Security White Paper

ORANGE BUSINESS

CLOUD AVENUE DYNAMIC

Version: 2.0
Date: 01/22/2026

Business

Document description

Properties				
Document title	Cloud Avenue Dynamic - White Paper Security			
Version	2.0			
Editor	Business Security Officer (BSO) Cloud Avenue Dynamic			
Status	❑ In progress	❑ Review	■ Validated	❑ Approved
Date	Thursday 22 January 2026			

Document classification

Classification	
Confidentiality	Free dissemination

Dissemination

Company	Function	Rights
Orange Business Global Delivery & Operations (GDO) Sales		Read
	BM-GDO Sales	Approve
		Read
Orange Business/ lobal Delivery & Operations (GDO) / Global Platforms & Service (GPS)	Chief Information Security Officer (CISO) GDO/GPS	Read
	BSO Cloud Avenue Dynamic	Write

Version history

Version	Operation	Name	Date
1	Creation of the document	BSO Cloud Avenue Dynamic	January 2026

Summary

Orange Business Security White Paper

1. Introduction 5

1.1. Purpose of this document 5
1.2. Document organization 5

2. Cloud Avenue Dynamic's security strengths 6

2.1. Governance & Compliance: 6
2.2. Accommodation 6
2.3. Architecture 6
2.4. Support and accompaniment 7

3. Organizational security measures 8

3.1. Security policy 8
3.2. Organization of security 8

3.2.1. Relationships with technology partners for vulnerability management and infrastructure optimization 8
3.2.2. Business Security Officer 8

3.3. Asset management 14

3.3.1. Inventory 14
3.3.2. Measures for the protection of supporting assets 14
3.3.3. Erasure of data 15

3.4. Access control 15

3.4.1. Access control for Orange operators 15
3.4.2. Access control for Orange customers 17

4. Security measures applicable to people 18

4.1. Mastery of the stakeholders 18
4.2. Selection of candidates 18
4.3. Awareness 18
4.4. Written commitment of the speakers 19

4.4.1. Confidentiality commitment of the stakeholders 19
4.4.2. Charter for the good use of computer resources 19
4.4.3. End of contract 19

4.4.4. Remote work 19

5. Physical security measures 20

5.1. Physical and environmental security of our accommodation centers 20
5.2. Physical and environmental safety of our operating platforms 22

6. Technological security measures 23

6.1. Cryptography 23
6.2. Operational security 24

6.2.1. Management of operational procedures 24
6.2.2. Protection against malicious code 25
6.2.3. Backup management 25
6.2.4. Logging and security supervision 26
6.2.5. Management of technical vulnerabilities 27

6.3. Communications security 29

6.3.1. Security of Orange Cloud architecture 29
6.3.2. Security exchange 30
6.3.3. Protection against denial of service and intrusion 31

6.4. Acquisition, development and maintenance of information systems 31

6.4.1. Risk analysis 31
6.4.2. Development and Integration Best Practices 32
6.4.3. Safety validations 32

6.5. Subcontractor Management 33

6.5.1. Contractual Subcontractor security 33
6.5.2. Monitoring the security of the services provided by our subcontractors 33

6.6. Security incident management 33
6.7. Security of business continuity management 35
6.8. Compliance 36

6.8.1. Compliance with legal and contractual requirements 36
6.8.2. Control of compliance with security policies 36
6.8.3. Certifications related to safety 37

1. Introduction

1.1. Purpose of this document

This Orange Business White Paper pertains to the provisioning of the Cloud Avenue Dynamic service offer to its customers. It describes the main technical and organizational security measures implemented by Orange Business to ensure the security of the offers contained therein.

This document applies to professional cloud offers marketed by Orange Business in all business-to-business contexts. The offers addressed in this document are:

- Cloud Avenue Dynamic

1.2. Document organization

This document follows the chapter organization of ISO 27002-2022 as follows:

- Chapter 1 constitutes the introduction to the document.
- Chapter 2 is a summary of the strengths of Cloud Avenue Dynamic on security aspects.
- Chapter 3 lists the organizational security measures implemented.
- Chapter 4 details the security measures applicable to people.
- Chapter 5 concerns the physical security measures implemented.
- Chapter 6 lists the technological security measures implemented.
- Annexes.

2. Cloud Avenue Dynamic's security strengths

This chapter highlights Cloud Avenue Dynamic's robust security policies.

2.1. Governance & Compliance:

The security of Cloud Avenue Dynamic is founded on rigorous governance and certified compliance. The offer benefits from a comprehensive normative framework, supported by numerous certifications such as ISO 27001, SOC 2, and CISPE standards, which ensure the implementation of best international practices in information security management and data protection within the context of European business-to-business cloud computing services.

Finally, compliance with GDPR is guaranteed by the data being located and fully processed within French territory and under the relevant national jurisdiction.

2.2. Accommodation

All data is hosted in datacenters located exclusively in France, specifically in Val-de-Reuil and Chartres. These infrastructures are owned and operated directly by the Orange Group.

Orange's datacenters are designed to provide a very high level of resiliency, featuring energy, network, and geographical redundancy, as well as continuous monitoring. These features, which customers can subscribe to, enable best-in-class on-premise, on-site, and multicloud mitigation strategies to support disaster recovery for all types of assets, whether virtual or physical.

2.3. Architecture

The technical architecture of Cloud Avenue Dynamic is built on a robust foundation based on VMware vCloud Director and NSX-T technologies. This foundation ensures strict client isolation through advanced network segmentation and secure resource virtualization.

Each customer benefits from distinct and controllable environments, with the option to choose dedicated infrastructures via the VMware vCenter On Demand component. These options guarantee both logical and physical partitioning of data and workloads.

Connections are secured by integrated network security features, such as distributed firewalls, flow filtering, IPsec VPN, and MPLS connectivity certified at EAL2+. Additionally, anti-DDoS protection mechanisms and advanced filtering options strengthen the availability and security perimeter of customer environments.

2.4. Support and accompaniment

Beyond its technological strengths, Cloud Avenue Dynamic is distinguished by the quality of its support. Support is provided by teams of cloud and security experts who are available around the clock. Orange Business offers a comprehensive set of documentation resources, technical guides, and best practices accessible via the Cloud Avenue Dynamic wiki, fostering customer autonomy while maintaining a secure framework: https://cloud.orange-business.com/offres/infrastructure-iaas/cloud-avenue/wiki-cloud-avenue/accueil/presentation-de-cloud-avenue/

Support for environment migration and security is also included in the offer, with tailored advice addressing the specific challenges faced by each customer organization.

3. Organizational security measures

This chapter corresponds to theme 5 of ISO 27002 version 2022.

3.1. Security policy

The security policies are aligned with ISO 27001 and ISO 27002 standards. Cloud Avenue Dynamic follows the security policies and regulations of Orange Group.

3.2. Organization of security

This chapter describes the organization of Cloud Avenue Dynamic from a security point of view.

3.2.1. Relationships with technology partners for vulnerability management and infrastructure optimization

We maintain strategic technological partnerships with leading vendors and integrators, including VMware, to enhance and secure patch management and continuous analysis of our production infrastructure. Each partner provides Orange Business with access to security advisories, best practices, and recommended escalation policies for each product line.

The goal is to ensure measurable security and operational readiness, while reducing vulnerability response times and minimizing the risk footprint for all our customers.

3.2.2. Business Security Officer

The customer (signatory) may subscribe to an additional Business Security Offer (BSO) service upon contract signing. In this context, Orange Business appoints a BSO to manage security for all or part of the duration of the service contract.

By default, this option's aims are to:

- Provide a privileged Business Security Officer contact within Orange Business' security department to monitor service security and provide security advice
- Furnish the collection of predefined safety indicators and periodic reporting in the form of a safety dashboard and safety committee oversight
- Contribute to the coordination and prioritization of corrective actions in the event of security incidents
- Support the infrastructure during its audits and follow corrective action plans
- Provide an annual update of the security documentation and a personalized Security Assurance Plan

The Business Security Officer, in relation to Cloud Avenue Dynamic, ensures that task segregation is respected and that the WSIS policy is properly applied, thereby providing relevant security indicators. (S)He guarantees the implementation of information security measures throughout the contractual service period. (S)He also considers the client's specific requirements and regulatory constraints (such as HDS certification, GDPR) to propose possible adjustments or new services.

The responsibilities of the Business Security Officer can be extended and customized according to your business needs, including reporting frequency, dashboard indicators, audit schedules, security documentation updates, and management of dedicated infrastructure security (such as premises, IT, and dedicated personnel).

3.2.2.1. Safety committees

The Cloud Avenue Dynamic "Security Committee" is a body that regularly monitors general implementation progress of our security policies as apply to our customer solutions. It is organized and facilitated by the Business Security Officer.

SW01 - COSEC (Safety Committee)		
Scope of the covered service	Entire service	
Typical agenda	For the past period ▪ Review of security alerts ▪ Review of safety indicators ▪ Review of the PAS	
Frequency	1 COSEC quarterly	
Participants	Orange Business Security: - BSO	Orange Business: - Cloud Avenue Dynamic
Input documents	Committee support documents	
Output documents	Report	

This frequency can be adjusted by the Business Security Officer according to the needs of Cloud Avenue Dynamic.

Indicators and dashboards

The SSI of the Contract will be managed through indicators that will all be produced by the BSO and analyzed in detail during the security committee.

Below, you will find a list of elements applicable to the contract and their reporting frequency.

3.2.2.1.1. Primary Indicators (Run)

Security Weather Reports

01

Security Governance

Security governance is a continuous steering committee for the security posture of the offer, in coordination with the Global Platforms & Services teams. Its scope covers the updating of risk analyses, vulnerability monitoring and remediation, execution and monitoring of action plans, incident management and changes with a security impact, as well as compliance/audits, security testing and business continuity.

02

Security Committee

Presented to the security committee, the security dashboard contains the various indicators of this Security Assurance Plan and more generally relates the health status of the Global Platforms & Services Cloud solution.

Vulnerability Review

01

Vulnerabilities Management

The Business Security Officer monitors vulnerabilities that may affect the solution's machines. A report is formalized in the form of indicators and reported to the safety committee.

02

Vulnerability Health

Particular attention is paid to level 4 (High) and 5 (Critical) vulnerabilities. This indicator is reviewed in the security committee. A report is formalized and reported to the security committee.

3.2.2.1.2. Complementary Indicators (Run)

Security Review

01

Accounts Access Review

The Business Security Officer conducts a review of all the platform's accounts and validates access. He reports to the security committee.

02

Password Policy and Rotation Review

The Business Security Officer verifies the password policy implemented on all the offer's accounts and the proper rotation thereof. He reports to the security committee.

Technical Review

05

System Configuration Review

The Business Security Officer follows the evolution of system configurations to identify any changes likely to lower the security level and/or identify opportunities for hardening.

06

Operation System Obsolescence

The Business Security Officer highlights and monitors the evolution of the obsolescence of the operating systems, equipment, and applications that make up the contract.

Physical Security Review

At the client's request, an annual visit to our datacenters can be organized as part of an audit to verify the proper implementation of the measures described in this document.

3.2.2.1.3. RACI

Cloud Avenue Dynamic is an IaaS (Infrastructure as A Service) type infrastructure. The following accountability model is applied:

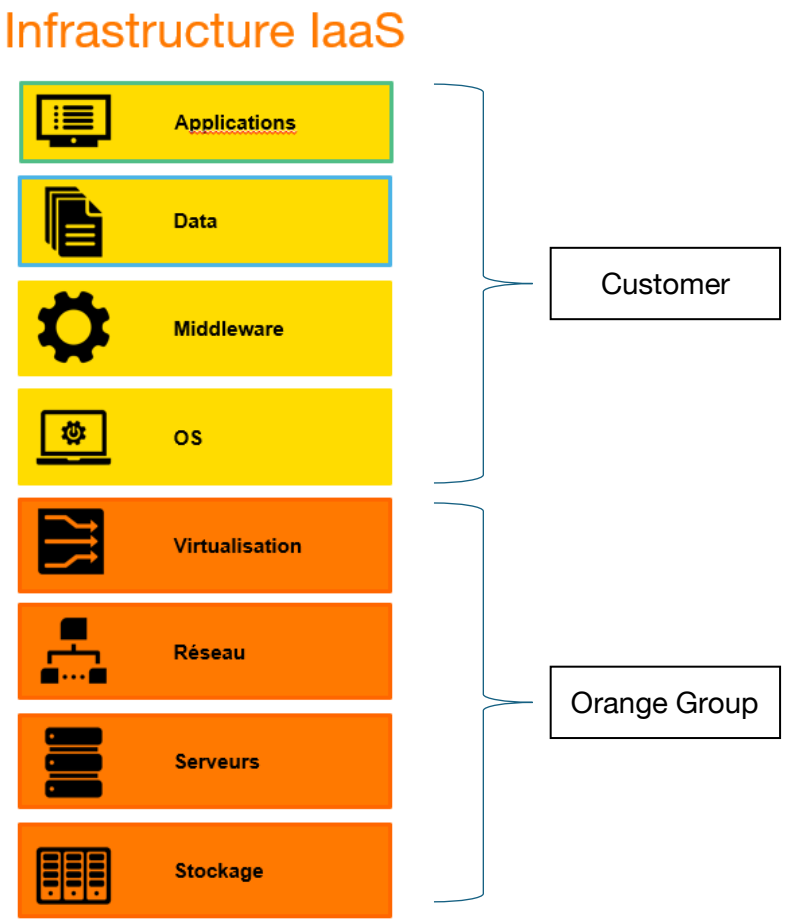

Figure 1: IaaS Infrastructure

3.3. Asset management

3.3.1. Inventory

The list of supporting assets (routers, switches, firewalls, storage bays, servers, virtual machines, software...) of the Cloud offers is maintained in internal Orange Business information systems tools. These tools trace both the components of the infrastructure of Cloud Avenue Dynamic and the components of the client's environment (e.g. Virtual Machine, virtual firewalls ...).

These inventories are updated as part of the change management process.

3.3.2. Measures for the protection of supporting assets

Classification of infrastructure resources

The infrastructure resources are classified on a 4-level scale, defined in Orange's Global Security Policy, and allowing the qualification of the damage for Orange and its customers in case of an incident on the resource:

- **Level 4**: vital impact, very important issues corresponding to unacceptable risks.
- **Level 3**: critical impact, important issues corresponding to risks whose effects must be limited.
- **Level 2**: sensitive impact, moderate stakes and controlled risks with limited harm to the company.
- **Level 1**: zero or near-zero impact.

All Cloud Avenue Dynamic resources hosted in our datacenters (routers, switches, storage and backup bays, servers, ...) are considered at least level **3 (either level 3 or level 4). Measures associated with the protection of these critical resources are described throughout this document.**

Classification, marking and protection of documentation

The documentation is classified and then marked, in accordance with internal Orange policy defined in the document 'Marking of documents'. Four levels are defined: **free distribution, restricted Orange, confidential Orange** and **Sovereign Orange.**

The operational documents of the Cloud Avenue Dynamic projects / offers are stored on file servers. Access is protected by nominative access control and rights management managed according to the need-to-know principle.

Classification of customer information

The classification of customer information hosted on the Cloud Avenue Dynamic offer is under the responsibility of the customers.

3.3.3. Erasure of data

Protection of de-allocated client data

Customer data on rescinded resources is protected from access by other customers. The products used by Orange, such as VMware, ensure that, for example, if storage resources are reallocated, the new customer cannot access or see the data of the previous customer.

Deletion of client data at the end of the contract

At the end of the contract, all resources assigned to clients are rescinded, and client data becomes unusable, as mentioned in the previous paragraph.

Only the backups are kept for a few months by Orange after the end of the contract. After this period, Orange no longer holds any data from its ex-clients.

3.4. Access control

Orange ensures access control on environments contractually under its responsibility. Access control of the systems and applications managed by the client is under (h)his responsibility.

3.4.1. Access control for Orange operators

Means of access

Orange operators administer the Cloud Avenue Dynamic infrastructure (servers, storage arrays, network equipment, security equipment...) as follows:

Note: for some offers, client VMs can be managed by Orange, we then talk about managed or co-managed services. This specific administration mode is not described in this paragraph but in the specificities of each offer (which are the subject of a white paper specific to these offers).

- **1 – Access from the Orange internal network.** The administration of the Cloud infrastructure is only possible from the internal Orange network and from highly secure bastions.
- **2 – Filtering and nominative authentication at the input of the administration platform.** The Cloud Avenue Dynamic platform is protected from the Orange internal network by an intermediate security zone, called the administration platform, which hosts bounce servers. This step allows us to ensure:
  - Network filtering
  - Of nominative authentication and access tracking
  - Logging sessions on a centralized log server
  - Only the administrator can access authorized resources for his profile
- **3 – Additional filtering on the cloud platform.** This is an additional set of rules (firewall/ACL/security groups) added to the existing one so that only administrative access to the cloud infrastructure comes from the administration platform.
- **4 - Authentication of operators on Cloud environments. The authorized administrator authenticates herself on the component they wish to administer:**
  - Authentication with centralized (AD, TACACS+) or local accounts
  - Logging sessions on a centralized log server
  - Authorization: the administrator can only access resources authorized by their profile
  - Traceability: tracking of administrator actions, automatic renewal of server passwords

Administrative access is always carried out securely via the SSL/TLS protocol (flow examples: HTTPS, SSH).

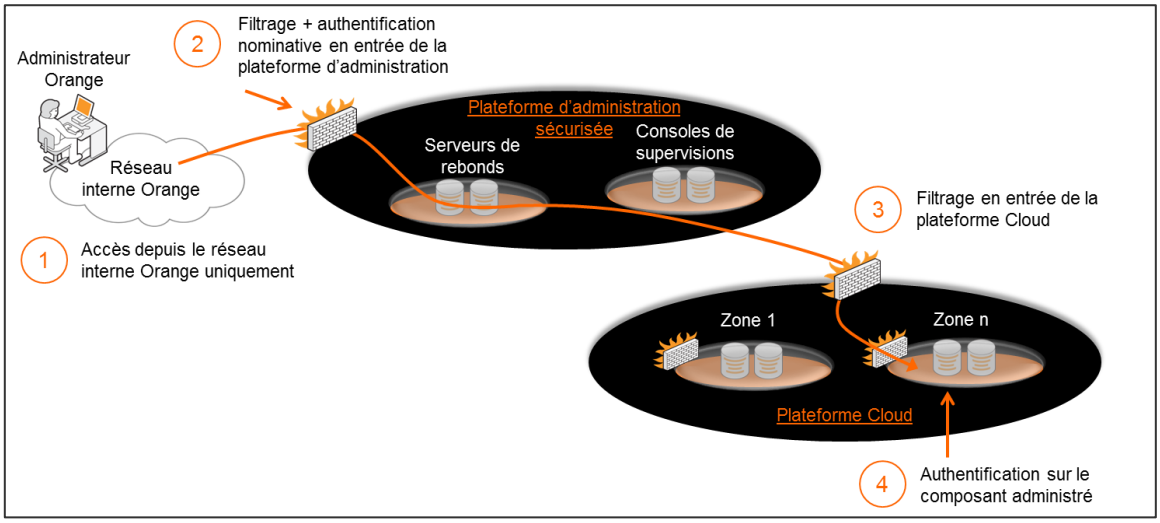

Figure 2: Access administration Cloud Avenue Dynamic

Authentication and password management

Logins with operational accounts adhere to internal password management policies. For staff, a token containing a certificate is issued by the Orange Group's PKI (Public Key Infrastructure) system and stored on this token to ensure enhanced multi-factor authentication.

Procedure for granting and revoking rights for Orange operators

The procedure for assigning/revoking an account and associated rights is applied and controlled. This procedure is a security measure of the ISO 27001 certified SMSI (Information Security Management Systems), implemented by Orange.

Shared accounts are only exceptionally allowed in the form of a waiver. They must be listed and justified.

Review of rights for Orange operators

A periodic review of authorizations and rights is conducted and documented. This activity involves extracting the list of users with operational accounts on Cloud Avenue Dynamic. The list is then reviewed by the manager, who determines whether each account should be maintained or deactivated. If an operational account is deemed unnecessary, it is subsequently deleted. In case of discovery of illegitimate rights, the appropriate measures are applied:

- Account suspension.
- Examination of traces of use to reveal any incidents.
- Taking corrective measures (updating procedures, management awareness...).

3.4.2. Access control for Orange customers

Customers connect to Cloud Avenue Dynamic environments for administration or application service access. Accesses are made via the Internet and/or a private network (client VPN) according to the offers and options selected by the client.

Client access is always carried out securely via the SSL/TLS 1.3 protocol (flow examples: HTTPS, SSH):

- Server authentication (administration portals, application servers) is systematically carried out via an X.509 "server" certificate issued by a recognized certification authority
- Customer authentication is performed using a login and password securely transmitted to each customer in advance. For certain offers, strong authentication can be implemented, such as the use of a software token generating a one-time password or the use of an X.509 client certificate.
- Network flows are systematically encrypted in accordance with state-of-the-art practices.

The client is responsible for the security of the authentication elements provided by Orange. To the extent possible, using password strength measurement tools, Orange enforces a minimum complexity requirement for all passwords managed by the client.

For certain offers, the customer may create access accounts himself (user profiles, administrator). The identifiers and associated access rights are the responsibility of the client.

All client connections are recorded in event logs which are archived in accordance with current legislation.

4. Security measures applicable to people

This chapter corresponds to theme 6 of ISO 27002 version 2022.

4.1. Mastery of the stakeholders

A list of stakeholders for Cloud Avenue Dynamic is maintained as part of the input/output management process. This list serves as a reference for reviewing logical authorizations. Access rights for stakeholders are updated or revoked promptly when their roles change or when they leave the company.

4.2. Selection of candidates

Candidates selected for employment based on CVs and cover letters are subject to multiple checks in compliance with local hiring regulations, including but not limited to a verification of the identity card, the recovery of diplomas or certificates of achievement (certifications, recommendations...).

The control of stakeholders by the authorities takes place within the framework of local regulations instead of hiring.

4.3. Awareness

Awareness-raising actions regarding Information Systems security primarily consist of training provided to all Orange staff.

Additional activities are regularly conducted to maintain awareness levels, including communication messages on good security practices and the involvement of security experts in team meetings. In case of imminent threats, security alert messages—such as phishing campaign notifications—are promptly sent to all employees.

Semi-annual awareness sessions focusing on security risks, especially legal and regulatory risks, are organized for top management.

A dedicated space on the company's social network is available for staff to access training materials, specific guidelines, and to ask questions to internal security experts through a dedicated forum.

4.4. Written commitment of the speakers

4.4.1. Confidentiality commitment of the stakeholders

Employees have a general obligation of discretion enshrined in their employment contract and/or in their collective agreement. Below is an excerpt from an Orange employment contract:

> 'Article 10: Professional secrecy and the duty of discretion
>
> Like all Orange staff, Madam/Sir _____ is bound by absolute professional secrecy. This requirement applies during the execution and suspension of the employment contract as well as after its termination, and concerns in particular the techniques implemented by Orange, as well as all studies and work carried out within the company.
>
> It also applies to any information of a confidential nature, in particular that is not usually communicated to the public, which Mr/Mrs _____ might collect on the occasion of his/her duties or solely because of his/her presence at Orange.
>
> Failure to comply with this confidentiality requirement would constitute misconduct and could be subject to civil and/or criminal proceedings.

4.4.2. Charter for the good use of computer resources

Similarly, all employees must, by internal regulations, comply with the charter for the proper use of IT resources.

4.4.3. End of contract

As part of the end of contract at Orange Business, the process is conducted in accordance with group policies and procedures. All materials are blanked (secure deletion), all access revoked, and the related data permanently erased. Compliance checks and associated evidence (revocation logs, erasure certificates) are duly archived.

4.4.4. Remote work

In accordance with the employment contract and the teleworking chart of Orange Business, both directors and all employees can carry out their activities remotely, within the limits and conditions provided for. (eligibility, weekly quota, managerial agreement, right to disconnection, HSE rules). The practical arrangements (provided equipment, support, support) are defined and communicated via the official Orange Business channels.

Remote work is, by default, framed by mandatory security rules: exclusive use of managed and encrypted equipment (MDM, up-to-date patches), connection via VPN with MFA, production access only via bastion/PAM according to the principle of least privilege. Privacy and data protection policies apply everywhere, with session locking, secure working environment and obligation to report any incident. Controls and audits verify compliance with these measures, with reinforced requirements for sensitive functions (administrators, privileged access).

5. Physical security measures

This chapter corresponds to theme 7 of ISO 27002 version 2022.

Physical and environmental security aims to protect the information system of Orange and its customers against:

- Environmental threats and disasters: explosions, earthquake, fire, water damage, power outage, air conditioning failure, telecom failure...
- Threats of physical intrusion: access to the room by an unauthorized person, theft of hard drives containing sensitive information...

5.1. Physical and environmental security of our accommodation centers

Our Cloud Avenue Dynamic offer (infrastructures, backups...) is hosted at two datacententers located in Val-De-Reuil and Chartres France. The main site is Val-De-Reuil, Chartres is the backup site.

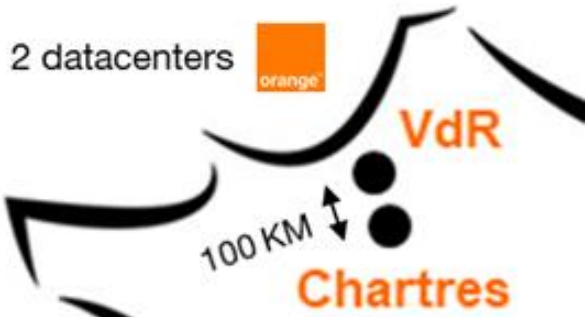

Figure 3: Location of Cloud Avenue Dynamic datacenters in France

The following security measures are implemented at these Orange datacenters:

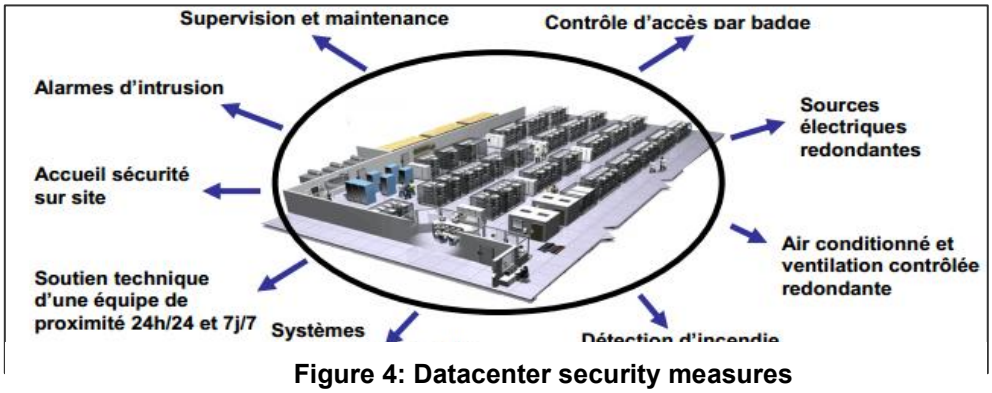

Figure 4: Datacenter security measures

ISAE 3402 - All aforementioned datacenters are certified ISAE 3402 Type II (ex. SAS 70). ISAE 3402 is the standard that allows clients who outsource to obtain assurance regarding the reliability of the internal control system for their services. Since 15 June 2011, it has replaced the SAS 70 standard and is applicable to international commitments. As such, independent auditors have performed rigorous checks over a 12-month test period to validate the quality, reliability and integrity of Orange's operational processes and controls. This independent audit report assures Orange Business customers that the services they receive meet the requirements of the US Sarbanes-Oxley Act and meet **key security**, change management and service continuity objectives.

TIER Classification - The datacenters of the Cloud Avenue Dynamic offer are built and operated to meet TIER IV requirements.

Fault and maintenance tolerance - The technical architecture implemented make it possible to meet the following operational constraints:

- Absence of impact on the load during the first fault
- High fault tolerance, up to 2 major defects without impact
- Absence of service interruption during a maintenance intervention

The management method and processes implemented ensure the safety of people, buildings, and hosted equipment.

The architecture implemented for Cloud Avenue Dynamic includes distribution across the 2 sites (Val-De-Reuil and Chartres France) in active/active mode at the server level. Internet access is doubled in active/passive mode on the 2 sites.

Detailed specifications in the site booklets[1] - The specifications of our datacenters are detailed in site booklets that address the following themes:[1]

- Energy (redundancy of adductions, redundancy of general low voltage distribution boards, generator with a minimum autonomy of 72 hours, inverters ...).
- Air conditioning (N+1 redundancy, that the breakdown of an air conditioning system has no impact on the cold production chain).
- Urbanization (alleys, false floors ...).
- Fire protection (detection, extinguishing, supervision center, ...).
- Water damage protection (detection, pumps ...).
- Intrusion protection (security barriers/walls, access control, video surveillance, guards, patrols, intrusion detection, guest management ...).
- Organization of security on sites (managers, 24/7 monitoring, responsiveness, ...).
- Environmental safety (absence of natural risk ...).

[1] Site booklets: these booklets are confidential but can be consulted at Orange premises after signing a confidentiality agreement.

5.2. Physical and environmental safety of our operating platforms

The operating facilities are the premises from which Orange Business operates its Cloud Avenue Dynamic offers. The different international support level teams and personnel are set up as follows:

- Orange Business major service center (MSC) in India, Egypt and Poland: levels 1 & 2 infrastructure support (firewall, servers, network...)
- Orange Business personnel in France: level 3 of Cloud Avenue Dynamic

The following operations centers, located in Cesson-Sévigné, India, Egypt and Poland, have an ISO 27001 security certification issued by AFNOR, whose site addresses are indicated on the certificates. The functional scope of certification is the implementation, provisioning and support of managed services and communications solutions.

As part of the provisioning of cloud services, Orange Business may have to transfer customer data outside the European Union to the MSCs mentioned above. Within the group, an 'Agreement for the transfer of customer personal data' has been in effect since January 2 2013. According to this "Agreement", the personal data that customers (as data controllers) transfer to Orange Business (as subcontractor or sub-processor) benefit from an adequate level of protection as required by the European Commission. Each legal entity of Orange Business located outside the European Union in a country that does not ensure an adequate level of protection as required by the European Commission has committed, by signing this "Agreement", to comply with the European Directive 95/46/EC, and has thus agreed to be bound by the standard clauses of the European Commission.

6. Technological security measures

This chapter corresponds to the theme 8 of ISO 27002 version 2022.

6.1. Cryptography

Cryptographic suites - All the cryptographic suites used on Cloud Avenue Dynamic offers (e.g. AES 256, SHA-256, TLS 1.3) are based on market standards with proven security levels. The ENISA technical study[2], 'Algorithms, Key Size and Parameters Report, 2013 Recommendations' was considered to choose the cryptographic suites. Administration flows are systematically encrypted using the SSL/TLS protocol.

Certificate management – Server authentication certificates are based on certification authorities (e.g. VeriSign, Thawte...) recognized by all current web browsers. The authentication certificates for our internal administration services (accessible only by Orange IT personnel) can be based on X.509 certificates generated by Orange's internal certification PKI authority.

Encryption of Orange operators' hard drives – To secure sensitive data, Orange IT personnel have an additional encryption solution with token authentication (ZoneCentral from Prim'X). This solution has been certified EAL3+ on its version 3.1 by the French ANSSI government oversight body (National Agency for Information Systems Security).

KMS: A key ceremony was conducted on Cloud Avenue Dynamic in accordance with our cryptographic management policy and ISO/IEC 27001 (key management) best practices. This includes security piloting with role separation and dual control, key generation and initialization in a certified HSM, full traceability (signed commitment charter, attendance list, registration and seal numbers), successful technical verifications (KCV, encryption/decryption tests), as well as the implementation of a controlled life cycle (e.g. planned rotation and revocation procedures).

[2] ENISA: European Network and Information Systems Agency

6.2. Operational security

6.2.1. Management of operational procedures

ISO 20000 and ITIL certification

The management of[3] services by Orange Business is ISO 20000 certified. The requirements of ISO 20000 certification are aligned with the best practices of the latest version of ITIL (v4 2019) for processes such as service provisioning, relationship management, problem solving, control and release, as well as reinforced security requirements.

Change management

Change management is carried out according to the ITILv4 model; this concerns changes related to security. Change management is carried out under the responsibility of Orange business Change managers'.

- Standard changes, pre-identified in a catalog, follow a simplified process and do not require security exptertise
- Changes identified as being "non-standard" (evolutions) are formalized in RFCs (Requests for Change) with a transition to a CAB (Change Advisory Board) meeting. The RFCs are subject to a prior security study by a security expert from Orange Business' Cloud Security Competence Center which provides opinions and oversight. Security is therefore represented at the CAB; it has the authority to prohibit a change deemed dangerous or uncompliant with security policies, and does so in an independent manner
- The CAB takes place weekly. For urgent changes (example: critical security updates), it is possible to immediately process the change request within the framework of an ECAB (Emergency Change Advisory Board) meeting.

The change management implemented by Orange Business thus allows for:

- Minimizing the impact of changes on operated user services
- Standardized methods, procedures and control mechanisms
- Identifying the interlocutors authorized to request changes
- Controlling changes so that they correspond to Orange Business security policiec
- Formalization of spot-on impact, priority, benefit, and change risk assessments
- Defining categories of associated changes and rollout timelines
- Managing change priorities based on risks and impacts
- Improving the quality of information and communication:
    - Ensuring that all relevant parties have been involved to limit incidents related to changes
    - Populating the configuration database with correct information
    - Ensuring that all changes are documented
    - Proactively communicating planned unavailability to customers/end users

[3] Associated certificate: https://certificats-attestations.afnor.org/certification=335171233155

Capacity management

Capacity management is carried out in accordance with the ITIL 4 model under the responsibility of an Orange Business Capacity Manager. The goal is to ensure a consistent level of service for customers. Capacity management makes it possible to anticipate each customer's future needs by analyzing measurements and consumption trends across the resources that make up both the individual and overall cloud infrastructure.

Capacity management monitors and acts primarily on:

- CPU/RAM resources
- Network resources (bandwidth, IPAM)
- Storage and backup resources
- Software licenses

For Cloud Avenue Dynamic, Capacity Managers regularly compile statistics with different indicators (technical measures, business forecasts).

6.2.2. Protection against malicious code

Client environment

The Cloud Avenue Dynamic offer includes a dedicated antivirus service (Trend Micro) for customer environments. If the customer already has its own antivirus solution, there is no need to install this service.
The antivirus agent installed on the systems updates its components every hour, including the agent version, the virus signature database for real-time threat detection, file behavior analysis, and memory inspection, through a dedicated update server located in a security zone reserved for customer machine updates. This antivirus signature server is itself updated in real time from public servers made available on the Internet by the publisher.

6.2.3. Backup management

Client environment

Data from customer environments are backed up according to the Cloud Avenue Dynamic backup policy and based on the options selected by the customer. In general, customer data is automatically and periodically saved with a retention period that depends on the chosen catalogue offer.

Backups can be of different types depending on the offers and options. For example:

- Backup in file mode ('file level'), particularly for application data
- Image level backup for virtual machines
- Raw data backup (file servers)

Data restoration and recovery methods vary according to the offers and customer needs:

- Restoration was carried out by the client independently
- Restoration carried out by Orange Business upon request for change via the administration portal

Orange Business Infrastructure

All configurations of the equipment of Cloud Avenue Dynamic infrastructures are saved regularly. In particular:

- Servers: Windows, Linux, application data (including databases)
- Network equipment (routers, switches)
- Security equipment (UTM firewall, VPN appliance)
- Storage equipment

For static configurations, backups are performed whenever the configuration is changed. The backup operation is governed by the change management process.

For dynamic configurations, agents perform automatic backups on a periodic basis. Configuration data is retained for at least 14 days, and several backup versions are kept.

All configuration backups are stored at third-party sites (separate datacenters) to ensure the availability of configuration data in the event of a major disaster affecting the production site. Backups are stored securely, with logical partitioning and access granted on a need-to-know basis.

6.2.4. Logging and security supervision

Orange ensures systematic supervision of its infrastructure and cloud services, particularly from a security point of view. Event logging is implemented for all components, notably security components. This logging has several aims:

- Detecting and analyzing security incidents
- Meeting legal obligations
- Enabling troubleshooting

All components are supervised 24/7 and on-call procedures are set up to intervene in critical incidents, particularly when safety is impacted.

Nature of the security logs

The logged events are defined component by component, according to two criteria:

- Legal requirements: In France, the LCEN[4] and CPCE[5].
- Security requirements:
  - Events related to administration activities for all components.
  - Events of security components (example: firewall logs).

In France, logging and monitoring of logs are carried out in accordance with the Data Protection Act.

[4] LCEN: Law for Confidence in the Digital Economy
[5] CPCE: Postal and Electronic Communications Code

Centralization of security logs

All components of the cloud infrastructure periodically or in real time send their logs to collection servers located in dedicated security zones. Security logs are integrity-protected and are accessible only to administrators responsible for security. Logs are retained for three months by default for troubleshooting and security purposes, and for one year in the case of legal logs.

Unique time reference

Log timestamps, including those of security logs, are generated using a single time reference for all Cloud Avenue Dynamic components. The time service is provided by different NTP servers installed in dedicated security zones. The time reference itself is provided by a dedicated physical server (a root server with a GPS antenna) installed in Orange Business's internal service areas.

Customer consultation of its logs

In Cloud Avenue Dynamic, the customer can access the logs of their environment, including application and firewall logs. Access to logs is secure and restricted to each customer's environment.

6.2.5. Management of technical vulnerabilities

The main objective of vulnerability management is to maintain the security posture of Cloud Avenue Dynamic's infrastructure and services. Vulnerabilities are identified through security monitoring and vulnerability scans. They are then assessed, and the appropriate patches are deployed in production.
Security monitoring, tracking, patch deployment, and reporting are the responsibility of Orange Business Operations Security Managers and the BSO.

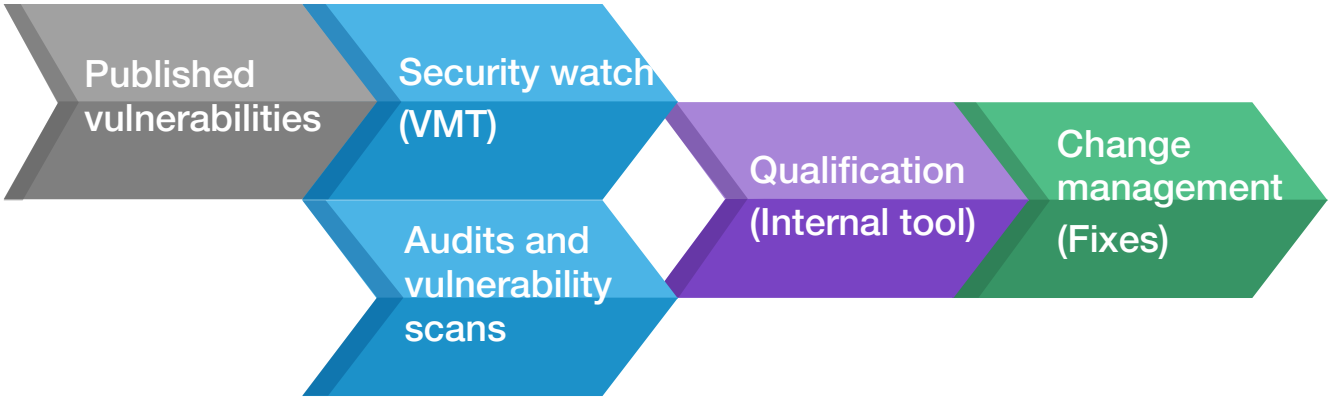

Figure 5: Vulnerability management

Security watch

All components are subject to a permanent security watch which aims to identify technical vulnerabilities that may impact on the security of Cloud Avenue Dynamic's infrastructures and services.

The security watch is fed by different channels:

- Security bulletins from product publishers (virtualization hypervisor, network and security equipment, OS...)
- Monitoring reports: VMT, CVE, NIST NVD, CERT-FR ...
- Customer feedback
- The feedback from our audits and vulnerability scans

Audits and vulnerability scans

Regular audits or continuous audits for the most critical infrastructures are carried out on our production platforms to assess the vulnerability status of those platforms and identify any vulnerabilities that may not have been detected by our monitoring infrastructure. To this end, Orange Business uses leading third-party market solutions for vulnerability scanning.

Independent penetration tests are systematically performed before each release of new Cloud Avenue Dynamic features. Major changes to existing features are also subject to such tests in order to maintain compliance with security requirements. When a critical vulnerability is identified, a follow-up investigation process is triggered after remediation to validate the effectiveness of the patches and verify the absence of regression. The BSO is responsible for tracking vulnerability remediation through to closure, based on the supporting evidence.

VMWare Tools update:

Under the **shared responsibility model,** updating VMware Tools is the sole responsibility of the customer. Any failure to apply patches or updates that may expose vulnerabilities **remains under her/his responsibility**. Accordingly, Orange Business cannot be held responsible for incidents, compromises or attacks exploiting such a vulnerability within the client's environments. In the event of an impact on Orange Business services or those of other clients attributable to this failure to update, **remediation measures** (e.g. VM isolation) and **financial penalties may be applied to the client, in accordance with the contractual conditions and SLAs in effect.**

Reporting

The BSO carries out monthly internal reporting of security monitoring and vulnerabilities addressed at this frequency. The latter is then presented during the COSEC and is not transmitted to clients for confidentiality reasons.

In the event of a critical vulnerability likely to have a significant impact on its customers, Orange Business communicates directly with its customers for information purposes.

6.3. Communications security

6.3.1. Security of Orange Cloud architecture

General principles

The architecture of the different areas of Cloud Avenue Dynamic is validated by a security manager under the governance of the Chief Security, Risk and Compliance Officer. The latter guarantees the consistency of the different architectures from a security point of view.

This approach based on a predefined model of architecture offers several advantages:c

- Simplification of the implementation of a new Cloud offer
- Homogeneity of practices and architectures between the different offers
- Mutualization of certain types of equipment
- Guarantee on the security of the offers: the models are validated then their implementation is controlled by the Security Cloud Competence Center. The security level of each new offer is also evaluated by audits and intrusion tests before any production rollout. The same applies to any major evolution. Internal intrusion audit and test results are not disclosed to customers for privacy reasons
- Simplification of maintenance in safety conditions

A systematic risk analysis for each new offer completes the security validation of the architecture. These 2 actions constitute the basis of the "Security by Design" approach, ensuring that security is considered in the design of offers.

Trust Areas and Security Zones

The architecture of Cloud Avenue Dynamic applies to the same model consisting in separating the areas of trust, notably on backend components (internal Orange) and frontend components bearing the Cloud services exposed to customers. The backend/frontend partitioning is physical, that means some servers are dedicated to the backend with others being dedicated to the frontend services.

Within each trust area, security zones ensure logical partitioning by implementing certain features such as:

- Virtualization (virtual machines, virtual firewalls, virtual load-balancers, virtual routers/VRF)
- VLANs (802.1Q)
- VPN virtual networks (IPSec, SSL)
- Virtual storage (virtual disks)

This logical separation notably guarantees the isolation of different client environments.

Communications between the different security zones are systematically controlled. The local configuration of the different components is also carried out in such a way as to reinforce partitioning and safety.

Orange Business Infrastructure

Infrastructure servers are grouped into security zones according to their function (such as administration servers or frontend servers used by customers), their nature (such as databases or web servers), and their level of exposure (for example, whether or not they are accessible to customers). As a result, dedicated security zones are assigned to Orange Business operating tools.
All servers have one interface dedicated to data flows and another technical interface dedicated to service flows, particularly for administration.
All cloud infrastructure components (servers, firewalls, routers, storage arrays, etc.) are configured in accordance with secure configuration guidelines established by the various engineering teams, with support from security experts within the Orange Business group.

Customer environments

The isolation between client environments is based on the virtualization functions described previously. Within Cloud Avenue Dynamic, the client has the possibility to manage security functions (including virtual firewall). The functions provided to customers vary depending on the options selected.

All details regarding client environments, contractual documents or platform certificates are listed following here.

6.3.2. Security exchange

Security of Orange internal flows

The following means are put in place to secure internal Orange exchanges:

- Networks: The interconnection networks between the Cloud platforms and the operating platforms are protected by one or more of the following solutions:
  - MPLS VPNs
  - Encrypted tunnels (IPSec, TLS)
  - Dedicated fiber networks
- Messaging: At the behest of clients, exchanges of sensitive data carried out by email between clients and Orange Business can be encrypted by a third-party tool agreed uponwith the client (e.g. Orange recommends zed).
- Administration flows: The administration flows are protected according to our state of the art SSL/TLS type connections (SSH, HTTPS).

Exchanges between the different security zones are systematically controlled by firewalls applying the basic principle "everything that is not explicitly allowed is prohibited".

Security of customer flows

Customers connect to Cloud Avenue Dynamic environments for administration or service access purposes. Client administration flows are systematically secured by protocols ensuring authentication, confidentiality and integrity (TLS, AES256...). Access methods will vary according to the options selected by the client.

The exchanges are secured with SSL/TLS connections that respect continual best in class state of the art solutions.

6.3.3. Protection against denial of service and intrusion

Orange Business' are hardened in such a way as to protect its customers against 'denial of service' attacks:

- **Anti-DDoS probes deployed at the heart of the Orange Group network**
  Cloud Avenue Dynamic benefits from the advanced "CleanPipe" protection system against large-scale denial-of-service attacks originating from the Internet. This system is activated by Orange's Security Operations Center (SOC) based on probes deployed at the core of the Orange Group's operator network.

- **Firewalls located at the entrance of the Cloud Orange platforms**
  The platform input traffic is supervised by firewalls that filter certain packets deemed suspicious by simple protocol analysis.

6.4. Acquisition, development and maintenance of information systems

6.4.1. Risk analysis

EBIOS RM risk analysis forms the foundation of Global Delivery & Operations' security management system. The operating principles are detailed below :

- Annual risk analysis of the Information Security Management System (ISMS) : as part of ISO 27001 certifications, a global risk analysis of the main services, processes, and tools of Global Platforms and Services is carried out, together with a risk treatment plan validated by the General Manager of Orange Business' Global Platforms and Services.
- High-Level Risk Analysis (HLRA) before each new service or solution rollout: this analysis makes it possible to assess the main risks (including personal data risks) and guides project teams towards secure solutions at an early stage.
- Security Risk Analysis: depending on the results of the HLRA, a full security risk analysis may be conducted. This analysis identifies risks related to the architecture, the operating model, and the organization.
- Risk analysis in the context of due diligence : this consists of verifying the security of a solution provider or subcontractor, including in the case of a company acquisition.

Risk analyses systematically result in recommendations for security measures to be implemented in order to mitigate the identified risks. These documents are not shared with clients for confidentiality reasons.

6.4.2. Development and Integration Best Practices

Cloud Avenue Dynamic systematically applies the security process from design to every new component and major evolution.

Development Best Practices

Specific developments carried out by Orange Business or by a subcontractor comply with the Orange internal best practice guidelines for secure development.

Best practices for integration / reinforcement of configuration security

The systems and software under the responsibility of Orange Business are configured with an enhanced level of security through the application of a "hardening guide". For example for VMware vSphere environments, Orange Business relies on the hardening security guides provided by VMware (https://www.vmware.com/security/hardening-guides.html).

Safety certification of critical components

The Cloud Security Competence Center of Orange Business ensures that critical components have recognized security certifications on an appropriate scope before being integrated into our Cloud offerings. Thus, the Security Cloud Competence Center generally relies on "Common Criteria" certifications (ISO 15408) and checks their relevance by controlling the following parameters:

- Level of assurance: EAL4 desired at a minimum.
- Security target covering sufficiently broad functional areas: cryptographic support, identification and authentication, sealing of virtual machines...

For example, the following critical components are certified as common criteria:

- VMWare: https://www.vmware.com/fr/security/certifications/common-criteria.html
- Juniper Firewall: EAL4.

6.4.3. Safety validations

Security validation of components

The most critical components of the Cloud Avenue Dynamic platform are subject to security testing (configuration and/or code reviews and/or penetration tests) to validate their level of security.
For example, the administration portals have already undergone several penetration tests and configuration and/or code reviews.
All templates (OS or application templates) provided by Orange Business are also subject to validation and are regularly tested and updated to take into account the latest vulnerabilities and available patches.

Non-production platform

Development, qualification, and preproduction platforms are available, notably to validate the security of changes and to conduct comprehensive penetration tests.
In the event of the deployment of patches or new services, these follow the security-by-design

process and are tested on these non-production platforms to validate their proper functioning and the absence of regression.

Lack of client data on non-production platforms

No customer data is present on non-production platforms, which are completely isolated.

6.5. Subcontractor Management

6.5.1. Contractual Subcontractor security

As part of the supplier onboarding process, Orange Business assesses the security management practices of its main suppliers, including the provision of a security assurance plan detailing the measures implemented by subcontractors to ensure the security of the services provided to Orange Business.
Approval by the internal security teams is one of the prerequisites for SEO.
Our service providers and suppliers are contractually bound to preserve the confidentiality and integrity of any data to which they may have access during the performance of their services and/or for the duration of the contract.
Subcontractors integrated into Orange Business internal teams use the same tools and processes as Orange Business staff and therefore, by default, comply with the best practices described in this document, including awareness, physical access control, and logical access control.

6.5.2. Monitoring the security of the services provided by our subcontractors

Orange Business provides for the possibility of auditing its subcontractors to verify compliance with the security commitments provided for in the contracts. These audits lead to security action plans that improve the level of security for subcontractors.

6.6. Security incident management

The security incident management policy is described in the Orange Business security policy.

Preparation of operational teams

This phase aims to prepare each stakeholder for incident handling through operational excellence measures, such as awareness initiatives and regular training on managing different types of incidents, as well as through rapid access to up-to-date documentation (asset inventories, network diagrams, technical documentation, logs, etc.).
During this preparation phase, operational staff are made aware of how to identify potential security incidents. The principle is that, when an operational incident is identified, the person in charge should be able to reasonably determine whether the incident may lead to a security

issue—typically if a protection system fails—or whether its origin may be security-related (malware, botnets, intrusion attempts, denial-of-service attacks, etc.).

Detection of security incidents

The detection means implemented to detect a security incident are:

- Standard supervision tools (Patrol, Zabbix) or security-specific ones (SIEM[6], anti-DDOS probes)
- Staff in charge of monitoring the logs (IDS, log FW, system logs, application logs...).
- Watch cell
- Security team (e.g. Cloud Security Competence Center)
- Alerts raised by the client

This monitoring is carried out on the components under the direct responsibility of Orange Business (portals, hypervisors, and customer environments whose security is managed by Orange Business, etc.).

Recording and qualification of security incidents

Orange Business has a security incident management tool.

Alerts are entered into the tool in the form of an incident ticket by two types of actors:

- The technical actors in charge of operations /service supervision
- Support center personnel, alerted by a call or an email from the client.

Alerts are qualified according to their nature and severity.

Nature of the Incident - The Incident Management Tool identifies four categories of incidents:

- Intrusion
- Dysfunction
- Vulnerability
- Legal (regulatory incident involving specific actors)

Severity of the incident - The table below summarizes the levels of severity of incidents as well as the actions to be taken:

Level	Description
1	**Critical** Complete loss of services for several users, or an incident having a critical impact on the client's activities. Requires immediate consideration and the urgent provision of dedicated resources until the incident is resolved.
2	**Major** Degraded services. Users may access the services but experience significant difficulties or delays. Requires immediate consideration and the provision of resources for rapid resolution of the incident.

[6] SIEM: Security Information Event Management, a tool for correlating logs linking different events to the same cause.

3	**Minor** Services provided with minor delays or difficulties. The company's activity is not significantly impeded. Requires scheduled maintenance to avoid significant service degradation.

Response security incidents

The following measures can be taken:

- Emergency measures (quarantine, ...)
- Activation of the crisis unit
- Communications to customers, partners, operators
- Applying patches
- Restoring systems
- …

Review and post-incident actions

Once the security incident has been handled, the Cloud Security Competence Center analyzes the nature of the incident and the quality of the response provided by Orange Business. If necessary, the Cloud Security Competence Center updates the security incident management procedures as part of a continuous improvement process.

Communication with customers

For incidents that may have had an impact on the security of Orange Business customers, communication is provided to customers in accordance with the terms set out in the contract. For customers who have opted for a dedicated Business Security Officer, communication is made directly with the customer's CISO.

6.7. Security of business continuity management

Availability rates are specified in the service descriptions.

All our cloud offers rely on fully redundant infrastructure distributed across several sites (or, by temporary exception, across several computer rooms), with high-availability mechanisms designed to make local failures transparent across the network (Internet access, VPN access, firewalls), administration portals, virtualization, storage, and other components.

All backups (including configuration backups and customer backups) are replicated to remote sites to ensure data availability in the event of a major disaster affecting the production sites.

Cloud Avenue Dynamic offers are operated from several operating platforms. As a result, in the event of the total unavailability of one operating site, continuity of administration for Cloud Avenue Dynamic offers is ensured.

Business continuity is regularly tested through simulations.

Reversibility clauses are included in the contracts for Cloud Avenue Dynamic offers. In the event of service termination, except in cases of termination for breach of contract, the customer may request that Orange Business initiate reversibility. Orange Business will then implement the means reasonably necessary to ensure service continuity, so that, at the end

of the reversibility period, the customer has the capacity to continue meeting their needs (see the contract for further details).

6.8. Compliance

6.8.1. Compliance with legal and contractual requirements

As part of the risk analysis approach applied to any Orange Business project, a review of legal and contractual obligations is carried out and an action plan is proposed. The corresponding deliverable is called the LOA (Legal Obligation Assessment). The topics covered include:

- Compliance with contractual clauses (licenses, industrial property, commitments specified in the service description, etc.).
- Compliance with specific regulations from the Orange Business field of activity (LCEN[7] and CPCE[8])
- Keeping a register of personal data processing operations, in accordance with the General Data Protection Regulation (GDPR). Orange Business Services has appointed a DPO (Data Protection Officer) who is responsible for maintaining the register. The DPO is a specialist contact for personal data protection, both for the person responsible for processing such data and in the latter's relations with the CNIL (National Commission for Informatics and Freedoms)., independent administrative authority responsible for ensuring compliance with the GDPR. The DPO thus occupies a central place in the secure development of new information and communication technologies and ensures, within the company, the dissemination of computer culture and freedoms and the control of risks on personal data.

Within the same risk analysis framework, a review of personal data matters is also proposed. The corresponding deliverable is called the PRA (Privacy Risk Assessment).

6.8.2. Control of compliance with security policies

The Cloud Security Competence Center is responsible for monitoring the application of the Security Policy for each cloud offer. It therefore performs continuous oversight and conducts periodic organizational and technical audits. audits.
In addition, Orange Business is subject to regular audits (such as AFNOR and ISAE 3402 audits) carried out by external bodies and resulting in assessments of its security level

[7] LCEN: Law for Confidence in the Digital Economy
[8] CPCE: Postal and Electronic Communications Code

6.8.3. Certifications related to safety

Orange Business has the following certifications adhering to the scope of Cloud offers:

- ISAE 3402 for datacenters
  - Orange's datacenters are certified ISAE 3402 Type II (ex SAS70).
- ISO 27001 security certification
  - Orange Business has ISO 27001 security certification for the scope of 'implementation, provision and support of facilities management services and communications solutions' for its sites in Cesson-Sévigné France, Cairo Egypt, Mauritius, Bangalore India and Warsaw Poland[9].
- SOC1 and SOC2 Certification
- ISO 27017 Certification
- ISO 27018 Certification
- ISO 9001 certification
- ISO 14001 certification
- ISO 20000-1 Certification
- CISPE (Cloud Infrastructure Service Providers Europe – Data Protection) certification
- Certification Common Criteria EAL 2+ (ISO 15408) on the security of the international network IP-VPN in 2008
- Common Criteria Certification (ISO 15408) of security equipment and virtualization equipment used on our offers:
  - VMWare: https://www.vmware.com/security/certifications/common-criteria.html
  - Juniper Firewall: EAL4.

[9] Associated certificate: https://certificats-attestations.afnor.org/certification=335181233155