manages authorizations and access to users and resources in the form of a directory.
12. **Managed Security:** Installation, monitoring and operation of security components managed by the Service Provider.
13. **Managed Citrix Workspace:** The Managed Citrix Workspace Service is a service provided by the Service Provider that enables the management of the Customer's Citrix Workspace on the Service Provider's infrastructure.
14. **Managed Exchange:** The Managed Exchange Service is a service provided by the Service Provider that manages the Customer's Tenant's Exchange messaging system.

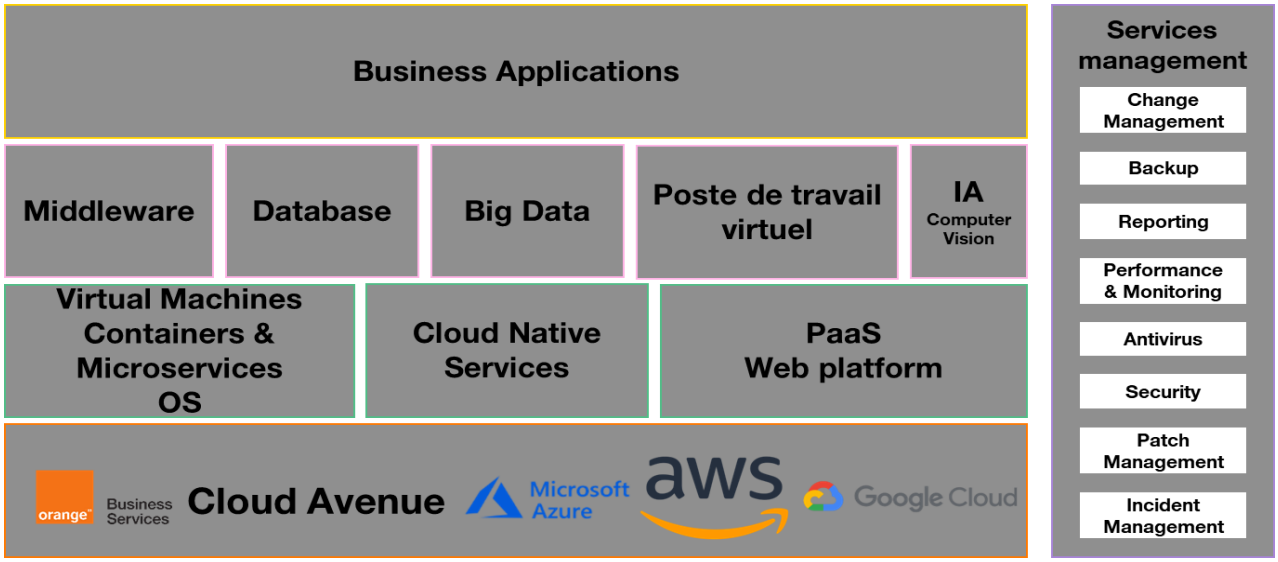


Figure 1 – Managed Applications service catalog

The Customer has the possibility of subscribing to different levels of management to for a single Project, however:

- For the managed database and managed middleware management levels, the Customer is required to subscribe to the managed OS management level as a pre-requisite.
- At the Managed Application management level, the Customer is required to subscribe to the managed OS management level, the managed database and managed middleware management levels, or to the managed service for Kubernetes® with tools Devops level, as the application requires that the related components be implemented in order to function.

Each of the Managed Tenant's virtual servers (VM) may have one of the possible management levels. The management level applies to the server in its entirety; different software cannot be hosted at different management levels on a single server.

Each of the Managed Tenant's for Kubernetes cluster may have one of the 2 possible management levels (managed Kubernetes, managed application on containers).

The Customer chooses at the time of ordering a support level among the available (Standard, Premium,) that applies to the entire Service. If the Customer wishes to benefit from different levels of support, he must subscribe to several Services, which will be deployed on separate Managed Tenants.

2.2 Geographical footprint

The Customer may subscribe to the “Managed Applications” Service on any IaaS proposed in the Order. The Region is selected by the Customer at the time of Order and recorded in the high level design document. The Service is available in France and abroad.

3 Management models

The Service Provider can support Customers in different ways for their use of the cloud.

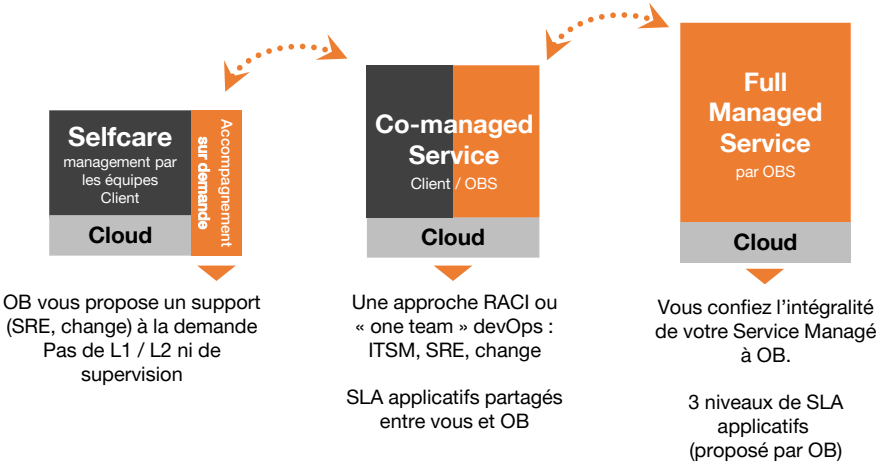


Figure 2 –Managed Applications management model

The **Fully Managed** option is a model by which the Service Provider takes care of all the deployment, the supervision, the operations of the workloads of the Customer. The Customer has the responsibility to provide a fully tested workload. This model is best suitable for the stable applications and workloads with a low amount of modifications and transformation. It provides operational efficiency.

The **Co-managed** model, whereby the Customer and the Service Provider share the responsibilities the deployment, the supervision, the operations of the applications and workloads. In this model, the Customer is taking care of the development and testing of the application. The Customer can propose deployment templates thanks to change process. The Service Provider is responsible for the monitoring and maintenance 24 x 7 inclusive of non-business hours and non-business days and / or 8 x 5 for less critical workloads. Both collaborate using a Git referential, a Continuous Integration and Deployment Chain and a shared tooling for monitoring, logging, alerting, dashboards and communication. This model is an efficient compromise for getting the development agility, transformation of the application and frequent push to production, while keeping an efficient service assurance through delegation to the Service Provider and preserving the critical development resources towards most value-added development tasks. The Co-managed model can be complemented with Cloud Center of Excellence or Cloud Expertise.

The **Selfcare** model, whereby the development team of the Customer is fully responsible for the development, the deployment, the supervision, the operations of the workloads. In that model, the Service Provider can propose professional services to the Customer, typically under the form of a **Cloud Center of Excellence or Cloud Expertise** to help the Customer setting the DevOps pipelines, tooling, landing zone and build to run activity. In this model, no Managed Services are offered. This model is best suitable for applications and workloads subject to intensive development and modifications with frequent deployments to production. Drawback is that the developers need to be mobilized in 24x7 and need to take care for some operational aspects during the whole project life.

Each customer case is specific, yet the Co-managed model is taking momentum especially with the use of Cloud Native functions / PaaS functions of the clouds.

The service description in this document **applies to both full managed and co-managed services**. During the presale or consulting phase, the Customer and the Service Provider will agree to the model of managed services required and adapt the RACI accordingly. This may vary from one Customer to another, from one service or application to another.

3.1 The co-management run delivery model

The scope of work and the delivery model for the run is established during the pre-sales phase depending on customer's needs. The present chapter establishes guidelines which will be adjusted depending on the customer scope of work.

The Level 3 are the experts about the service component. They are the most knowledgeable to troubleshoot and resolve an incident on the service component. They implement the observability, the alerting and the procedures for troubleshooting, the backup, and the procedure for repairing the service component. They validate the procedures and handoff those procedures to the Level 2. They troubleshoot incidents and problems in last resort when the Level 2 cannot fix it.

For a Business Functions of the Application, the Level 3 is typically customer's responsibility: Customer's development and test teams - or 3rd party teams subcontracted by the customer - who have coded, deployed and tested the Business Application and the Business Function. Customer may contract support to the software editor of the Business Application and Business Function.

Customer can subscribe SRE and Cloud Expert Services from the Service Provider to strengthen the team.

Would the customer request the Service Provider to take responsibility for the Level 3 of a 3rd party Business Application (with a potential partner for 3rd party application maintenance), a specific scope of work and agreement shall be established.

For the IaaS, PaaS, OS, Database, it is typical that the customer may rely on the Service Provider to take care of the Level 3. However, other patterns are possible and can be discussed and established during the presale phase.

Here is an example of responsibility pattern for a project:

Component	Level 3	Level 2	Service Desk / Level 1	Comment
Business Application	Customer devops team with contribution of SRE	OBS based on procedures provided by Level 3	OBS	
Business Function	Customer devops team with contribution of SRE	OBS based on procedures provided by Level 3	OBS	
External Interface	Owner of the interface (3rd party ?)	Notifies customer	OBS	Owner of the interface may be a 3rd party
Business Function specifics metrics and alerts on Micro-services, MW, DB, IaaS, PaaS	Customer devops team with contribution of SRE	OBS based on procedures provided by Level 3	OBS	
Middleware	Customer with support of 3rd party editor	OBS based on procedures provided by Level 3	OBS	
Middleware (part of OBS portfolio)	OBS L3	OBS	OBS	Supported middleware and middleware versions
SAP, SAP Hana	OBS L3	OBS	OBS	L3 for SAP business workflows with a partner
Map reduced, ELK (Big data)	OBS L3	OBS	OBS	L3 for Big Data business analysis with a partner or OBS D&D
Database	OBS L3	OBS	OBS	Supported DB versions
Kubernetes cluster	OBS L3	OBS	OBS	
OS	OBS L3	OBS	OBS	Supported OS versions
IaaS & PaaS Cloud Native Services	OBS L3	OBS	OBS	Support from CSP shall be subscribed by customer / or IaaS / PaaS resold by OBS

Figure 3 – Example of a responsibility matrix

Note: for some solutions in Service Provider portfolio, typically Managed SAP, Managed Computer Vision, Flexible Web Platform, Hub EDI, Corporate e-Invoicing, LogaaS, The Service Provider takes the responsibility for the Level 3 and has established partnership and support agreement with the involved 3rd party applications maintenance or software suppliers.

4 The build of services & managed services

4.1 The build and deployment scope of work

The **Full Build** and deployment of a business application, services and managed services on a given cloud platform involve:

- **The build of the cloud infrastructure including:**
  - The Landing Zone transversal for multiple applications
  - The cloud infrastructure specific to each application
- **The deployment of the business application software on the infrastructure**
- **The build of the operations layer including:**

    - The selection and configuration of tooling used for operations, including tooling services of the given platform
    - The configuration and deployment of exporters of observability metrics, logs, agents, backup and other operational parameters necessary to the operations
- **The integration into the Service Provider administration backend including:**
    - Provision and connectivity for administrative access to the cloud platform
    - Integration of GCP monitoring alerting towards the Service Provider Level 1 / 2 & 3 supervision tooling
    - Integration of troubleshooting procedures into operations Knowledge Database
    - Configuration and provision of the Service Provider's ITSM tooling for Incident Tickets and Change Requests handling.
    - Configuration and provision of the Service Provider's portal for access to contractual documents and billing.

At the end of the build, all pre-requisites shall be available and ready to meet the criteria for the run.

Depending on the project status and on customer's request, **the remaining Scope of Work for the build to meet the criteria for the run may be the full build or a partial build.** The scope of work of the build is discussed during the pre-sale phase.

The customer **may retain or delegate part of the Build responsibilities to the Service Provider:**

- The Build of the Cloud Infrastructure layer (IaC)
- The Build of the Operations layer
- The integration into the Service Provider administration backend tooling

The Build effort estimation is custom and depends on the Scope of Work of the project. Upon customer's request, the Service Provider can provide **Cloud Expert resources** and **Service Reliability Engineer** prestation to join and strengthen customer's development team.

While the build effort and its estimate can be custom, for sake of simplification and budgetary anticipation by the customer, the **Service Provider has pre-defined 4 models of build** for a managed cloud native resource:

- **Model "No build":** no build requested from Service Provider – resource is not managed.
- **Model "Backend build":** The Service Provider is only requested to integrate in its administration backend. The customer takes care of all other aspects of the build
- **Model "Operations build":** The Service Provider is requested the build of the operations layer and the integration in its administration backend. The customer takes care of the build of the infrastructure and software deployment
- **Model "Full build":** The Service Provider is requested to build the infrastructure with IaC, to build the operations layer and to integrate in its administration backend. The customer takes care of the Software.

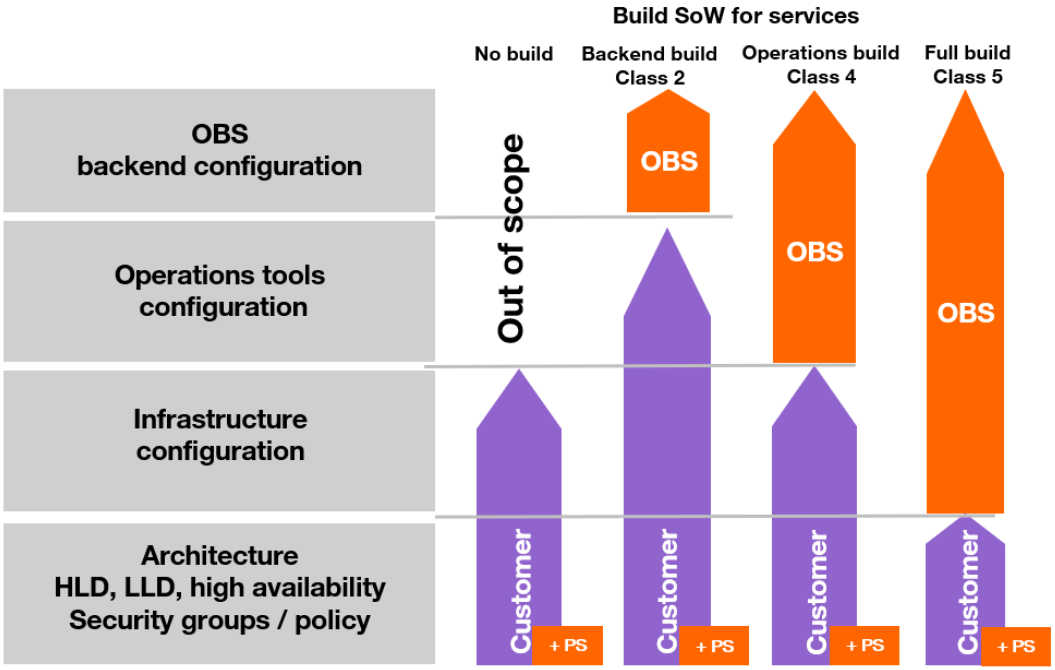


Figure 3 –Main models of build Scope of Work requested to the Service Provider

As far as the Scope of Work is concerned, building the first cloud native resource of a given type usually involves a larger effort than building a subsequent resource of same type, as the Infrastructure as Code might be mostly reused. This possibility depends on the cloud native resource considered.

As result, **each build model distinguishes:**

- **The effort and price of build for the first resource of a given type**
- **The effort and price of build for the subsequent resource of the same type**

For the Scope of Work differ from the models, a custom scope of work shall be estimated.

4.2 Project management and coordination during the build phase

During the build phase, a Scope of Work is defined for Project Management and Service Implementation Coordination to ensure efficient execution of the project between the Customer and the Service Provider.

Optionally, the project may require **Cloud Expert Services, Service Reliability Engineering** or **Data Reliability Engineer.**

Those services are charged based on time and material.

4.3 Detailed build methodology

The following chapter describes the build methodology followed by The Service Provider for the **Full Build** model. It is also the method recommended to the customer when building his cloud infrastructure and operations layer.

The quality of the build will determine the resilience, the maintainability, the recovery of the workloads and the efficiency of the run operations.

The methodology varies from one project to another and as such the quote is specific and depends on the scope of work.

4.3.1 Inputs to the build

For proper accurate quote of the build and kick-off of a build task the following specifications are pre-requisites:

- Architecture diagram of the application and its layout of deployment on GCP services

- Description of the environments required (Dev, Pre-Prod, Prod)
- Security policies and access control
- Environments topology
- Type and inventory of applications, middleware, IaaS/PaaS services used
- Scope and RACI

Should the Customer provide the information during the pre-sales, the Service Provider would quote the build accurately.

Alternatively, should the Customer not have such information during the pre-sales phase, then generic hypothesis would be taken for the build estimation. The build specification and quote would be updated during the initial phase of the project after an audit or after the information is provided.

Nevertheless, please find here-below the Service Provider default reference approach for building Managed Services on a given platform. The scope of work will vary depending on a Customers' projects.

4.3.1.1 Initialization of the project: building the landing zone

At the start of the project, we build a "**Landing Zone**".

We use **Infrastructure as Code** (IaC) for quality, replicability and disaster recovery. Cloud Platform services are deployed using this IaC, as opposed to using the man-machine interface:

- Deployment code can be tested and validated on a non-production environment (e.g. dev, integration, staging, preprod) before going into production.
- Can be duplicated and evolved
- Can be used to restore service after a disaster.
- Can be versioned
- Can combine resource deployment and operations configuration (monitoring, logging, backup, etc.).
- Optional: when available in a multi-cloud tool, e.g. Terraform, IaC can be exploited for other clouds with minimal changes.

By default, the Service Provider uses **Terraform and cloud-native** tools as the IaC language.

- Terraform is more generic and can be used on several clouds with limited adaptations.

IaC is managed with a tool chain:

- By default, the preference would be to use Terraform.
- As an option, multi-cloud platforms can be offered on the basis of cloud-agnostic **OpenSource** such as Concourse, Gitea / Gitlab, Terraform and Rancher, Quay for containers. In this case, a specific estimate will be made for the use of these tools, separate from the Cloud Platform subscription.
- The use of a customer-specific Software Factory requires an assessment of feasibility and scope, as it has an impact on Build and Run processes.

3 main parts of **IaC** are leveraged:

1. **The GIT-based repository where the IaC code base is stored and versioned.**
2. **Pipelines for Build**
3. **Pipelines for versions/modifications**

Based on the specifications, the Provider's IaC developer assigned to the Build will code the IaC and prepare the pipelines for the Build according to the Terraform plans.

For example, the code may be structured in several **Build pipelines** and Terraform plans for :

- underwriting,
- management
- Identity
- VM
- database
- etc...

The IaC developer will test the quality of the code.
Example

- He makes a pull request on the master branch.
- He automatically launches a Terraform Format, a Terraform validate to validate the syntax.
- It launches a deployment on the Cloud platform to validate correct deployment.

The Service Provider's IaC libraries save time in developing the IaC, but projects often have their own specificities and require adaptations and customized developments.

Next, the Provider's developers create the "**deployment pipelines**".

- ⇨ The deployment pipeline is the way IaC is deployed on each Cloud environment.
- ⇨ The deployment pipeline automates the process of deployment on the dev platform, then integration/staging, then preprod, then production as an example if the Customer has such environments.
- ⇨ The release pipeline is a code base that evolves according to the environment.
- ⇨ For each environment, the Service Provider's IaC developers define **environment variables** to adapt resource consumption to the platform: for example, a small VM for dev, a large one for prod.

Custom development may be required to meet the customer's specifications, and will be the subject of a specific quotation. For example, the implementation of a DNS forwarder for platform connectivity.

The Service Provider's developer enriches the IaC Build pipelines with **Operation tools**, i.e. supervision, logging and backups. The connection to the Managed Application Provider's central supervision system is then configured to alert level 1 in the event of an incident.

If the customer subscribes to managed services for the application layer, this will be added to the pipelines using Ansible or Jenkins. The pipeline can be decoupled or combined with the infrastructure layer.

Application layer pipelines can deploy applications on a variety of services, whether IaaS, Kubernetes, DBaaS or PaaS, taking advantage of greater or lesser decoupling from the underlying infrastructure, greater or lesser agility and separation of tasks between application management and infrastructure management. This architecture is a key factor in bringing agility to application developers through PaaS automation of the underlying infrastructure layers. It also determines the RACI between the Service Provider and the customer's developers.

Several RACIs can be envisaged between the Customer and the Service Provider, depending on the desired level of delegation or on the environment platforms.
For example, there may be a Software Factory for application code under the Customer's responsibility, deployed on an infrastructure managed by the Service Provider via a Software Factory separate from the Infrastructure.

Example 2: Developers can test alarms themselves in the development, integration and staging environments and then, thanks to SoW and procedures, these alarms can be used by the Service Provider to monitor the production environment.

4.3.2 Transition from build to run

The Service Provider Managed Applications promotes the principle by which the team in charge of the run develops the IaC. Nevertheless, the developer of the IaC needs to explain the use of it to the whole team involved in the run including how to edit and release.

5 Managed Services Run

The items below describe how the service is managed, as operated by the Provider, for all services provided.

Services are organised as follows:

- The Services Center, and more specifically, the Customer Support Center,
- Services Support, with the following processes:
  - change management,
  - incident Management,
  - problem management,
  - Configuration management,
  - Release management.
- Services provision, with the following processes:
  - service level management,
  - availability management,
  - continuity management,
  - capacity management,

5.1 Organisation of Support

The Services Center establishes 2 contact points via which the Provider can gather Customer demands (e.g.: change, modifications, dysfunctioning, etc.) in order to provide responses.

The two contact points are as follows:

- The Provider **Customer Support Center** (CSC), available 24/7, throughout the year. Each CSC enjoys visibility on the entirety of the service and customer applications hosted,

- The **Managed Services Manager** (or SDM, for Service Delivery Manager), as part of Premium Support.

The purpose of the Provider support is to manage Requests and Incidents, by carrying out the following actions:

- Take charge of the Requests and Incidents, and processing and resolving them;
- Communicate the appropriate, up-to-date information to the Customer regarding the processing of the Incidents and Requests which have been duly reported;

5.2 Customer obligations

The Customer establishes and maintains a nominative list of contacts authorized to report incidents and to contact the Service Provider's Service Desk. The Service Desk responds only to duly designated persons in possession of their login and access codes.

The customer's main contact guarantees that contact information is up-to-date and valid.

5.3 Support plans

The Provider offers the following 3 levels of support, depending on the criticality level of the applications for which the Service is intended: **Initial, Standard and Premium**.

These 3 levels of support are available in 2 support chains **Off-Shore** or **Full France**, both determined during the Pre-Sales phase with the Service Provider's experts.

Table 1: Service package by level of Support

Managed Applications		Initial	Standard	Premium
Support Service	Service opening	8x5	24x7	
	Through the Cloud Store Portal	✓	✓	
	By mail	✓	✓	
	By telephone. Limited to 5 named contacts.	✓	✓	
Managed OS		Initial	Standard	Premium

Supervision	Infrastructure supervision	✓	✓	✓
	Operating system supervision	✓	✓	✓
Capacity management	Reporting on infrastructure use (VM)	✓	✓	✓
	Reporting on resource use by VM (ram/cpu/disk)	✓	✓	✓
Managed Database		Initial	Standard	Premium
Supervision	Database supervision	✓	✓	✓
Capacity management	Reporting on resource use by database			✓
	Capacity review (using history and trends)			✓
Managed Middleware		Initial	Standard	Premium
Supervision	Middleware supervision	✓	✓	✓
Capacity management	Reporting on resource use by middleware			✓
	Capacity review (using history and trends)			✓
Managed Application		Initial	Standard	Premium
Supervision	Application supervision	✓	✓	✓
Version management	Max. number of versions per month	1	2	4
	Execution scripts delivered by the Customer for deployment automation	✓	✓	✓
	Previous versions maintenance			1 month
Capacity management	Reporting on resource use by Application (ram/cpu/disk)			✓
	Capacity review (using history and trends)			✓

Support service subscriptions are taken out for a minimum of 6 months. The Customer may modify its order only to move to a higher-range support offer during the commitment period. It then commits once again for 6 months at the new subscription level.

Changes in support level come into effect at the start of the calendar month.

5.3.1 Level 0 Support (Service Desk)

The Service Desk represents level 0 of the Customer Support Center and provides the following services:

- a single point of contact for customer-designated representatives
- a single telephone number and a single e-mail address,
- exchanges in French ou English,
- handling and processing of customer telephone calls,
- identification of the caller and his commercial offer,
- the opening of an incident ticket or exchange ticket relating to the handling of customer calls,
- redirecting the ticket to the appropriate level 1 team,
- transferring the customer call to the Level 1 team.

The Service Desk operates 24 hours a day, 7 days a week.

Customer requests are recorded in tickets in the Service Provider's repository. Information is entered into the ticket in accordance with the procedures described in the documentation produced after service initialization.

5.3.2 Level 1 Support

Level 1 Support provides the following services:

- ticket classification,
- initial processing of tickets
- incident recovery management (request for Level 2 teams),
- customer communication,
- management of customer requests,
- alerting to trigger the major incident and crisis management procedure,
- closing tickets.

Proactive management is carried out by a Level 1 Monitoring team (standard process). This team is responsible for events affecting infrastructure and service elements. For events corresponding to impacts or risks of impacts on the service, the team opens a ticket in the Océane incident management application and carries out the initial diagnosis (standard process).

Level 1 Support operates 24 hours a day, 7 days a week.

Tickets stored in the Service Provider's repository are used to record all customer contacts and actions taken, and to activate (if necessary) Level 2 teams.

Tickets remain the responsibility of Level 1 until the ticket is closed and a ticket closure notice is sent to the customer.

5.3.3 Level 2 Support

Level 2 Support is available 24 hours a day, 7 days a week. During French non-working hours, Level 2 support is provided by off-site staff on call.

Level 2 Support ("Technical Management") provides the following services:

- change management: under the supervision and responsibility of the SDM, and after analysis of technical impacts, contractual commitments, completeness of procedures and feedback, and after risk assessment, carries out "change management" actions,
- event management: handles Warning-type events and, if necessary, triggers incident, problem or change management for these events. N2 monitoring support configures monitoring tools and hypervisor.
- Incident management : Level 1 Service Desk support: provides support in resolving incidents that do not fall under the responsibility of level 1 (complexity, new problem, risk of non-compliance with contractual SLAs),
- problem management: under the guidance and responsibility of the SDM, participates in problem management, analysis, follow-up and proposal of technical/functional corrective and/or remedial action,
- production launch: under the guidance and responsibility of the SDM, implements changes,
- ticket management: under the guidance and responsibility of SDM, manages support teams and relations with partners in the context of incident resolution, problem management and/or change management,
- manages on-site interventions by local teams,
- production performance monitoring: Capacity Planning,
- support to SDM: for incident reports, dashboards, operational customer meetings,
- application of escalation procedures,
- operational maintenance of technical components and associated procedures: for example, updating the procedures used by the Service Desk and Level 1 Support.

These documents evolve throughout the life of the project, under the responsibility of the RUN teams.

5.3.4 Level 3 Support

Level 3 Support provides its services during French working hours.

Level 3 Support (or Engineering) provides technical support to Level 2 Support, and may contact the Service Provider's suppliers and partners if necessary.

Level 3 Support also covers the following activities :

- industrialization and documentation of technical platform components (hardware, operating system, application products, databases, etc.),
- proactive monitoring of technical developments (hardware and operating system upgrade proposals, etc.),
- integration of major application releases.
- management of support access authorizations
- management of access to publisher support (Microsoft, etc.)
- definition of business rights and associated restrictions (access to Cloud, AD, CyberArk)

5.4 Incident Management

The Provider includes an incident management process, including the opening of tickets towards the Customer's IaaS supplier by the Provider. The aims of this process consist of:

- Responding as soon as possible in the event of actual or potential breakdown in Customer applications hosted,
- Maintaining communication between the Provider and the Customer regarding the situation stemming from the incident,
- Assessing the incident to determine the risk of its reoccurring or whether it is a sign of a chronic issue.

The Provider addresses incidents:

- proactively, when an incident has been detected by the supervision tools,
- In response mode, when an incident has been reported by the Customer via the CSC.

The incident management stages (whether reported proactively or in response mode) are as follows:

- Incident taken into account,
- Incident categorised by degree of Priority,
- Analysis and diagnostic review,
- Resolution and resumption of activity,
- Incident case closed following Customer agreement.

5.5 Change management

The entry points for a request for change are as follows:

- The Cloud Store Portal
- The Customer Service Center,
- The Managed Services Managers, for Customer contracts benefiting from the Business or Premium support levels

Any non-standard request for change is submitted to the Provider validation and may be rejected.

The list of persons authorised to submit requests for change is updated by the Customer and addressed to the Customer Service Center or to the Service Delivery Manager so that the modifications can be incorporated.

If the request for change is originated by the Provider, the Customer's explicit agreement is sought before implementation can begin. An exception will be made to this procedure where the change was required in response to an Incident of Priority level 1, as defined in the Service Level Agreement. In that event, the Provider notifies the Customer as promptly as possible following implementation of the change.

Through the Cloud Store Portal, the customer can access to the change catalogue for raising the change request. An act of change during standard business hours will be charged the equivalent costs of number of Tokens as indicated in the catalogue. When performed outside the Business Hours or the Business Days of the delivery centres, an act of change accounts for the double (x2) of the number of Tokens indicated in the change catalogue.

The Customer may purchase Tokens on demand or subscribe one or more monthly Token packs, which must be purchased until the end of the commitment period. Tokens not consumed from a pack are not carried over to the next month.

5.6 Release management

The Provider incorporates upgrades offered by hardware and software suppliers. This includes minor updates - patches, corrections, service packs - as well as major upgrades.

Major upgrade application is considered an additional service and will be invoiced as such to the Customer.

When the Provider decides to produce a new component, the production launch procedure is treated like a request for change, in line with the rules set out for change management.

The Provider ensures that all production servicing is traceable, thanks to an operation tool used by the CSC. These data are stored by the Provider throughout the Contract period and shall be considered as authentic by the Provider and the Customer for execution of this contract.

5.7 Configuration management

The Provider manages the reference bases containing the configuration for all elements included in the Service.

5.8 Scheduled maintenance

Recurring maintenance intervals are specified in the PQSC.

In addition, certain administration tasks, such as patching and security maintenance, are carried out proactively by the Service Provider.

Recurring security updates will be deployed in agreement with the customer on a predefined schedule over one year.

Exceptionally, the customer may be notified in the event of urgent and/or important action deemed necessary by the Service Provider for the protection and proper operation of its managed environment.

5.9 Infrastructure services included

5.9.1 Antivirus service

This solution is composed of antivirus software installed on each server (Endpoint Protection).

5.9.2 Managing patches and “service packs”

The Service Provider provides the Customer with patches and service packs for 3 levels of management:

- Managed OS
- Managed database
- Managed middleware

Updates are tested and validated by the Service Provider before being authorized on the platform.

The Customer validates whether or not patches are applied.

The Service Provider cannot be held responsible for any problems related to service pack deployment. The Customer may request the restoration of the last virtual machine image.

5.9.3 Supervision Service

The Provider undertakes to test the Customer solution infrastructure and application components to ensure smooth operation 24/7 and 365 days a year, at each management level (OS, database, middleware and Application) for which it is responsible. Any dysfunction alert confirmed by the supervision teams will give rise to an incident report with the Help Desk.

5.9.4 DNS Services

The Provider will provide two DNS services to respond to the following needs:

- Internet address resolution
- Customer Public DNS entry management

5.9.5 NTP Services

The Provider makes an NTP server available as the default time server.

5.10 Managed backup and recovery service

This Service allows the Customer to back up and restore **at the file level** the content of servers deployed in **physical environments** or in the **Cloud.**

The Customer can also benefit from the Office 365 Managed Backup. It allows to backup data from Office 365 applications: Exchange Online, SharePoint Online, OneDrive for Business and Team. It also provides full management of granular recovery of Office 365 data by application and backup policy.

This Service is based on a BaaS backup solution (integrated into the Provider's infrastructure). The cost of the BaaS Service is borne by the Customer as part of the underlying IaaS offer.

5.10.1 Description

The backup and recovery service includes the following services:

Table 2 : Backup & recovery description

Phase	Activities
Backup & restore Implementation	▪ Install and configure the agent on customer servers ▪ Configure the central backup platform to perform backups and restores on customer servers ▪ Perform an acceptance test
Backup & restore Operation	▪ Monitoring of client backups ▪ Restart backup in case of failure ▪ Perform restores on customer request (via change) ▪ Monitor the backup platform on a 24x7x365 basis ▪ Evaluate, schedule and execute system change requests ▪ Capacity planning on the backup platform

5.10.2 Caractéristics

The Backup and Recovery Service can be provided to Customers who already subscribe to the Managed OS, Managed Database, Managed Middleware, Managed Application services. This Service can also be provided to Customers who have on-premise or cloud-based data backup/recovery needs.

The following frequency and retention policies are predefined in the Provider's backup system.

The first backup in file mode or for Office 365 performed by the Service Provider is a full backup, the following backups are incremental according to the backup policy chosen by the Customer.

Table 3 : Standard retention policy

Retention policy	Policy Details	File / Office 365	
WEEKLY-1	Weekly backup with 1 week retention	✓	
WEEKLY-2	Weekly backup with 2 weeks retention	✓	
MONTHLY-1	Monthly backup with 1 month retention	✓	
MONTHLY-3	Monthly backup with 3 months retention	✓	✓
MONTHLY-6	Monthly backup with 6 months retention	✓	✓
MONTHLY-12	Monthly backup with 12 months retention	✓	✓

Retention policy	Policy Details	File / Office 365	
MONTHLY-36	Monthly backup with 36 months retention		✓

Customers may request specific retention policies and customized backup frequencies. Specific requests are submitted to the Service Provider for approval and will be quoted to the Customer.

5.10.3 Limitations

The following activities remain the responsibility of the Customer:

- Full acceptance tests which will be recorded in an acceptance report.
- Decision to restore a file or a group of files

5.11 Managed Business Application

5.11.1 Objectives

The customer can delegate continuous 24/7 supervision of the Service Provider's business applications. The customer's development teams can continue to evolve the code and architecture of the business application. In the co-management mode, the Service Provider's SRE will participate in the customer's Scrum team meetings to contribute to the enablers required to manage the business application.

The customer and the SRE can concentrate on defining the Provider's procedures for Observability and business function management and rely on standard managed services to manage the underlying dependencies.

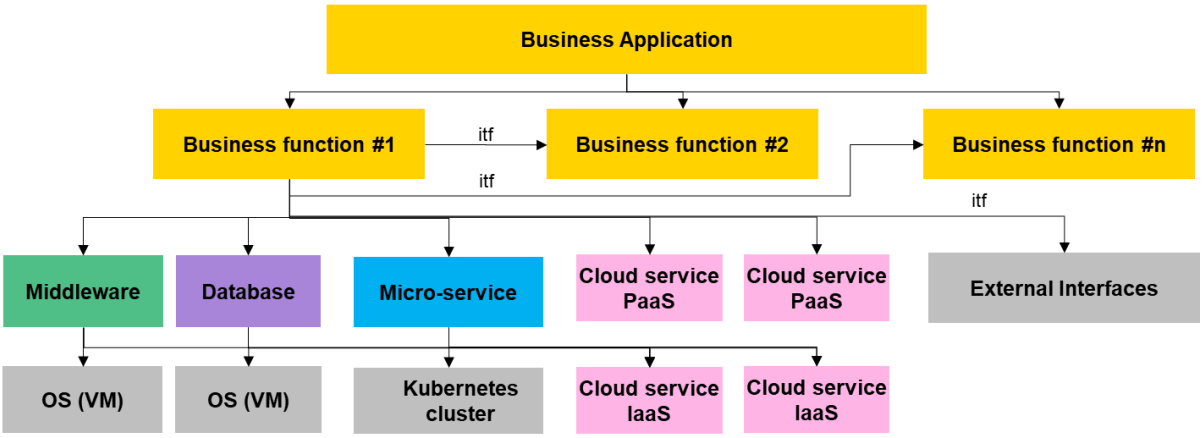
5.11.2 Scope of Work

The Scope of Work for co-management of the Business Application is defined between the Customer and the Service Provider.

The architecture of the Application is explained by the customer to the Service Provider's expert to identify which components need to be supervised and maintained among:

- The business functions
- Their dependencies on interfaces with other Application business functions and with external services.
- Their dependencies on operating systems, middleware, databases, micro-services, Kubernetes services, cloud services, big data services

Business Application management



The main assumption for co-management of the business application is that the software is coded by the customer's own developers, or by a third-party software supplier to the customer. The customer is responsible - by himself or through his supplier - for the maintenance of the software and the business application architecture, for the operation

of the business application and for testing on the cloud environment prior to the transition to the service managed by the Service Provider.

5.11.3 Application management

5.11.3.1 Managing the dependencies

To manage business functions properly, you need to manage dependencies. The managed services catalog includes predefined units of work for known middleware, databases, microservices, Kubernetes clusters, OS and native cloud services. The customer and the Service Provider identify the necessary dependencies to be managed and add them to the SoW in accordance with the service definition in the service catalog (please refer to this document and the description of a managed application).

5.11.3.2 Managing the external interfaces

Dependencies may include interfaces to external systems, or interfaces to other business functions. These also need to be monitored in order to quickly detect and identify the root cause of an incident. Responsibility for restoring an external system is not part of the SoW.

5.11.3.3 Managing the business functions

For business application functions, the SoW will be established on the basis of data and deliverables provided by the customer:

- How is the business function supervised? What is the RACI between the customer and the service provider?
- How critical is the business function to the service?
- What are the known problems? What procedure should be used for restoration?
- How is the business function restored in the event of failure? Is it based on redeployment from Infra as Code? Is it based on restoration from a backup? What is the procedure?
- Are there any specific routines to be run?
- How is the business function created and deployed? What is the dev, preprod, prod chain? What is the RACI between the customer and the service provider on the different environments?
- What are the security policies and firewall rules to be applied?
- Is a disaster recovery plan necessary? How is it implemented?
- Are other services required from the service provider: consulting, health checks, performance, capacity?
- What is the frequency of incidents and changes?
- How often are releases rolled out?
- How mature is the component?

Since the specifics of business applications are the specific knowledge of the customer and its third-party supplier, the customer is responsible for level 3 support for the business application (potentially through its third-party supplier).

The Service Provider's level 1 and level 2 tasks consist of :

- Supervise the business functions agreed in the SoW
- Apply remediation procedures in the event of an incident
- Resolve an incident on a managed dependency
- Notify and escalate to the customer's level 3 if resolution is not possible thanks to the procedure.

5.11.4 Summary

The following table summarizes the service:

Service	Type	Configuration	Monitoring and alerts configured in GCP Cloud Monitoring & Cloud Logging	Backup configured in GCBDR	Recovery procedure	Patch management	Antivirus management	Specificities

Business Function supervision	Managed	Deployment, redeployment of the Business Application is based on Time and Material. Pre-requisite: Image or deployment script provided by the customer. The Business App has been successfully tested on the infrastructure prior to transition to run.	Metrics exporters, alerters to GCP Cloud Monitoring or Prometheus provided by customer as a prerequisite.	Backup and restore is an option. Customer to identify backup procedures necessary to protect business application data. And confirm whether backup of the underlying components is sufficient or not.	Troubleshooting and recovery procedure provided by the Customer. Procedure shall last less than15 min. Otherwise would be charged time based. The Customer is performing Level 3 support.	Customer is responsible for the software and software patching.	Customer is responsible for the software antivirus of the Business Application.	Optional: Scope of work to be defined with Customer Pre-requisite: dependencies shall be managed.
Supervision of an External Interface	Managed	A pre-requisite is that the external interface is exposed and reachable. Out of scope of the Managed Service.	A part of the software or a probe tests the availability of the external interface.	n/a	Customer is notified when the external interface down. The support of the external interface is out of scope of MA service.	n/a	n/a	n/a
Cloud Services dependencies	Managed	Refer to each cloud managed service (as per catalogue) on which the Business App is dependant.						

5.11.5 Pre-requisites

Application architecture and deployment in the cloud must be defined. The architecture is outside the scope of the service.

The application must be deployed and tested by the customer before being transferred to the operations team.

In general, testing is successful in pre-production, with an iso-production pre-production environment. The business application exports metrics to a native Cloud monitoring service.

Data backup and disaster recovery strategies are provided by the customer.
Troubleshooting and service restoration must be provided by the customer.
If a procedure requires logs or a Dashboard, these must have been developed by the customer before being managed by the Service Provider.

An incident remediation procedure must not last longer than 15 minutes. Beyond this time, the effort will be invoiced on the basis of the time spent.

The customer must have subscribed to the managed application service for the underlying components on which the business application depends.

5.11.6 Limitations

Services required by Cloud Service Providers for Observability, logging, supervision and backup are not included in the service and are therefore invoiced as part of the CSP subscription.
Business application software and third-party application maintenance are not included in the service. Customers are responsible for application patching, vulnerability and freedom from viruses.

The scope of the Managed Business Application service and the Service Provider's responsibility for security are limited to the configuration of firewalls and CSP policy groups, in accordance with customer specifications. If other security services are required, they will be part of a mutually agreed optional specification.

End-users of business applications are neither managed nor supported.

Application performance management is the subject of a bespoke specification and quotation.

Application build, pipeline and deployment are outside the SoW of the standard work unit. A specific specification must be drawn up.

5.11.7 Charging model

Service	Unité d'oeuvre
Service Reliability Engineer	Temps et matériel
Fonction métier – supervision – priorité faible	Par source de supervision
Fonction métier – supervision - standard	Par source de supervision
Fonction métier – supervision - critique	Par source de supervision
Interface externe – supervision – priorité faible	Par source de supervision
Interface externe – supervision - standard	Par source de supervision
Interface externe – supervision - critique	Par source de supervision
Sauvegarde de données	SoW
Reprise après sinistre	Scope of Work
Dépendances: OS, middleware, database, Kubernetes, microservices, big data	Unité d'œuvre du catalogue des services managés
Incident signalé par le client	Par ticket d'incident

5.11.8 Changes catalogue – in Tokens, per act

Changes examples	Effort
Adding a new alarm	On quote or estimation in tokens based on time spent. Additional recurring work unit
Deploying the business application	On quote or estimation in tokens based on time spent
Adding a new troubleshooting procedure to the operational knowledge database	On quote or estimation in tokens based on time spent
Troubleshooting beyond 15 mins due to lengthy procedure	Estimation in tokens based on over-time spent

6 Content of the Service

6.1 Guidance and advice services

6.1.1 Service Delivery Manager

The Service Delivery Manager (or SDM) is the Customer's main point of contact for the proper functioning of the Managed Applications Service This service must be subscribed for each Project that includes at least one Premium Support Level Managed Tenant. This service is not available for Projects that include only Standard Support Level Managed Tenants.

The Service Delivery Manager provides the following services:

- Taking part in implementing upgrades / improvement to Customer Service during the run phase,
- Monitoring due functioning of Customer Service during the run phase,
- Advising Customer on possible upgrades to Services subscribed to,
- Servicing in escalation mode, either at the Customer's request, or at that of the Provider teams, or proactively,
- Implementing and steering the quality assurance process,
- In charge of capacity management on the Customer environment (Disk, CPU, RAM). Informing the Customer about upgrades to be taken into account to allow optimal functioning of the environment.

6.1.2 Contract Business Manager

The Contract Business Manager (CBM) is the main contractual contact for the Customer's IT department for Managed Applications Service.

This service must be subscribed for each Project that includes at least one Premium Support Level Managed Tenant. This service is not available for Projects that include only Standard Support Level Managed Tenants.

The Contract Business Manager provides the following services:

- He ensures that the Provider' contractual and commercial commitments to the Customer are respected
- It implements, monitors and updates the Customer's document repository
- He leads governance: Steering Committee and Strategic Committee
- He is the Customer's privileged contact for all matters relating to contractual developments in the life of the solution

6.1.3 Lead Technician

The Lead Technician is the Customer's main technical contact during the run phase of the Service. This service is recommended for complex projects.

The Lead Technician provides the following services:

- Organization of technical committees to improve the performance of the solution;
- Investigation of malfunctions and proposal of solutions;
- Study and implementation of changes.

6.1.4 Architectural design

The architecture design service consists in providing an high level design for the Customer's project at the end of a study based on the Customer's specifications. This service is recommended for complex projects.

6.1.5 DevOps expertise

The DevOps expertise service provides advice and technical assistance for the Customer's implementation of a continuous integration / delivery approach on its Managed Tenant.

A report containing the recommendations will be sent to the Customer at the end of each intervention.

6.1.6 The Service Reliability Engineer (SRE)

The Service Reliability Engineer is a key actor of the managed services on public clouds especially in the DevOps model and co-managed model.

The SRE is a named expert, knowledgeable about operations and software engineering, simultaneously participating to the run of the managed service within Service Provider’s operations team and working closely with the customer’s development team.

The SRE works closely with Customer's development Team to identify and implement the observability indicators, automation of operations and infrastructure as code to meet business needs. He contributes his expertise to the development team for delivering the enablers necessary to a reliable run.

On longer term, the SRE contributes to continuous improvement of the reliability of the business application and its operations.

The SRE participates (remotely) to regular meetings with Application owners for continuous improvement Alignments.

6.1.6.1 Deliverables

The SRE contributes together with the development team to the following deliverables:

- Guidelines for DevOps automation (Infra as Code, Integration, Blue-Green deployment, etc.) according to customer’s team maturity
- Infra as Code necessary to deploy / redeploy the resources in case of service loss or misconfiguration
- Identification and implementation of observability metrics necessary to monitor the business activity
- Define and manage SLO, SLI
- Implementation of automated dashboards allowing analysis of metrics and trends. Pieces of advice for the tooling for implementing them.
- Identification of alarms / thresholds on metrics and alarm collection mechanism
- Identification of necessary backup procedures and security measures for the application and data to meet customer's needs
- Write-up of main procedures necessary to handle the known incidents. Procedures which will be handoff to the level 1 & 2 core operation teams.
    - Simple procedures are typically integrated in the infrastructure as code to accelerate the remedial actions.
- Review/ validation of technical procedures for the changes proposed by the Service Delivery Manager for inclusion in the change catalogue.
- Identification and implementation of log collection to detect anomalies and ease troubleshooting for the business application. Setup of automated correlations and alerts from logs analysis.

- Cold analysis of dashboards, logs for preventive maintenance when requested.
- Configuration of security tooling and SIEM.
- Definition and write-up of recurring check procedures when necessary.
- Criteria for “go” to pre-production. RACI between the customer and the Service Provider for the deployment to pre-preproduction. Automation of deployment if requested.
- Criteria for “go” to production taking into consideration technical and business constraints (deployment time, particular events, etc.). RACI between the customer and the Service Provider for the deployment to production. Automation of deployment if requested.

6.1.6.2 Limitations

- The architecture is not the responsibility of the SRE. It is rather, the responsibility of the customer or of an architect i.e. the Technical Design Authority.
- As such, the design of the Disaster Recovery is not in the mandate of the SRE but of a TDA.
- The build and design of the architecture, including disaster recovery, HLD and LLD is the responsibility of the customer or of an architect i.e. the Technical Design Authority. Following their validation by the Service Provider, the SRE maintains architecture, HLD and LLD during RUN phase and identifies the necessary updates in terms of fault tolerance, auto healing, resilience and reliability to meet new business needs.

6.1.7 The Data Reliability Engineer (DRE)

The Service Data Reliability Engineer (DRE) is a key player in managed services in the managed Big Data environment. The Data Reliability Engineer is responsible for helping to deliver high data availability and quality throughout the data lifecycle, from ingestion to visualization.

The roles and missions of the DRE expert are defined in consultation with you, and can evolve over time according to your needs:

- Define with your business teams the indicators and service level objectives (SLI/SLO) to be met to guarantee data availability and quality.
- Configure metrics and monitoring to check whether or not objectives have been met.
- Alerting configuration to detect and anticipate problems during the data journey: latency, abnormal traffic variations, bottlenecks, errors, throughput or saturation on pipelines, etc.
- Automation and optimization of data chains (pipelines), adaptation of IaC scripts and architecture design to achieve SLOs.
- Detection of failed tasks and automation of their automatic restart.
- Identification with our team of root causes following complex incidents, and implementation of corrective measures.

6.2 Managed OS

With this service, the Customer is provided with complete operating system management, including tasks connected with the VM (Virtual Machine). It is available only to the Customer's Managed Tenants.

By accepting the Purchase Order, the Customer expressly accepts the conditions defined in the document "Technical Annex to the Managed Applications Service Description - Managed OS" accessible here https://cloud.orange-business.com/en/technical-appendix-to-the-managed-applications-service-description-managed-os/ applicable to the Managed OS service, which may be subject to regular updates by the Provider.

6.3 Managed Database

The Provider technically operates the Customer database(s) as well as optimisation and upgrading activities.

For managed DBaaS (DataBase as a Service), database software licenses are provided :

- ✓ as part of the IaaS service subscribed by the Customer.
- ✓ by the Provider, holder of the Licenses. In other cases, the licenses of the database software are subscribed
- ✓ or by the Customer, depending on the Software publishers' terms.

For managed DBaaS, the cost of the DBaaS service is borne by the customer as part of the IaaS service it has subscribed to.

By accepting the Purchase Order, the Customer expressly accepts the conditions defined in the document "Technical Annex to the Managed Applications Service Description - Managed Database" accessible here https://cloud.orange-business.com/en/technical-appendix-managed-database/ applicable to the Managed Database service, which may be subject to regular updates by the Provider.

6.4 Managed Middleware

The « Middlewares » are installed and configured by the Service Provider.

The operating system is always fully managed by the Service Provider, and the customer must subscribe to the Managed OS service.

By accepting the Purchase Order, the Customer expressly accepts the conditions defined in the document "Technical Annex to the Managed Applications Service Description - Managed Middleware" accessible here https://cloud.orange-business.com/en/technical-appendix-managed-middleware/ applicable to the Managed Middleware service, which may be subject to regular updates by the Provider.

6.5 Managed Service for Kubernetes®

The Kubernetes® cluster management service is offered by the Provider on the Public Cloud IaaS Cloud Avenue infrastructure. This service includes:

- The deployment of Kubernetes® clusters according to the configurations provided by the Client.
- 24/7 supervision and maintenance of operational conditions of the clusters.
- Incident management, including notification and cluster remediation interventions.
- The restoration of clusters from a backed up repository.
- Managing changes on clusters.
- Managed tools for collecting, storing and viewing logs and metrics.
- A visualization tool for the Customer to observe the configured metrics and alerts.
- Optional access to DevOps tools (Managed DevOps Toolkit) for deploying applications on clusters.

By accepting the Purchase Order, the Customer expressly accepts the conditions defined in the document "Technical Annex to the Service Managed Applications – Managed Service for Kubernetes®" accessible here Technical-appendix-Managed-Service-for-Kubernetes®.pdf applicable to the Managed Service for Kubernetes®, which may be updated regularly by the Service Provider.

6.6 Managed Application

The "Managed Application" management level provides the customer with the following services:

- Installation of the application server,
- Application operation and administration,
- Application reporting and statistics,
- Application supervision
- Application backup.

The Service Provider can take on the complete management of the customer's applications on request.

Managed Applications for SAP® is a managed business application supported by the Service Provider to manage your SAP® environments:

- We provide you with SAP® landscapes on a 100% virtualized and certified cloud
- We manage your environments so you can focus on your applications and your business
- We take charge of the deployment, migration and maintenance of your SAP® environments.

By accepting the Purchase Order, the Customer expressly accepts the conditions defined in the document "Technical Annex to the Managed Applications Service Description" accessible here https://cloud.orange-business.com/en/technical-appendix-managed-application/ applicable to the Managed Applications service, which may be subject to regular updates by the Provider.

6.7 Managed Native Services Hyperscalers

The Service Provider ensures the technical operation and monitoring of the Customer's AWS, Azure or GCP Native Services, as well as optimization and upgrade activities by setting up a network interconnection between the Service Provider's "service area" and the provider's Cloud platform.

At the start of the project Customer:

- ❖ An audit is required to determine the inventory of resources to be managed, their Transition Class, the scope of work remaining to be completed to be ready for operation, the RACI and the limitations of the service to be managed.
- ❖ Construction of a landing zone is required. Infrastructure deployment is modeled as Infrastructure as Code (IaC) for quality, reproducibility and disaster recovery. Native Services, AWS, Azure or GCP are deployed using this IaC.

The definition of Transition Classes for resources to be transferred and then managed by the Service Provider are specified in the AWS, Azure or GCP technical appendix.

The tariffs indicated in the AWS, Azure or GCP Native Services tariff sheet only concern the service delivered by the Service Provider. Pricing for the IaaS resources of the Hyperscalers concerned are not included in the Service Provider's service, and appear on the Customer's IaaS invoice.

The price of the services referred to in this paragraph and applicable to the Customer is calculated taking into account the following elements:

- The number of Native Services units managed or for which the managed service is subscribed after validation with the Customer through an HLD (High Level Design). The Service Provider's service and price commitment is based on the native services indicated in the HLD, as well as the underlying micro-services, middleware, applications and databases.
- Of the Transition Class applied, following the inventory of resources to be managed, which the Service Provider will carry out during the audit. For some services, the Service Provider's responsibility may be limited to IaC maintenance and change management only, or may include supervision.
- Of SRE (Site Reliability Engineering), which corresponds to the maintenance of the infrastructure as code or to a proactive recommendation for improvement of the IaC by the Service Provider. A proportion of SRE is included as standard in the Managed Service operated by the Service Provider, and a provision is made beyond this, which will be invoiced as a controlled expense by the Customer.
- The support chain used:
  - "Standard" via our support chain located in Cairo for the L0/L1 service desk
  - "Full France", in which the customer can have a Full France channel or a Full France channel with enhanced security, via our support channel located in France. The incidentology (number of monthly L0/L1 tickets) will be defined with the Customer and the Service Provider according to their needs.
- The number of governance days via :
  - The Managed Services Manager for monitoring monthly kpi/reporting,
  - Managed Contracts Manager for contract monitoring and invoicing.
- The number of managed tenant(s) hosting the customer's environment, administered and supervised by the Service Provider's teams,
- The number of token(s) per unit or per pack subscribed by the Customer for the change management required for the start-up of the Customer project or during the life of the solution.

By accepting the Purchase Order, the Customer expressly accepts the conditions defined in the document "Technical Annex to the Managed Applications Service Description – Managed Native Services Hyperscalers accessible here :

- Azure : https://cloud.orange-business.com/en/technical-appendix-managed-applications-on-azure-2/,
- AWS : https://cloud.orange-business.com/en/technical-appendix-managed-applications-on-aws-2/,
- GCP : https://cloud.orange-business.com/en/technical-appendix-google-native-managed-service/,

applicable to Managed Native Services Hyperscalers, which may be subject to regular updates by the Provider.

6.8 Managed Big Data

Managed Big Data is a service that enables customers to generate value from their business data (such as predictive maintenance, fraud detection or customer knowledge).

This service is made up of different solutions, all managed by the Service Provider (Infrastructure and Big Data Components). These solutions operate according to the same philosophy: collect data in batch or streaming mode, store data, process data and visualize data.

The service includes some or all of the following elements:

- A secure administration portal supplied with the Big Data platform,
- A dedicated tenant to ingest, store, process and visualize customer data,
- A 24/7 monitoring and alert solution,
- Installation, configuration and maintenance of Big Data solution components by the Service Provider,
- Implementation by the Service Provider of the following services, subject to quotation:
  - Data and architecture assessment audit
  - Migration of an existing Big Data solution to the Service Provider's environment,
  - Development of business use cases with the Service Provider's internal partners,

The following Big Data software solutions are offered and managed by the Service Provider. Each solution can be selected according to the customer's needs:

- Big Data with Cloudera CDP / CDF,
- Native Big Data services with Flexible Engine,
- Native Big Data services with Google GCP,
- Native Big Data services with Azure,
- Native Big Data services with AWS,
- Log As A Service solution.

For self-service Big Data Services offered by the Public Cloud Provider (Flexible Engine, GCP, Azure and AWS), the Provider manages the infrastructure and Big Data components for the Customer.

By accepting the Purchase Order, the Customer expressly accepts the conditions defined in the document "Technical Annex to the Managed Applications Service Description - Managed Big Data" accessible here https://cloud.orange-business.com/en/technical-appendix-managed-big-data/ applicable to the Managed Big Data service, which may be subject to regular updates by the Provider.

6.9 Managed Computer Vision

Computer Vision Managed Service is a service provided by the Service Provider that uses Artificial Intelligence techniques to enable the Customer to extract data from its video equipment through alerts and a dedicated dashboard.

The Service provided to the Customer comprises:
- A Computer Vision-type software solution
- A Cloud hosting solution operated and administered by the Service Provider.
- A global operating service for the software and hardware solution, managed by the Service Provider.
- Support services for customers implementing the service.

The service comprises the following elements:
- Development or configuration of the Computer Vision application:
  - Implementation of dataset and tools (training, labeling, augmentation, etc.),
  - Artificial Intelligence design (internal framework / inference, engine learning, image processing, video, audio...),
  - Statistics generation and extraction, dashboard construction,
  - Application installation and configuration based on documentation provided by partner.
- Operation, administration, 24 x 7 of the solution in production and non-production environments.
- Supervision and maintenance of solution deployment
- Third-party application maintenance with support for the data lifecycle
- Incident, change, event and security management.

The Service Provider can take over the complete management of the customer's applications, on request.

Depending on the customer's needs and uses, the Service Provider integrates the application expertise of its network of ISVs (Independent Software Vendors) or of the Service Provider's experts.

By accepting the Purchase Order, the Customer expressly accepts the conditions defined in the document "Technical Annex to the Managed Applications Service Description - Managed Computer Vision" accessible here https://cloud.orange-business.com/en/technical-appendix-managed-computer-vision/ applicable to the Managed Computer Vision service, which may be subject to regular updates by the Provider.

6.10 Managed Remote Desktop Service

The Managed RDS (Remote Desktop Service) is a Service from the Provider that enables the Customer's RDS, hosted on a Public Cloud IaaS infrastructure from the list below.

✓ From the Provider :
- Cloud Avenue
- Flexible Engine

✓ Partners :
- AWS,
- Microsoft Azure,
- Google Cloud

Managed RDS relies on complementary services:

- Managed AD,
- Server SSL certificates, self-signed or issued by a recognized certification authority.

Prerequisites for this offer:

- Subscribe to an IaaS infrastructure offer for hosting the RDS service, as recommended by the Service Provider.
- Subscribe to the Managed OS offer for the VMs where the components are hosted.
- Subscribe to the Managed AD offer for the AD required to deliver the RDS service.

By accepting the Purchase Order, the Customer expressly accepts the conditions defined in the document "Technical Annex to the Managed Applications Service Description - Managed RDS" accessible here https://cloud.orange-business.com/en/technical-appendix-remote-desktop-service/ applicable to the Managed RDS service, which may be subject to regular updates by the Provider.

6.11 Managed Active Directory

As part of this Service, we manage your AD DS hosted on a Public Cloud IaaS infrastructure from the list below.

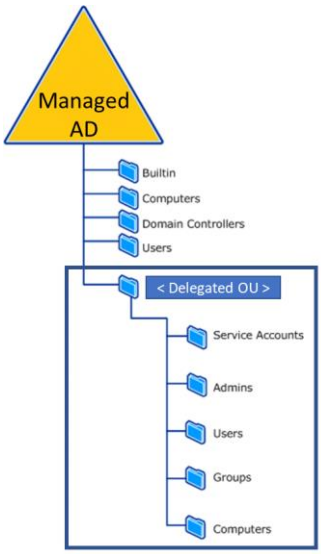
The Provider:

- Cloud Avenue

Flexible Engine Service AS DS Managed enables the Customer to administer user accounts and computers via delegation on one or more 'WHERE'.

The Service Provider is responsible for the following activities:

- Selecting the components required for your Managed AD
- Setting up the service
- Maintenance
- Configuration and monitoring of AD services
- GPO management (excluding delegated OU) and AD service management
- Standard AD backup



The prerequisites are as follows:

- Subscription to the Managed OS offer for the VMs where your AD is hosted,
- Infrastructure composed of a minimum of 2 VMs according to Microsoft recommendations,
- Single-forest, single-domain AD,
- Compliance with best practices and recommendations of the Service Provider.

By accepting the Purchase Order, the Customer expressly accepts the conditions defined in the document "Technical Annex to the Managed Applications Service Description - Managed AD" accessible here applicable to the Managed AD service, which may be subject to regular updates by the Provider.

6.12 Managed Security

The Managed Security service is a service provided by the Service Provider that enables the management of the following security components:

- Management of third-party firewall(s) hosted on the Service Provider's infrastructure or Hyperscalers (Azure, AWS, GCP)
- Management of native firewall(s) hosted on the Service Provider's infrastructure,
- Management of third-party Load Balancer(s) hosted on the Service Provider's infrastructure or Hyperscalers (Azure, AWS, GCP).

Pricing for the security components of the Managed Security Service, as well as the technical description of the security components, form an integral part of the Managed Applications contractual package.

By accepting the Purchase Order, the Customer expressly accepts the conditions defined in the document "Technical Annex to the Managed Applications Service Description - Managed Security" accessible here https://cloud.orange-business.com/en/technical-appendix-managed-firewall-and-load-balancer/ applicable to the Managed Security service, which may be subject to regular updates by the Provider.

6.13 Managed Citrix Workspace

The Citrix Workspace Managed Service is a service provided by the Service Provider that enables the management of the Customer's Citrix Workspace hosted on the Service Provider's Public Cloud infrastructure.

The Citrix Workspace Managed Service includes:

- Production of the Customer's infrastructure.
- Deployment of Users' Virtual Desktops as an option, if subscribed to by the Customer.
- Maintaining the infrastructure base and Virtual Desktops in operational condition.
- Support, covering the processing of reports and change requests.
- Optional customer relations management by a Customer Service Manager (CSM) or Service Delivery Manager (SDM).

By accepting the Purchase Order, the Customer expressly accepts the conditions defined in the document "Technical Annex to the Managed Applications Service Description - Citrix Managed Workspace" accessible here applicable to the Citrix Managed Workspace service, which may be subject to regular updates by the Provider.

6.14 Managed Exchange

The Managed Exchange Service is a Service provided by the Service Provider which consists of managing the Exchange messaging service of the Customer's Tenant. The Service is subscribed to for all active users on the Customer's Tenant. The Customer may increase the number of users during the course of the contract. Additional users are invoiced at the same intervals as the initial order, with prorated billing.

The Service Provider accompanies the Customer throughout the life of the Contract: from Service implementation to support.

The Service Provider offers 2 models:

- Exchange on Cloud Avenue
- Exchange Online - Office 365

By accepting the Purchase Order, the Customer expressly accepts the conditions defined in the document "Technical Annex to the Managed Applications Service Description - Managed Exchange" accessible here applicable to the Managed Exchange service, which may be subject to regular updates by the Provider.

7 Access to the Service

7.1 Prerequisite

The "Managed Applications" service can be broken down as follows:

- It can be based on an IaaS service, to which the Customer must also subscribe. In this case, the Tenant subscribed to by the Customer is a Managed Tenant, administered by the Service Provider.
- It may be based on an IaaS service, to which the Customer must also subscribe. In this case, the Tenant subscribed to by the Customer is a Co-Managed Tenant, administered by the Service Provider in accordance with a RACI defined between the Customer and the Service Provider.
- The Customer can use the Service Provider's **M**ulti**C**loud **R**eady (**MCR**) offer, which enables the resale of Cloud Services from our Hyperscaler partners AWS, GCP and Azure. ***Our support model for Managed Applications cloud services complements our infrastructure support offer.***

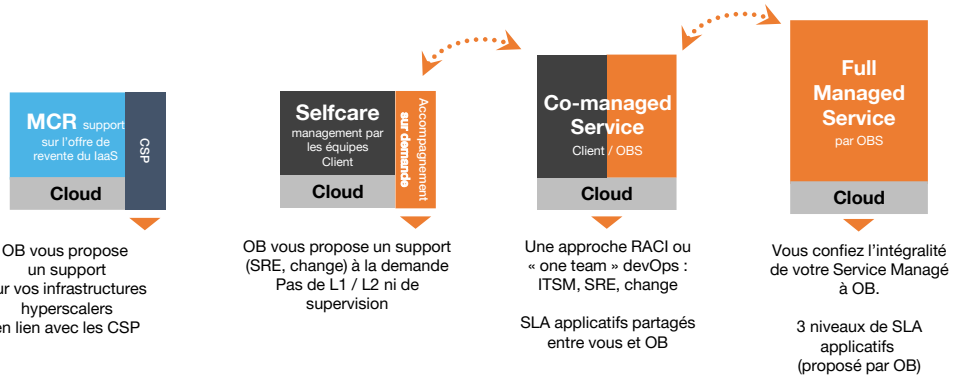


Figure 4 – Managed Applications management model with MCR

7.1.1 Managed Tenant

In the case of a Managed Tenant administered by the Service Provider, the Customer must subscribe to the IaaS support level of his choice and will be invoiced for IaaS support under the corresponding contract. For Flexible Engine and Cloud Avenue IaaS, the support level to be subscribed to is "Managed Tenant".

The IaaS service corresponding to the Managed Tenant shall be billed as soon as it is put into operation, without waiting for the Managed Applications managed service acceptance.

For Managed Tenant, some IaaS functionalities will not be available to the Customer:

- ⇨ Change management, incident management, and releases (security rules, VM upgrades, etc.) are run under the “Managed Applications” service.
- ⇨ The IaaS console and reporting tools in the Cloud Store are available in read-only mode.
- ⇨ The Customer delegates to the Provider responsibility for selected management tasks on its Managed Tenant, in accordance with the provisions of the document herein.

7.1.2 Management levels Managed tenant

The customer may subscribe to different management levels for the same project:

- For Database managed and Middleware managed management levels, the customer must subscribe to the OS managed management level.
- For the Managed Application management level, the Customer must subscribe to the Managed OS management level, and to the Managed Database and Managed Middleware management levels, or to the Kubernetes management levels, when the operation of its application requires the implementation of the corresponding components.

Each virtual server (VM) of the Managed Tenant can have one of 4 possible management levels (Managed OS, Managed DB, Managed Middleware, Managed Application). The management level applies to the entire server, and software with different management levels cannot coexist on the same server.

Each Managed Tenant Kubernetes cluster can have one of 2 possible management levels (Managed Kubernetes, Managed Application). The management level applies to the entire cluster, and software with different management levels cannot coexist on the same cluster.

At the time of ordering, the customer chooses one of the three support levels available (Initial, Standard, Premium), which applies to the different types of environments for the Service subscribed to by the customer.

Several types of environments are available:

- Production environment
- Pre-Production environment
- Integration environment
- Development environment

If the Customer wishes to benefit from different levels of support, this must be specified when subscribing by environment. Deployment may take place on one or more Managed Tenants, depending on the SoW shared between the Customer and the Service Provider.

7.2 Portal – Cloud Store Customer Space

Figure 5 - The Cloud Store Portal

The Cloud Store Customer Area allows to manage all contracts to which they have subscribed, in particular via the following sections:

- Contract: this section offers viewing general information on contracts and orders made.
- Dashboard: enables Customers to access the IaaS console through SSO (Single Sign On), in read only mode.
- Services: enables Customers to order online services or access the change request tools.
- Invoices: enables Customers to view all invoices on-line and access the information needed to contact the invoicing department
- Documents: documentation management space allowing the Customer to access documents organized in five directories: User guides, performance reports, technical dashboards, meeting minutes, miscellaneous.
- Support: provides access to the incident reporting tool and information needed to contact the customer support centre.
- Users: enables Customers to manage user rights on each offer and on the customer space.

8 Service quality commitments

The purpose of this service description is to define the conditions under which the Service Provider provides the "Managed Applications" service (hereinafter the "Service") to the Customer.

8.1 Service quality commitments

- The Service Provider undertakes to provide quality of service under the conditions defined herein and/or in the Technical and Financial Proposal for the Service concerned.
- The service quality commitments may give rise to the payment of a penalty, the amount of which is specified herein and/or in the Technical and Financial Proposal. This penalty shall constitute a lump-sum compensation covering the loss suffered, excluding any claim for damages for the same reason.

8.2 Service Credits

- In the event of non-compliance identified by the Customer and confirmed by the Service Provider with the commitments set forth herein and/or in the Technical and Financial Proposal, and upon the Customer's express request, the Service Provider undertakes to issue Service Credits for the month in question in accordance with the provisions of said document.
- To obtain these Service Credits, the Customer must send the Service Provider the Service Credit request form duly completed to the contact mentioned on the invoice, indicating in the subject line "SLA Claim" followed by the name of the Service concerned, within a maximum period of 30 days following the month concerned by the failure to comply with the service quality commitment. Otherwise, the Customer will not be entitled to any Service Credit.
- The request form is made available to the Customer by the Service Provider on a User Interface, or otherwise is available from its usual contacts.
- The request must detail the nature of the problem, the start and end dates and times of each incident observed, as well as the identifiers of the impacted resources. Only incidents that have been ticketed can be considered. It must also include all system traces documenting the incident, for each period concerned. Traces containing sensitive or confidential data must be anonymized beforehand by masking the information that cannot be disclosed.
- Within 30 days of the Customer's request, the Service Provider shall confirm in writing to the Customer the amount of Service Credits, if any, that will be granted to the Customer in respect of such request. In the event of disagreement as to the level of service achieved, the Provider's records and information shall prevail.
- The Service Credits awarded to the Customer shall be discounted on one or more of its subsequent invoices for the Service for which the service level commitments have not been met, to the exclusion of any other method of reimbursement.

8.3 Services range

Service ranges means the different time slots during which monitoring, operation and administration services are provided:

Services ranges		
Monitoring range	24h/24 – 7j/7	Monitoring includes the implementation of standard technical monitoring tools to detect any abnormal malfunction of a service, from the hardware layer to the behaviour of middleware. Application monitoring is not part of the standard service and its implementation must be handled by pre-sales team.
Operating range	Production environment : P1 and P2 : 24h/24 – 7j/7 P3 : 09h-18h working days Non-production environment : P1, P2, P3 : 09h-18h working days	Operations takes care of the management of technical incidents reported by Customers and the monitoring system. Operations also supports changes directly related to incidents.
Administration range	09h-18h working days	This range corresponds to the management range for change requests: placing work orders, application integrations (MEP=Going into production) not related to incidents. Any change to be made outside the administration range is subject to a commercial proposal.

Working days: Monday to Friday in Metropolitan France

8.4 Application conditions

8.4.1. The service quality commitments described in the "Commitments and Penalties" article herein apply in accordance with the General Terms and Conditions.
8.4.2. For the full application of the Service Provider's service quality commitments and in accordance with the General Terms and Conditions, the Customer undertakes to cooperate with the Service Provider:

a) providing the Service Provider with any information likely to enable or facilitate the delivery of the Service(s) and/or Product(s).
b) making available to the Service Provider, within a reasonable timeframe, the resources required for its operations.
c) by conforming its environment to the prerequisites necessary for the Service Provider's interventions.

8.4.2. Service quality commitments apply only to Managed Service Units within the scope of the Service Provider's work and for which the prerequisites for managed services are provided and validated by the Service Provider. They include connectivity, monitoring, supervision, patching, backup and restoration procedures according to the agreed Build responsibility model (see Managed Applications - Service Description Technique).
8.4.3. Service quality commitments apply to production Service Units. These service quality commitments also apply to non-production Service Units in accordance with the operating ranges and administration ranges defined above. Penalties do not apply to non-production Service Units.
8.4.4. For co-managed Service Units,

d) The Availability Rate Guarantee and the Recovery Time Guarantee do not apply during periods when the customer is involved in the cause of the incident.
e) The Recovery Time Guarantee does not apply to Service Units for which the Service Provider is not responsible for Level 3 support.
f) The investigation and repair time spent by the Service Provider for an incident generated by a misconfiguration or action by the Customer will be invoiced on a time basis in the form of Change Tokens.
g) In the event of shared responsibility, the Customer and the Service Provider must work together to achieve the Guaranteed Recovery Time. They will each share 50% of the time spent.

8.4.5 For Service Units built according to the "Backend Build - Class 2" model (see Managed Applications - Technical Service Description), as the Customer is in charge of building the infrastructure, configuring the native Hyperscaler tools and providing service recovery procedures, the scope of the Service Provider's responsibilities is limited to the detection, investigation and recovery possibilities provided by this tooling configuration and these procedures.

8.4.6. Service quality commitments do not apply during periods when the Customer's IaaS is unavailable. In respect of such excluded periods, the Customer may, where applicable, assert its rights to service credits with its IaaS provider, in accordance with its contractual terms and conditions.
8.4.7. For the Managed Computer Vision service, the service quality commitments do not apply if the cause of the incident is a bug in the third-party artificial intelligence software used for training and inference.
8.4.8. Restrictions specific to each Functionality are specified, where applicable, in the "Commitments and Penalties" article.
8.4.9. Under no circumstances may Service Credits granted to the Customer exceed 15% of the monthly recurring amount billed to the Customer for the Service concerned for the month in question.
8.4.10. The same Incident may not give rise to Service Credits under both the GTD and the GTR. In the event that both are applicable, the higher of the two Service Credits will be granted to the Customer.
8.4.11. For the Managed Service for Kubernetes®, quality of service commitments apply only to clusters with at least three control nodes, with a version of Kubernetes® validated and supported by the Provider. Availability measurement will be performed at 5 consecutive minute intervals. This SLA does not include scheduled downtime, loss of connectivity, or failures of Kubernetes® nodes or pods running on these nodes.

8.5 Commitments and penalties

8.5.1 Portal services

For portal services: The Service Provider is committed to ensuring an Availability Rate of 99.5% for each portal. The list of portal concerned is as follows:

- portal Espace Client Cloud Store (ECCS).

8.5.2 Guaranteed Availability Rate (GAR)

8.5.2.1 Commitment

The Service Provider undertakes to comply with an Availability Rate in the chart below for each Managed Function, in accordance with the level of support to which the Customer has subscribed:

Guaranteed Availability Rate			
Service range = Monitoring range			
Level of support	Initial	Standard	Premium
by Managed Function	98,5%	99,5%	
Managed Service for Kubernetes® (Kubernetes® API availability)	98,5%	99,5%	

8.5.2.2 Gap calculation

The "Availability Gap" is calculated as follows for the month in question and for each Managed Function impacted by a Downtime:

$$\text{Availability Gap} = \textit{Guaranteed Availability Rate} - \textit{Measured Availability Rate}$$

8.5.2.3 Penalties

If during a given month, the Availability Rate of a Managed Function or portal services is strictly less than the Guaranteed Availability Rate, the Service Provider undertakes as per General Terms and Conditions to issue Service Credit equal to the percentage listed in the table below, of the recurring monthly figure minus tax invoiced to the Customer for the Managed Function assigned for the relevant month, in accordance with the Availability Gap recorded:

Availability Gap	Service Credit Percentage
More than 0 to 1 percentage point	2%
More than 1 to 2 percentage points	5%
More than 2 percentage points	10%

8.5.3 Guaranteed Fault Repair Time (GFRT)

8.5.3.1 Commitment

The Service Provider undertakes to comply 95% of the following Fault Repair Times each month, depending on the level of support to which the Customer has subscribed, time being counted solely during the periods covered:

Guaranteed Fault Repair Time				
Service range = Operating range				
Level of support		Initial	Standard	Premium
Incident Priority	Priority1	1 day HO*	8h	4h
	Priority 2	No SLA	24h	8h
	Priority 3	No SLA	48h	32h
	Priority 4		No commitment	

Working days: 9am to 6pm CET

8.5.3.2 Gap calculation

The “Fault Repair Gap” is:

- If the total number of Incidents resolved in the month is greater than or equal to 5:

$$\text{Fault Repair Gap} = \frac{Number\ of\ Incidents\ resolved\ after\ the\ deadline}{Total\ number\ of\ Incidents\ resolved\ within\ the\ month}$$

- If the total number of Incidents resolved in the month is less than 5:

$$\text{Fault Repair Gap} = \frac{Number\ of\ Incidents\ resolved\ after\ the\ deadline}{5}$$

8.5.3.3 Penalties

If for a given month, the Guaranteed Fault Repair Time is exceeded, the Service Provider undertakes as per General Terms and Conditions to issue Service Credit equal to the percentage listed in the table below, of the recurring monthly figure minus tax invoiced to the Customer for all the Service's production Services Units for the relevant month, in accordance with the Fault Repair Gap recorded:

Fault Repair Gap	Service Credit Percentage
more than 5% to 25%	2%
more than 25% to 50%	5%
more than 50%	10%

8.5.4 Guaranteed Change Time (GCT)

8.5.4.1 Commitment

The Service Provider undertakes to comply with the following Change Times for each subscribed Service Unit in production, depending on the level of support to which the Customer has subscribed, time being counted solely during the periods covered:

Guaranteed Change Time			
Service range = Administration range			
Level of support	Initial	Standard	Premium
Execution of a simple change	No SLA	24h	8h
Execution of a simple accelerated change	No SLA	12h	4h
Execution of a complex change	No SLA	72h	48h
Execution of a complex accelerated change	No SLA	36h	24h
Response to a request for non-standard change	No SLA	5 WD	3 WD

NB: Exchange requests for Native Services > 1 Token are complex exchange requests.

8.5.4.2 Penalties

If for a given request for change the Guaranteed Change Time is exceeded, the Service Provider undertakes as per General Terms and Conditions to issue a Service Credit equal to 50% of the change price corresponding to the Token's "pay-per-use" rate.

9 Price conditions

9.1 Minimum duration

The minimum duration of the Service is one year. The duration of the Customer's commitment is specified in the Order.

A Managed Tenant may host several Customer Projects, which may have different end-of-commitment dates.

9.2 Price

The pricing of the service is different for:

- Service units ordered when the contract is signed;
- Additional service units ordered at a later date;
- Backup and restore services ;
- Tokens on demand;
- Support services.

The Service is subject to a Service access fee and a monthly minimum charge, the amounts of which are indicated in the Tariff Sheet, plus the price of the Service Units and services subscribed to (restoration, backup, support and Tokens).

Backup and restore services, support services and on-demand tokens are invoiced at the price shown on the Tariff Sheet in force at the time of subscription.

Rates are defined by region.

Where rates depend on the customer's commitment period, the commitment period taken into account for the subscription of additional services is equal, unless otherwise stipulated, to the remaining commitment period rounded up to the next higher period specified in the Tariff Sheet.

The Managed Applications Service rates do not include the price of the Managed Tenant, which the Customer must also subscribe to with the IaaS provider according to the rates in force.

9.3 Price revision

9.3.1 SYNTEC price revision

The unit prices of the Services (excluding backup and restoration services, support services and tokens on demand) may be revised each year on the anniversary date of the Contract by applying the following formula:

$P1 = P0 \frac{S1}{S0}$

Where P1 = revised price

P0 = original price

S0 = latest SYNTEC index published on the date of conclusion of the Contract or on the date of the previous revision

S1 = latest SYNTEC index published on the revision date.

The base prices and indices are the prices and indices at the date of the first monthly invoice.

Services invoiced at the beginning of the revision period are invoiced on the basis of the latest known indices. Additional invoices will be issued as soon as the relevant indices are published, and subsequent invoices will be adjusted accordingly.

In the event of the SYNTEC index disappearing, the ad hoc committee must select a new index within one month, and if this is impossible for any reason whatsoever, the President of the Paris Commercial Court is expressly empowered to define an index to be included in the revision formula. This index must be chosen so as to be as close as possible to the index that has disappeared.

9.3.2 Specific price revision

In the event that the equipment used by the Service Provider to administer the Customer's service units requires a physical hosting area, then the prices of these service units may be revised each year on the anniversary date of the Contract - in addition to the revision linked to the SYNTEC index - by applying the following formula:

P = P-1 * [⅔ (S/S-1) + ⅓ (T/T-1)]

Where:

- P is the revised amount, P-1 is the amount in effect prior to the revision date,

- S is the latest construction cost index published by INSEE at the revision date (ICC base 100 at 4th quarter 1953, quarterly), and S-1 is the construction cost index published twelve months prior to the revision date,

- T is the monthly index of the cost of medium-voltage electricity published by INSEE (electricity sold to companies with a contract for capacity > 36 kVA) at the revision date, and T-1 is the monthly index of the cost of medium-voltage electricity published twelve months prior to the revision date.

In all cases, the Service Provider will apply at least the tariff conditions linked to changes in energy costs published by INSEE.

In the event of the disappearance or non-publication of one of these indices, it will be replaced by an index of comparable effect.

9.3.3 Revision of license and managed equipment prices

The Service Provider reserves the right to increase its prices in the event that the third party supplier of the licenses or managed equipment necessary for the proper provision of the Service increases its published public price list and/or notifies the Service Provider of a price increase for such equipment and licenses. This increase will be limited to the increases notified by the third-party supplier for equipment and licenses.

The Service Provider will inform the Customer of any price increase imposed by the third party supplier and the impact on prices.

9.4 Minimum guaranteed income (MRG)

The initial contract stipulates the Global Revenue expected by the Service Provider for the RUN phase.

In return for the resources and specific organization put in place by the Service Provider for the execution of the Contract, the Customer undertakes, during the RUN phase, to maintain a Guaranteed Minimum Revenue (GMR) corresponding to 80% of the Global Revenue amount stipulated in the Contract.

At the end of each RUN year, the Parties will ensure that the annual MRG has been reached. The Annual MRG is calculated by dividing the Global MRG amount by the number of RUN years provided for in the Contract.

If the amount actually invoiced by the Service Provider for a RUN year is less than the Annual MRG amount, the difference between the Annual MRG amount and the Amount invoiced during the year (hereinafter the "Differential") will be owed by the Customer to the Service Provider and invoiced within thirty (30) days of written notification by the Service Provider of the existence of this Differential. If an annual MRG is exceeded, this overrun will contribute to the annual MRG for the following year.

In the event of an upward variation in the scope of services (new service(s) and/or modification of planned services) having a price impact of more than 15% in relation to the Overall Revenue provided for in the Contract, the Overall MRG will be revised upwards in proportion to the percentage price variation recorded by the Parties in respect of this change in scope.

9.5 Support prices

Support services are defined in the customer contract as follows:

- a support level: Initial, Standard or Premium
- a type of support: Off-Shore or full France
- and a number of tickets, determined specifically for each customer.

The number of tickets actually used by the Customer over the past period will be regularly reviewed. Any excess over the number of tickets defined in the contract will be invoiced at the unit price per ticket indicated in the Managed Applications price sheet.

9.6 Incident ticket prices

Service Desk billing is linked to the customer's environment. The customer can subscribe to the following 4 types of environment as part of the Managed Applications offer, according to his needs:

- Production environment
- Pre-production environment
- Integration environment
- Development environment

In addition, there are four levels of support, corresponding to four rates for trouble tickets:

- Ticket SLA Premium
- Standard SLA Ticket
- SLA Initial ticket
- No SLA ticket

If a customer has subscribed to several environments, with different levels of support for different environments, the trouble ticket price will be that of the highest ticket.

9.7 Prices for additional service units

The price of the service units ordered at contract signature is fixed during the customer's commitment period.

Any order for units of service other than those ordered on signature of the contract will be invoiced at the price of the units of service in the price list in force at the time of the order.

9.8 Build and Run billing

9.8.1 Billing Build

Customer billing by the Service Provider during the Build phase can be carried out in 2 ways:

1. For small projects, the Service Provider invoices 30% of the Build amount on receipt of the purchase order duly signed by the Customer, and invoices the remaining 70% on completion of the Build phase.
2. For customer projects where the Build is spread over several months, the customer's sales representative will define batches/payment deadlines with his project manager, in agreement with the customer. The Service Provider invoices the Build amount in batches, respecting the payment deadlines.

9.8.2 Run billing

Invoicing for the run starts on delivery:

- Either the entire Build,
- Or a defined batch, in the case of batch billing.

9.9 Outgoing reversibility

Reversibility conditions are defined as follows:

- The duration of the reversibility period is limited to 3 months.
- During the reversibility phase, the "Restoration Time Guarantee" does not apply.
- In particular, the Service Provider undertakes to supply technical information on the service architecture (PQSC, SRF), provided that the information requested does not constitute know-how protected by the Service Provider.
- The Service Provider reserves the right to withdraw any product or license contracted by it with a third-party supplier, in order to remain within the legal rights of use of each publisher's license.
- In the event that the Service Provider is requested to provide additional assistance and guidance to that defined above, the Customer will receive :
- A remunerated assistance proposal specifying the conditions of its assistance, the personnel dedicated to reversibility operations, and any hardware and physical installations required.
- The financial conditions applicable to the implementation of this additional assistance.

For its part, the Customer undertakes to provide all the technical, human and, where applicable, financial assistance required to complete the migration of the service. The conditions of the Contract will continue to apply until the end of the Reversibility Period.

In any event, the Customer will be solely responsible for its relationship with the assignee and for the latter's actions.

9.10 Specific conditions of use of the Service

In order to enable use of the Services in accordance with the description and SLA set out in the Contract, unless otherwise stipulated in the Service Description, the Customer undertakes to maintain its equipment interfaced, without passing through a routing and filtering system, with the Equipment used by the Service Provider to supply the Services or the Customer Equipment managed by the Service Provider as part of the Services, in the conditions of updating and security requested by the manufacturers of such Equipment or the publishers of the software making up such Equipment.

Consequently, the Service Provider shall in no way be held liable in the event of the compromise of one or more of the aforementioned Equipment(s), made possible by the obsolescence of the Equipment(s) or the Customer's failure to update the security level of the Equipment(s). The Service Provider reserves the right to invoice the Customer for all or part of any intervention by the Service Provider which may prove necessary to restore the said compromised Equipment to working order.

Unless otherwise agreed between the Parties, in the event that the Customer manages its own Equipment and/or otherwise stipulated in the Service Descriptions, the Customer is responsible for the security policy of its networks, virtual machines, Software and Data, and for any procedures concerning the response to security breaches and attacks.

The Service Provider reserves the right to apply any measures it deems necessary to ensure the security of the service: hardening, versioning/patching, configuration, scripts and agents, security functions, anti-virus, version upgrades in the event of obsolescence.

Consequently, the Service Provider cannot be held liable in any way in the event of compromise of one or more pieces of Equipment, made possible by the obsolescence of the Equipment(s) or the failure to update the security level of the Equipment(s), or by deactivation by the Customer.

10 Definitions

In addition to the definitions in the General Terms and Conditions and the Specific Terms and Conditions for Integration, Maintenance and Related Services, the following specific definitions apply to this Service Description.

Accelerated Change refers to a Simple or Complex Standard Service change requiring an expedited release of the Customer's request. The price of the expedited change is double the change requested by the Customer. Customer may request expedited processing of a Simple Standard or Complex Change on an exceptional basis up to a maximum of 6 per year.

Availability Rate, unless otherwise stated for a specific Feature, refers to the rate defined by the following formula:

$$\text{Availability Rate} = \frac{(t_{month} - t_{downtime} + t_{exclusion})}{t_{month}}$$

where:

- t_{month} is the time during which the concerned Feature is subscribed for the month involved
- $t_{downtime}$ is the Downtime of the concerned Feature for the month involved
- $t_{exclusion}$ is the Downtime of the concerned Feature for the month involved during which quality-of-service commitments of the Service Provider are not applicable as per contractual provisions, such as scheduled interventions.

Availability Rates are measured on a calendar month basis. The Availability Rate of a Managed Function is the average of the Availability Rates of the Service Units that constitute it.

Availability Zone means a data center that is isolated or sufficiently remote from any other data centers in the Region to enable local resilience. The Availability Zones for each Region are listed in the Service Description.

Axway Vision Gateway: refers to a file transfer gateway that secures the exchange of files between different networks.

BaaS (Backup as a Service) stands for online backup service, also known as cloud backup. It's an off-site backup method in which a company's data (files, folders, applications, ...) are regularly backed up by a service provider to secure remote Cloud storage via a network connection.

Change Time refers to the time elapsed between the Request for Change and the end of its implementation as notified by the Service Provider, minus the periods during which the Service Provider' engagements do not apply.

CCE Cloud Container Engine refers to a container service in the Provider's Flexible Engine cloud.

CI/CD (Continuous Integration / Continuous Deployment) refers to the tools solution provider's Cloud Container Build and Deployment service.

CFT (Cross File Transfer) refers to the file transfer protocol.

Class 2 refers to the scope of the Service Provider's activities, in which the Service Provider supports the managed service of the resources according to the procedure guide provided by the customer (Change), and in which the Service Provider is responsible for data recovery in the event of failure. This scope includes the integration of alarms from the relevant CSP into the Service Provider's back-end systems, the input of customer-supplied procedure guides into the Service Provider's operations knowledge repository, and the preparation of operations.

Class 4 refers to the scope of the Service Provider in which the Service Provider configures and maintains CSP management tools to manage the service, as well as integration into the Service Provider's backend systems.

Class 5 refers to the scope of the Service Provider in which the Service Provider configures the Infrastructure as Code (IaC) required for the resources and for the CSP management tools concerned, as well as integration into the Service Provider's backend system.

Cluster means a group of nodes providing distributed computing/processing capacity.

Computer Vision means the service that exploits Artificial Intelligence techniques to enable the Customer to extract data from its video equipment through alerts and a dedicated dashboard.

Complex Standard Change refers to a Standard Change of more than one Token at the initiative of the Customer or the Service Provider, which requires a significant effort, or which has an impact on several services, implemented by a procedure validated by the Service Provider and accepted by the Customer. Any change considered as Standard

Complex is defined in the list of standard changes in the change catalog accessible through the Cloud Store Customer Area.

Customer Administration Environment refers to the environment in which the Customer's Service is hosted (build and deployment). The actions of creating, destroying, modifying and listing resources and associated functionalities are limited to the Service Provider.

Customer Environment refers to the environment in which the Customer's Containers are deployed. The actions of creating, destroying, modifying and listing resources and associated functionalities are allocated to the Service Provider and the Customer. The Customer can use this tenant to run applications and use IaaS functionalities outside the tools Devops solution.

Domain Controller means the set of servers running the Active Directory Domain Services role.

Downtime refers to the period(s) during which an Incident causes a significant malfunction of the Service or Feature concerned, affecting all Users. Calculating the duration of the unavailability obeys specific criteria for each Service or Feature. A Downtime is logged by a ticket with Priority P1.

DRE (Data Reliability Engineer) refers to the Service Provider's expertise in the managed Big Data environment.

Environment refers to a virtual private space of resources on the IaaS to which only Users authenticated by login and password can have access. The actions of creating, destroying, modifying and listing these resources and associated functionalities are limited to these Users only.

Fault Repair Time refers to the time elapsed between an Incident ticket's opening and its resolution, minus the periods during which The Service Provider' engagements do not apply.

Full France: the teams providing service and/or support are based in France.

General Terms and Conditions refers to the Service Provider' general terms and conditions for Cloud Services.

General Terms and Conditions means the general terms and conditions relating to the Service Provider's Cloud Services.

Git is a software program for managing code versions.

Guaranteed Availability Rate (or **GAR**) refers to the Availability Rate to which the Service Provider commits, for a given Managed Function, in accordance with the level of support to which the Customer has subscribed.

Guaranteed Change Time (or **GCT**) refers to the Change Time to which the Service Provider commits in the event of change request, limited to those changes in production environment described in the catalogue and validated by the Service Provider, in accordance with the level of support to which the Customer has subscribed.

Guaranteed Fault Repair Time (or **GFRT**) refers to the Fault Repair Time within which the Service Provider commits in the event of Incident in production environment, in accordance with the level of support to which the Customer has subscribed.

Hours worked refers to the hours between 9am and 6pm, Monday to Friday, excluding French public holidays.

IaaS means the cloud infrastructure service, including any associated complementary services (such as PaaS, CaaS, DBaaS, etc.), subscribed to by the Customer for the purpose of hosting its Managed Tenant.

IaC refers to infrastructure as code.

Incident refers to an unplanned event that causes Downtime or degradation of the Service or Feature concerned. An Incident is logged by a ticket with Priority P1, P2 or P3.

Kubernetes® means open source software for the deployment and management of containers. Kubernetes® Kis a registered trademark of The Linux Foundation. Please see kubernetes.io

Log As A Service refers to the service provided by components of the ECE (Elastic Cloud Enterprise) suite.
Middleware refers to the software components required to run an application, apart from operating systems (OS) and databases.

Managed Base refers to the technical foundation provided by the Service Provider to install and operate the subscribed Service Units.

Managed Function refers to the Service Units or sets of Service Units in production defined below:
- all Managed Service for Kubernetes® Units taken collectively.
- all Managed Computer Vision Service Units, taken collectively.
- all Managed Big Data Service Units, taken collectively.

- each Managed Application Service Unit, taken separately.
- each Managed Security Service Unit of the same type, taken separately.
- each Managed Backup Service Unit, taken separately.
- all Hyperscaler Native Service Units, taken collectively.
- all Log As A Service Units taken collectively.
- all Managed Middleware Service Units, taken collectively.
- all the Managed Database Service Units, taken collectively.
- all Managed OS Service Units, taken collectively.

Managed Tenant refers to the Tenant in which the Customer's Service is hosted. The actions of creating, destroying, modifying and listing resources and associated Features are limited to the Service Provider.

Middleware refers to the software components required to run an application, apart from operating systems (OS) and databases.

MRC (Monthly Recurring Charge) refers to monthly recurring charges.

Node refers to a virtual machine included in a cluster.

Native Hyperscaler Services means the services provided by the IaaS hyperscalers Amazon Web Services (AWS), Microsoft Azure (Azure), and Google Cloud Platform (GCP).

Off-Shore: the teams providing the service and/or support are partly based outside France.
Scheduled Maintenance Operations: refers to all Maintenance or Patch Management operations carried out at regular and anticipated intervals on hardware or software infrastructures within the Perimeter.

OTC (One Time Charge) refers to initialization costs and corresponds to a single charge.

Perimeter: refers to the Configuration Elements and Services to be performed by the Service Provider in accordance with the provisions of the Contract. At the Customer's request, this Scope may be modified either by amendment or during the RUN phase.

Platform means a subset of a Managed Tenant hosting one or more Software Products, which may include several Clusters.

Priority refers to the following levels used by The Service Provider to classify Incident tickets:

- **Priority 1** (or **P1**): complete loss of Service for multiple Users, or Incident with a critical impact on the Customer's activities
- **Priority 2** (or **P2**): Services deteriorated, Users are able to access the Services, but experience difficulties or must deal with significant delays.
- **Priority 3** (or **P3**): Services provided with delay or minor difficulties. The Customer's activity is not significantly impeded.
- **Priority 4 (**or **P4):** these tickets are not related to Incidents, and quality of service commitments by the Service Provider are not applicable.

Project means the project for which the Customer subscribes to the Service and referenced in the Order.

PQSC (Customer Service Quality Plan) means all the measures taken by the Service Provider to provide services within the scope of the Contract, in compliance with the provisions of the Contract. The PQSC specifies the conditions under which services are to be provided, which are visible to both Parties, and not information which the Service Provider alone has control over and visibility. No provision of the PQSC may call into question the provisions of the Contract.

RACI refers to the definition of responsibilities between the Customer and the Service Provider. R = Responsible, A = Authority responsible, C= Consulted, I = Informed.

Recovery Time means the time elapsing between the opening of an Incident ticket and its resolution, less any periods during which the Service Provider's commitments do not apply.

Region means a geographical area in which the Service is available on one or more Availability Zone(s).

Scheduled Maintenance Operations: refers to all Maintenance or Patch Management operations carried out at regular, anticipated intervals on hardware or software infrastructures within the Perimeter.

Service means the Managed Applications service provided for a Managed Tenant. Each Managed Tenant Customer constitutes a separate Service.

Service Credit means financial compensation granted to the Customer in respect of penalties for failure to meet service quality commitments.

Service Unit means a subset of the service provided on a Virtual Machine (VM) or on a physical server in the case of the Managed OS, Managed Database or Managed Middleware Functionalities, and on one or more VMs or physical

server(s) in the case of the Managed Application Functionality. The Customer subscribes to the Service Units by means of the Purchase Order.

Service Pack means a set of Software updates, fixes and/or enhancements delivered as a single package that can be installed in a single operation.

Simple Standard Change refers to a Standard Change to a Token initiated by the Customer or the Service Provider that requires little effort, or has an impact on a limited number of services, implemented by a procedure validated by the Service Provider and accepted by the Customer. Any change considered Simple is defined in the list of standard changes in the change catalog accessible through the Cloud Store Customer Area.

Slave node: a data node responsible for responding to read and write requests from file system clients, as well as for creating, deleting and replicating blocks on the instructions of the master node, and for monitoring tasks carried out by a cluster node.

Standard Change refers to a change initiated by the Customer or the Service Provider, implemented by a procedure validated by the Service Provider and accepted by the Customer. Any change considered as Standard is defined in the list of standard changes in the change catalog, accessible through the Cloud Store Customer Area. The price of standard changes is defined and known by the Customer.

SIEM (Security Information and Event Management) refers to the management of security-related information and events.

SoW (Scope of Work) refers to the scope of work during the pre-sales phase, based on the customer's requirements.

SRF (Service Request Form) refers to the form to be completed to describe the technical characteristics of the services to be delivered.

SRE (Site Reliability Engineer) refers to the expertise provided by the Service Provider for ongoing advice and technical assistance on the Customer's environment.

SSO (Single Sign-On) refers to a method enabling a User to access several functionalities by means of a single authentication.

Token refers to the work unit used to state the prices applicable to the changes requested by the Customer, as mentioned in the Price List.

Tenant means a virtual private space of resources on the IaaS to which only Users authenticated by login and password can have access. The actions of creating, destroying, modifying and listing these resources and associated Functionalities are limited to these Users only. For VMware IaaS, the Tenant is also referred to as the "Organization".

Transition class refers to the scope of responsibility of the Customer and the Service Provider for the transition of the Customer's environment to the Cloud. An inventory of the resources to be managed is carried out by the Service Provider to select the transition class best suited to the Customer's context.

URL (Uniform Resource Locator) refers to an access point in the form of a web address.

Workload means a Customer's application environment to be executed on a Service Provider's Cloud resource.

Working days means days from Monday to Friday, excluding French public holidays.

11 Annexes

1.1 Managed OS: https://cloud.orange-business.com/en/technical-appendix-to-the-managed-applications-service-description-managed-os/

1.2 Managed Database: https://cloud.orange-business.com/en/technical-appendix-managed-database/

1.3 Managed Middleware: https://cloud.orange-business.com/en/technical-appendix-managed-middleware/

1.4 **Managed Service for Kubernetes®:** Technical-appendix-Managed-Service-for-Kubernetes®.pdf

1.5 Managed Application: https://cloud.orange-business.com/en/technical-appendix-managed-application/

1.6 Managed Services Natifs Hyperscalers:

1.6.1 Azure: https://cloud.orange-business.com/en/technical-appendix-managed-applications-on-azure-2/

1.6.2 AWS: https://cloud.orange-business.com/en/technical-appendix-managed-applications-on-aws-2/

1.6.3 GCP: https://cloud.orange-business.com/en/technical-appendix-google-native-managed-service/

1.7 **Managed Big Data:** https://cloud.orange-business.com/en/technical-appendix-managed-big-data/

1.8 Managed Computer Vision: https://cloud.orange-business.com/en/technical-appendix-managed-computer-vision/

1.9 Managed Active Directory:

1.10 Managed RDS: https://cloud.orange-business.com/en/technical-appendix-remote-desktop-service/

1.11 Managed Security: https://cloud.orange-business.com/en/technical-appendix-managed-firewall-and-load-balancer/

1.12 **Managed Citrix Workspace:** Annexe-technique-Citrix-Workspace-Manage.pdf

1.13 **Managed Exchange:** Annexe-technique-Exchange-Manage.pdf