OVHcloud

System and Organization Controls (SOC 2®) 2 Type 2 Report

Report on Management's Description of OVHCloud's Public Cloud System and on the suitability of the design and operating effectiveness of its controls relevant to Security, Confidentiality, Availability, Privacy, CCM and C5

For the Period from January 1, 2024 to December 31, 2024

Table of content

-Intentionally left blank-

SECTION I
Independent Service Auditor's Report

KPMG S.A.
Tour EQHO
2 Avenue Gambetta
CS 60055
92066 Paris La Défense Cedex

To the Board of Directors of

OVH Groupe S.A., Roubaix, France

-hereinafter also referred to as "OVHcloud" or "the Company"-

Scope

We have examined management of OVH Groupe S.A. ("OVHcloud")'s accompanying description of its system titled "Management of OVHcloud's Description of its Public Cloud System" throughout the period January 1, 2024 to December 31, 2024 (the Description), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria* (the Description Criteria), and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period January 1, 2024 to December 31, 2024 to provide reasonable assurance that OVH Groupe S.A.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality and Privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*. We have also examined the suitability of the design and operating effectiveness of controls related to security at a cloud service provider to provide reasonable assurance that the service organization's business objectives, security requirements and compliance obligations were achieved based on the control specifications set forth in the Cloud Security Alliance's ("CSA") Cloud Controls Matrix ("CCM") Version 3.0.1 ("CCM criteria") and the objectives set forth in the Bundesamt für Sicherheit in der Informationstechnik ("BSI") Cloud Computing Compliance Criteria Catalogue ("C5").

The information included in Section V, "Other Information Provided by Management of OVH Groupe S.A.", is presented by management of OVH Groupe S.A. to provide additional information and is not a part of the Description. Information about OVH Groupe S.A.'s other information has not been subjected to the procedures applied in the examination of the Description, the suitability of the design of controls, and the operating effectiveness of the controls.

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at OVH Groupe S.A., to achieve OVH Groupe S.A.'s service commitments and system requirements based on the applicable trust services criteria and to achieve its business objectives, security requirements and compliance obligations based on the CSA CCM and BSI C5 Framework. The Description presents OVH Groupe S.A.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of OVH Groupe S.A.'s controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls

Service Organization's Responsibilities

OHV Groupe S.A. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that OVH Groupe S.A.'s service commitments and system requirements were achieved. Management of OVH Groupe S.A. has provided the accompanying assertion titled "Management of OVH Groupe S.A.'s Assertion" (the Assertion) about the Description and the suitability of design and operating effectiveness of controls stated therein. OVH Groupe S.A. is also responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion; providing the services covered by the Description; selecting the applicable trust services criteria and the CSA CCM and BSI C5 Frameworks and stating the related controls in the Description; and identifying the risks that threaten the achievement of OVH Groupe S.A.'s service commitments and system requirements.

Management of OVHGroupe S.A. is also responsible for selecting CSA CCM and BSI C5 as additional criteria, and for implementing and operating effective controls to meet the requirements set forth in the CSA CCM Version 3.0.1 control specifications and the objectives set forth in the BSI C5.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of the design and operating effectiveness of the controls stated in the Description based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and in accordance with International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board.[i] Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, the Description is presented in accordance with the Description Criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and the CSA CCM and BSI C5 Frameworks.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- obtaining an understanding of the system and the service organization's service commitments and system requirements and the service organization's business objectives, security requirements and compliance obligations
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria and achieve its business objectives, security requirements and compliance obligations based on the CSA CCM and BSI C5 Frameworks, if those controls operated effectively
- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria and achieved its business objectives, security requirements and compliance obligations based on the CSA CCM and BSI C5 Frameworks, and

- evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with the relevant ethical requirements in the United States of America relating to the examination engagement. We have complied with those requirements. We have also applied the statements on quality control standards established by the American Institute of Certified Public Accountants and accordingly maintain a comprehensive system of quality control. The firm also applies International Standard on Quality Management 1 which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that each individual report user may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria or that the service organization has achieved its business objectives, security requirements and compliance obligations based on the CSA CCM and BSI C5 Frameworks. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section IV.

Opinion

In our opinion, in all material respects,

- the Description presents OVH Groupe S.A.'s Public Cloud system that was designed and implemented throughout the period January 1, 2024 to December 31, 2024in accordance with the Description Criteria

- the controls stated in the Description were suitably designed throughout the period January 1, 2024 to December 31, 2024 to provide reasonable assurance that OVH Groupe S.A.'s service commitments and system requirements would be achieved based on the applicable trust services criteria and its business objectives, security requirements and compliance obligations would be achieved based on the CSA CCM and BSI C5 Frameworks, if the controls operated effectively throughout that period, and user entities applied the complementary controls assumed in the design of OVH Groupe S.A.'s controls throughout the period January 1, 2024 to December 31, 2024

- the controls stated in the Description operated effectively throughout the period January 1, 2024 to December 31, 2024to provide reasonable assurance that OVH Groupe S.A.'s service commitments and system requirements were achieved based on the applicable trust services criteria and its business objectives, security requirements and compliance obligations were achieved based on the CSA CCM and BSI C5 Frameworks, if complementary user entity controls, assumed in the design of OVH Groupe S.A.'s controls, operated effectively throughout the period January 1, 2024 to December 31, 2024.

Restricted Use

This report, including the description of tests of controls and results thereof in Section *IV*, is intended solely for the information and use of OVH Groupe S.A., user entities of OVH Groupe S.A.'s Public Cloud system during some or all of the period January 1, 2024 to December 31, 2024, business partners of OVH Groupe S.A. that were subject to risks arising from interactions with OVH Groupe S.A.'s Public Cloud system, and practitioners providing services to such user entities and business partners, who have sufficient knowledge and understanding of the following:

- the nature of the service provided by the service organization
- how the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- internal control and its limitations
- complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- user entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- the applicable trust services criteria
- the control specifications of the CSA CCM and BSI C5 Frameworks
- the risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.

Paris,

August 19, 2025

KPMG S.A.

Jacques Pierre
Partner, Audit

Fayçal El Belghami
Partner, IT

SECTION II Management of OVHcloud's Assertion

We have prepared the accompanying description of OVH Groupe S.A.'s system titled "Management of OVHcloud's Description of its Public Cloud System" throughout the period January 1, 2024 to December 31, 2024 (the Description), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria* (the Description Criteria). The Description is intended to provide report users with information about the Public Cloud system that may be useful when assessing the risks arising from interactions with OVH Groupe S.A.'s system, particularly information about system controls that OVH Groupe S.A. has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality and Privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*, and to provide reasonable assurance that its business objectives, security requirements and compliance obligations were achieved based on the control specifications set forth in the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) Version 3.0.1 and the objectives set forth in the Bundesamt für Sicherheit in der Informationstechnik (BSI) Cloud Computing Compliance Criteria Catalogue ("C5") relevant to the security of a system.

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at OVH Groupe S.A., to achieve OVH Groupe S.A.'s service commitments and system requirements based on the applicable trust services criteria and to achieve its business objectives, security requirements and compliance obligations based on the CSA CCM and BSI C5 Frameworks. The Description presents OVH Groupe S.A.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of OVH Groupe S.A.'s controls.

We confirm, to the best of our knowledge and belief, that:

a) The Description presents OVH Groupe S.A.'s Public Cloud system that was designed and implemented throughout the period January 1, 2024 to December 31, 2024, in accordance with the aforementioned Description Criteria.

b) The controls stated in the Description were suitably designed throughout the period January 1, 2024 to December 31, 2024 to provide reasonable assurance that OVH Groupe S.A.'s service commitments and system requirements would be achieved based on the applicable trust services criteria and its business objectives, security requirements and compliance obligations would be achieved based on the CSA CCM and BSI C5 Frameworks, if the controls operated effectively throughout that period, and user entities applied the complementary controls assumed in the design of OVH Groupe S.A.'s controls throughout the period January 1, 2024 to December 31, 2024.

c) The controls stated in the Description operated effectively throughout the period January 1, 2024 to December 31, 2024 to provide reasonable assurance that OVH Groupe S.A.'s service commitments and system requirements were achieved based on the applicable trust services criteria and its business objectives, security requirements and compliance obligations were achieved based on the CSA CCM and BSI C5 Frameworks, if complementary user entity controls, assumed in the design of OVH Groupe S.A.'s controls, operated effectively throughout the period January 1, 2024 to December 31, 2024.

OVH Groupe S.A

Mathieu Delobelle

Chief Information Officer

Signé par :
Mathieu Delobelle
FA645F25290F435...

August 19, 2025

SECTION III
Management of OVHcloud's Description of its Public Cloud System

1. Company Overview and Services Provided

OVH Groupe S.A ("OVHcloud") was founded in 1999 as an internet hosting company in France. Over the last 20 years, OVHcloud has developed its infrastructure and expanded its presence in Europe, North America and Asia, diversifying its cloud offerings and expanding its activities globally.

OVHcloud is a cloud provider supported by a vertically integrated production model that provides enterprises with a comprehensive suite of solutions for multi-cloud and hybrid cloud strategies distributed into four core cloud categories:

- **Bare Metal Cloud:** with dedicated physical servers to customers;
- **Hosted Private Cloud:** in a fully dedicated environment to its business customers;
- **Public Cloud:** based on open-source technologies such as OpenStack and Kubernetes;
- **Web Cloud:** with website hosting and domain registration, telecommunications, and internet access.

1.1. A Vertically Integrated Model, Based on Exclusive Technology

1.1.1.A Server and Data Center Integrated Model

OVHcloud has developed an integrated model to fully manage in-house each step of both server and data center lifecycles limiting the dependency on subservice organizations.

OVHcloud's vertically integrated supply chain includes server manufacturing, data center operations, network provisioning and IT infrastructure management. By designing and assembling all its servers in-house, OVHcloud fully owns server design, production and management. OVHcloud has built its strong vertical integration through proprietary technology and in-house operations in various geographies.

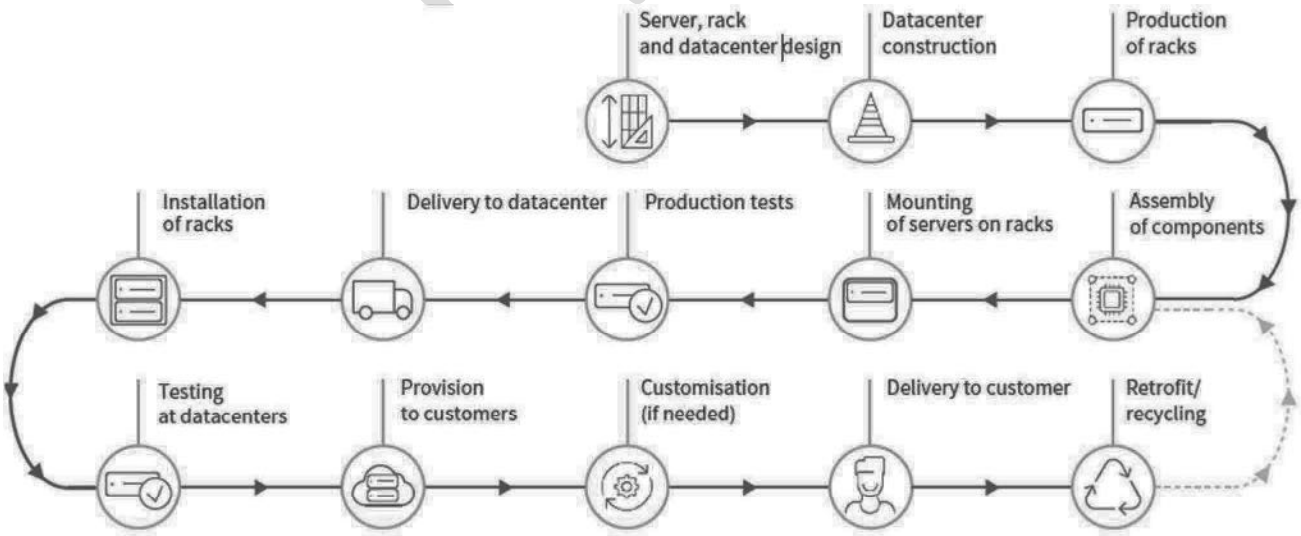


Figure 1: Integrated model for server and data center lifecycle

OVHcloud has two dedicated production sites—in France and in Canada—for assembling different
hardware components into servers. Once the various components have been assembled, they are
transported to the data center and customized as necessary prior to delivery to the customer.

OVHcloud reduces the risk of supply chain disruption by manufacturing its servers in-house and removing dependencies on a third-party manufacturer.

The capacity to manufacture servers proved to be essential in allowing OVHcloud to respond rapidly to restore service in case of incidents.

1.1.2.A Data Center Proprietary Water-Cooling Technology

OVHcloud has developed and used over 20 years a proprietary water-cooling technology within its data centers. OVHcloud's water cooling technology combines water-cooled servers with air-cooled data centers, thereby removing the need for air conditioning. It uses direct water cooling to remove the heat from CPUs, and air—which is then cooled inside the rack using water through a heat exchanger—to remove the heat from other components. The heated water is then cooled using dry cooling towers. In addition to being highly energy and water efficient, OVHcloud's water cooling technology also has relatively low maintenance costs.

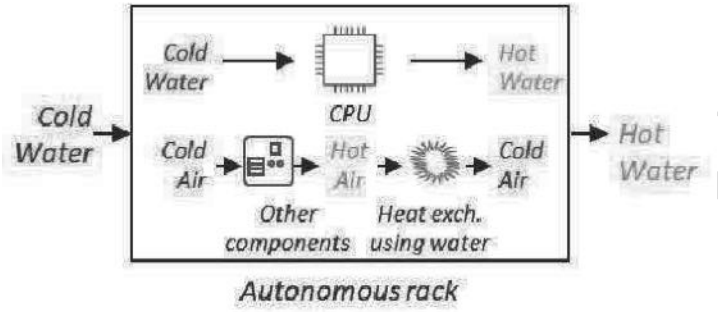


Figure 2: OVHcloud proprietary water-cooling technology principles

In addition, OVHcloud developed its own concept where air-conditioning units were replaced by a natural ventilation system that, thanks to hot and cold airflow, ensured that temperatures were regulated. This concept complemented water-cooling to participate in energy saving.

1.2. OVHcloud Universe of Cloud Offerings

Cloud computing means providing users with storage, computing and network resources, over the internet, on demand. Cloud resources are in data centers that house servers and equipment used to process, store and transmit data. User entities of cloud computing services can access stored data and instruct processing units to perform computing functions automatically, without the need for human interaction, minimizing the computing and storage capacities needed on their devices (such as personal computers, tablets and mobile phones). Wherever they are located, so long as they have an internet connection, user entities can access IT services through the cloud.

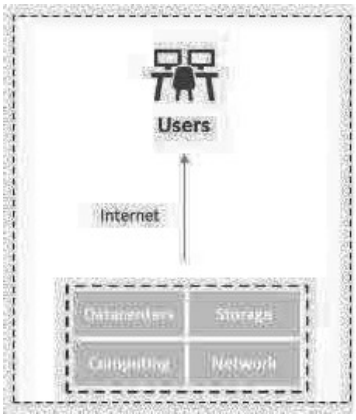


Figure 3: Basic structure of a cloud computing system

Servers maintained in data centers can be used for multiple functions, each of which is accessed through a "virtual machine" created on the server. The virtual machines are operated and separated from one another through a software platform known as a "virtualization stack." Each virtual machine can have its own operating system that permits user entities to develop and run applications. Through a function known as a "hypervisor," the server's capacity is allocated to the virtual machines in accordance with the demands of user entities. More recently, software applications have been written to be bundled in "containers" that run directly on the operating system of the server itself, coordinated through platforms known as "orchestration" systems, which generally take less space and can provide better performance than hypervisor-based virtualization stacks.

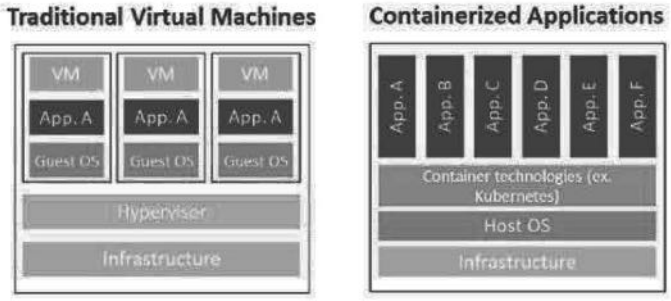


Figure 4: Traditional virtual machine structure and containerized application structure

The ability to create multiple virtual machines on each server or to deploy container-based systems allows a cloud service organization to allocate its capacity among multiple user groups or user entities in a secure manner. Service organizations can dedicate a server to a single user entity (a "private cloud" system), allocating the server's capacity among user groups authorized by the user entity. Alternatively, a server can be shared among multiple user entities (a "public cloud" system). Private cloud user entities generally pay monthly charges for dedicated capacity, whether or not they use that capacity. Public cloud user entities generally pay for the capacity they use.

To optimize the cost of cloud services, many businesses are deploying "hybrid cloud" strategies, in which they combine on-premises or outsourced private cloud capacity for their most sensitive functions and data, with public cloud capacity for their less sensitive needs. User entities are also deploying "multi-cloud" strategies, purchasing cloud services from several user organizations.

The following table summarizes the key features of OVHcloud's main private cloud and public cloud offerings:

	Private Cloud		Public Cloud	
	Bare Metal Cloud	**Hosted Private Cloud**	**Virtual Private Servers**	**Shared Public Cloud**
Hardware	Dedicated to user entity		Shared	
Operating system	Selected and managed by user entity	Selected and managed by OVHcloud		
Virtualization Stack	Selected and managed by client (if any)	VMware Hosted and managed by OVHcloud		Hosted and managed by OVHcloud via OpenStack

Cloud computing encompasses a range of services that include providing access to infrastructure
(Infrastructure as a Service or "IaaS"), selecting and operating platforms such as operating systems,
virtualization stacks and security systems (Platform as a Service or "PaaS"), and offering applications
that are developed and can function on cloud platforms (Software as a Service or "SaaS").

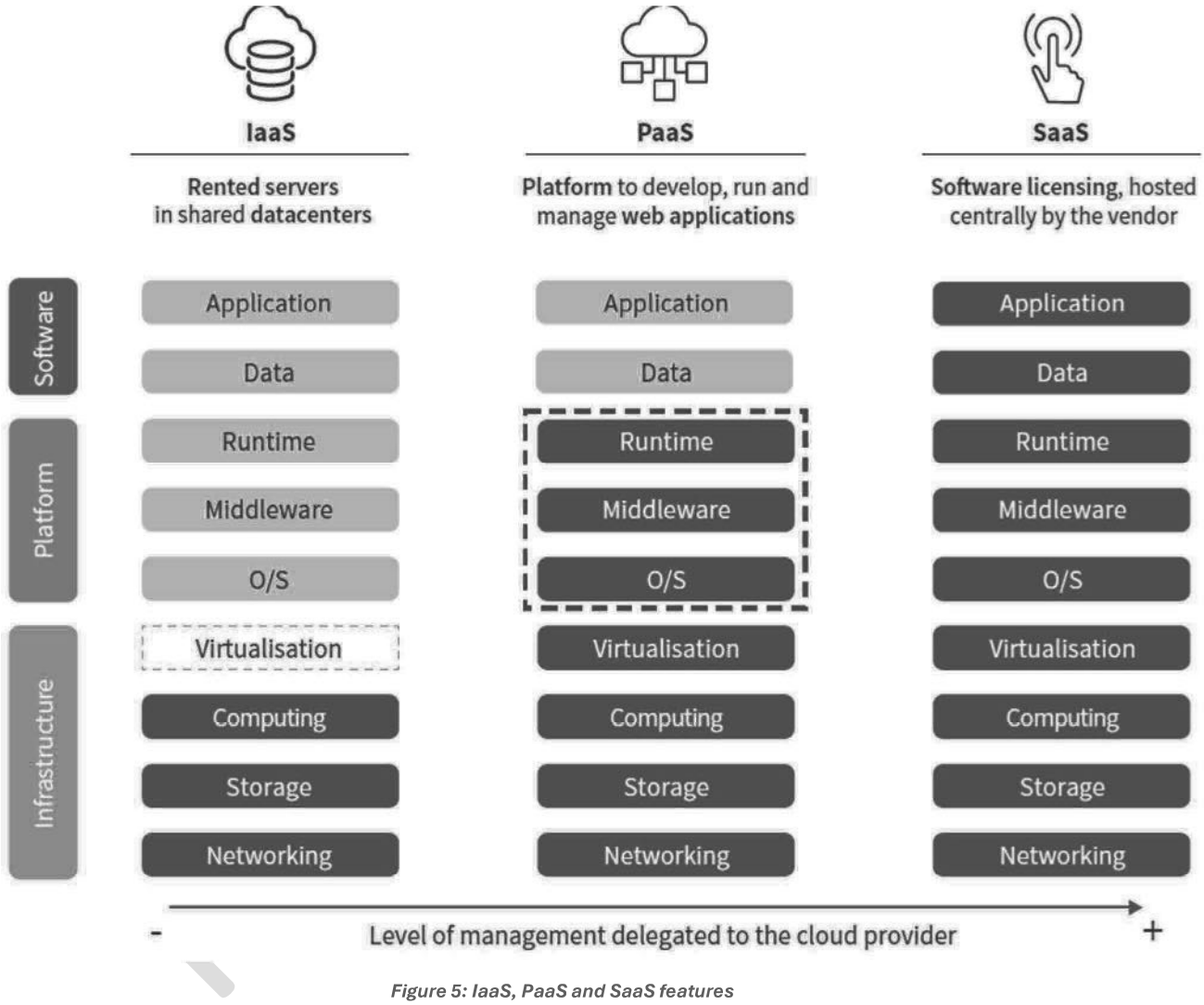


Figure 5: IaaS, PaaS and SaaS features

The cloud solutions market also includes the web cloud market largely consists of web and domain hosting, including renting servers for websites, selling secondary services (such as software packages) and domain name registration, renewal and transfer services.

1.2.1. Bare Metal Cloud

OVHcloud's Bare Metal Cloud service provides dedicated physical servers to user entities, which have full control over the server, including the choice of operating system, which allows them to

have an experience similar to what they would have with on-premises solutions managed by their internal IT staff, while taking advantage of the benefits offered by outsourcing.

Bare Metal Cloud offers high performance and high scalability with the best price/quality ratio in just a few minutes, for development, production and backup. Highly reliable, customizable and scalable, Bare Metal Cloud provides user entities with instant provisioning and fully automated access to dedicated servers on which the user entity operates and manages all software layers, including the operating system.

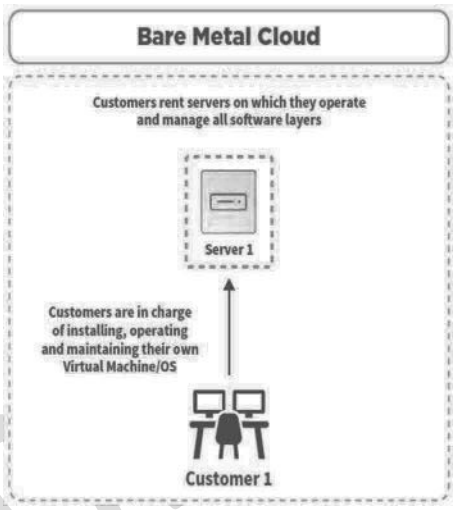


Figure 6: Bare Metal Cloud service

Bare Metal cloud services provide user entities with high-level computing power and strict Service Level Agreements, in a secure environment appropriate for data-sensitive applications. The server can be customized to meet user entity requirements and can be operated without a need to allocate the server's capacity to virtual machines through a hypervisor, which allows the customer to use the server's full capacity. Any unused capacity can be deployed within minutes, although the total capacity is limited by that of the dedicated server. Bare Metal user entities are typically responsible for making their own data backup arrangements, although they can also choose from several backup options offered by OVHcloud (with backed-up data stored within the same data center or at a different location). Bare Metal cloud user entities may choose various additional service options such as specific performance levels, server customization or data backup.

Bare Metal Cloud services provide security, performance, customization and cost effectiveness, and are typically used for data intensive operations such as media encoding (like 3D animation), media streaming, complex data-computing (such as analyzing oil and gas field seismic data), low latency operations such as high frequency trading, media streaming, online gaming and online advertising, critical corporate applications requiring high-security operations such as ERP and CRM system operations, specialized applications such as customized Internet-of-Things, and applications designed to meet strict regulatory compliance requirements in highly regulated sectors.

1.2.2. Hosted Private Cloud

OVHcloud offers hosted private cloud services in a fully dedicated environment providing dedicated servers and platforms fully managed by OVHcloud, including the operating system and the virtualization stack (using VMware technology).

OVHcloud's hosted private cloud services provide user entities with private access to servers that can be customized to meet the user entities' specific requirements. The server provides high performance, although slightly below that of high-end Bare Metal cloud service, because the hypervisor uses some of the server's capacity. It meets the needs of user entities seeking isolation and security, scalable resources (within the limits of the server's capacity) and resilience.

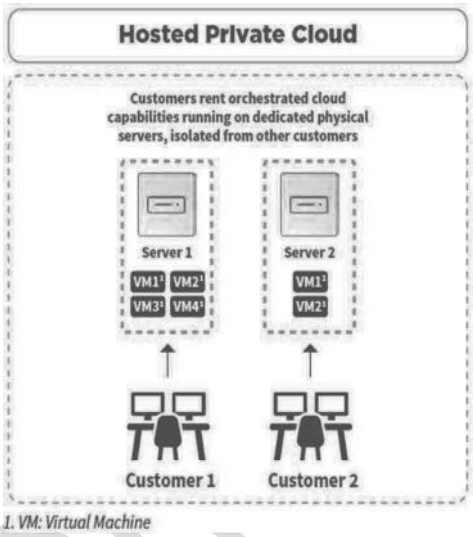


Figure 7: Hosted Private Cloud service

The main usages for hosted private cloud services include deployment in hybrid cloud strategies, media encoding, big data analytics and disaster recovery, as well as the storage and processing of sensitive data in key sectors such as healthcare, finance and the public sector.

1.2.3. Public Cloud

OVHcloud offers public cloud solutions based on open-source technologies such as OpenStack (a platform that controls diverse, multi-vendor pools of processing, storage, and networking resources) and Kubernetes (an industry standard container orchestration platform). The use of these standard platforms provides user entities with easy data transfer capability and access to source code, facilitating reversibility and eliminating "vendor lock-in". It is particularly adapted for user entities seeking to deploy hybrid cloud strategies.

Public cloud solutions provide users with virtually unlimited computing capacity, with the only constraint being the demands of other users and the total installed capacity of the cloud provider.

Capacity can generally be accessed automatically in seconds. Because public cloud service is based on shared servers offering user entities the highest degree of scalability and continuity, customization options are limited. OVHcloud provides high SLAs given the flexibility of the hardware architecture.

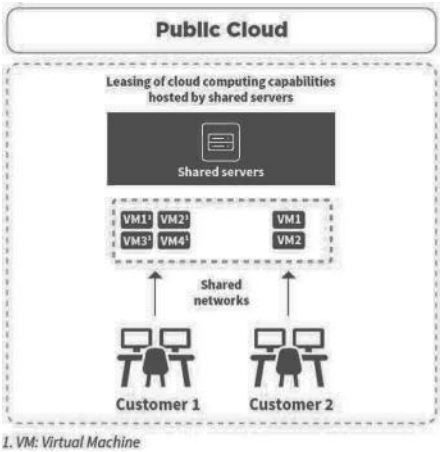


Figure 8: Public Cloud service

Public cloud offering provides three core cloud computing services: computer performance, storage and network capabilities. It also provides five additional, high-level services: orchestration and containerization, including tools to manage processes and software stacks; data analytics, including data collection and processing services; artificial intelligence, including automated deployment, launch, training and evaluation of machine learning models; management interfaces; and project management solutions. User entities of OVHcloud public cloud solutions can choose a virtual private server option, providing computing

capabilities located on shared servers, but with “virtual machines” isolated using virtual private networks.

The virtual private server option is particularly adapted for user entities seeking tailored resources, particularly for short-duration operations with volatile workloads and server demand across multiple access locations, and a high degree of resilience. Virtual private server solutions are used primarily for applications testing and other one-time projects, the management of short-duration peak loads and backup functions. OVHcloud also offers fully scalable public cloud services on virtual machines that are housed on share servers but are not isolated through virtual private networks.
This service is used for applications with high demand bursts (such as e-commerce websites) and services that use large volumes of data, such as video and music streaming. Public cloud services can also be used by user entities for workloads that are not sufficiently mission-critical to warrant the use of private cloud resources.

1.2.4. Platform-as-a-Service Solutions

OVHcloud provides PaaS offers on its private cloud and public cloud IaaS products, primarily in the following areas:

- **Artificial Intelligence and Analytics**: Artificial intelligence and analytics solutions include tools and services supporting data analysis and data presentation, such as the management of end user queries, data labelling, and image and text presentation. OVHcloud is active in providing high performance computing solutions for artificial intelligence and machine learning and intends to pursue its development in this area.
- **Data Management Software**: Data management software allows users such as database managers and developers to manage databases to allow for queries and random updates, and it represents the largest single segment of the PaaS market. It includes programs that execute queries on data and provide visual representation of the data in formats such as spreadsheets, enabling users to build applications faster and automate database management.
- **Application Platforms**: Application platforms are back-end server software solutions providing developers with a cohesive application execution environment (e.g. application execution, access to data, authentication coordination, session management). OVHcloud integrates key application platforms from VMWare.
- **Web cloud Platforms**: beyond its web cloud offer, OVHcloud provides an end-to-end web platform allowing developers to build, run and scale applications.
- **High Performance Storage**: including Block Storage, Object Storage and Cold Archive.

— **Security and Encryption**: including identity access management and encryption solutions, including end-to-end encryption.

1.2.5.Web Cloud

OVHcloud has offered web cloud services since its founding in 1999. OVHcloud provides user entities with web cloud services, including website hosting and domain registration, telecommunications and internet access, as well as a "marketplace" for third-party software solutions to help user entities empowering their digital journey.

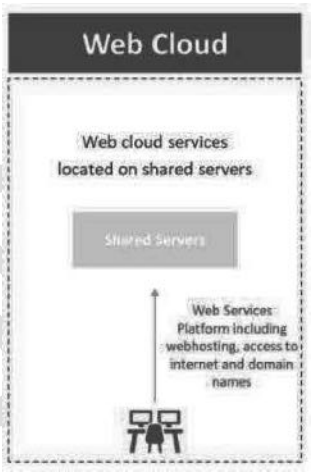


Figure 9: Web Cloud service

OVHcloud offers three principal solutions to web cloud user entities:

— **Web hosting and domain registration**: This includes the rental of capacity on web servers, allowing user entities to connect their websites to the internet, as well as domain name registration, renewal and transfers together with email addresses and storage options. OVHcloud offers web hosting customers additional services, such as Secure Socket Layer (SSL) certificates, which allow secure connections from a web server to a browser.

— **Telephony and Network**: User entities may purchase Voice over IP systems providing phone numbers and unlimited calls to fixed lines (and, in the high-end package, mobile lines), and enabling usages such as telephone switchboards and interactive voice response systems. OVHcloud also provides large-volume telephony options that are capable of handling video and other media. OVHcloud also offers customers internet access through ADSL and fiber networks, with basic and professional packages.

— **Software Marketplace**: Web cloud user entities have access to OVHcloud's software marketplace, providing more than 250 fully digital SaaS and PaaS solutions with 6 categories from third-party vendors that can run on OVH's infrastructure, in areas such as collaboration, emailing and social networking, managed services (such as outsourcing), corporate tools (business intelligence, CRM and ERP), coding and applications development, and solutions for specific industries such as e-learning, healthcare, legal and real estate.

1.3. Scope Covered in this Report

Our service "Public Cloud Infrastructure" provides a wide variety of cloud services integrated with each other, forming a coherent offer of infrastructure as a service. The core of the service is built with Openstack and consists in compute, block storage and object storage. Specifically, it provides the following services and features:

- Public Cloud **Compute** is a platform that uses pooled virtual resources to build and manage public clouds. The tools that comprise the PCI platform, called "projects," handle the core cloud-computing services of computer, networking, storage, identity, and image services. PCI Compute service provides three kind of instances that aim at different goals:
    - balanced instances: Catalogue of top-range instances, with fully guaranteed resources. General Purpose instances have a balanced distribution of resources and suit most uses. CPU instances are particularly powerful in terms of

computing capacity. As for RAM instances, they offer a very high volume of memory.
    - IOPS instances: IOPS instances deliver the fastest disk transactions in the Public Cloud range. They offer direct access to NVMe drives, each of which deliver at least 400,000 read/write operations per second. These cloud solutions are designed to host database (DB) servers and big data applications.
    - GPU instances: GPU instances integrate NVIDIA Tesla V100S graphic processors to meet the requirements of massively parallel processing. These cloud servers are adapted to the needs of machine learning and deep learning.
- **Object Storage** (Swift / OpenIO) offers a high-performance, scalable and secure storage space. It allows the user to upload static files (videos, images, web files) to an unlimited space and use them from an application or make them accessible on the web via a S3 API. This storage space can be scaled up as the project grows, with no need to plan for it in advance. It can meet the requirements of big data, artificial intelligence (AI) and document catalogues, or simply help to get the most out of csutomers' data. Object Storage also includes **Cold Archive** service, which provides long-term, cost-efficient storage. Data is stored on an S3 buffer before being sent to magnetic tapes in smaller scale datacenters, dedicated to this service.
- **Block storage** Ceph-as-a-Service (CaaS) is a framework that can deploy and maintain Ceph based clusters. Ceph is a unified, distributed storage system designed for excellent performance, reliability and scalability and Ceph-as-a-Service is a system for complete life-cycle management of Ceph clusters. When persistent storage requirements increase, the user instantly meets growing demands by hot-adding extra disks to increase the instance's capacity. These volumes are securely hosted in OVH's clusters and can be used to meet the requirements of applications that handle large volumes of data.

The billing is based on the volume and typology of services consumed; a key component is pay-as-you-go, meaning that only resources consumed are billed, and hourly billing is available. See https://www.ovhcloud.com/fr/public-cloud/prices/ for details. Entry-level offers are affordable; therefore Public Cloud clients range from small entreprise to large accounts.

We also provide Platform-as-a-Service (PaaS) products that are built on top of Public Cloud Infrastructure products. These products are hosted on Public cloud instances and are preconfigured to provide specific services

Kubernetes products include two individual products:

- **Managed Kubernetes** (K8s) which is the industry-standard container orchestrator, used by companies of all sizes. It facilitates the deployment, resiliency and scalability of the customer's applications, even in hybrid or multi-cloud infrastructures. The "Managed Kubernetes" solution is powered by OVH's Public Cloud instances. OVH deploys, hosts and maintains all the components needed for Kubernetes to work, including updates linked to bugs and security patches. OVH also maintains the necessary components on the customer's nodes. Kubernetes launches containers and configures the Load Balancer for the customers, and they can instantly add new computing nodes. The customers can also define the health conditions for each service, after which Kubernetes will relaunch any pods and containers that do not meet these criteria. The customers' nodes can be monitored, and their services benefit from the high availability of OVH Infrastructure-as-a-Service (IaaS) solutions.

- **Private registry**, which enables customers to host helm charts and docker images. The ISMS covers the full set of these products / services.

Data products include two individual products:

- **Cloud Databases**: offers a fully managed database service. The customer is billed hourly according to the resources he ordered.
- **AI Products**: provide a fast and easy way to get through a Artificial Intelligence pipeline. This offer is split into three products AI Notebook, AI Training and AI Deploy. The computer engine is based on Kubernetes. The customer is billed by the minute and only for what resources he consumes. AI Products enables clients to leverage GPU hardware simply and without compatibility headaches.

Several services and features are included in the Openstack framework and thus available in all Public Cloud projects by default.

- Identity service (Keystone)
- Managed private registry and public catalog
- WebUI service
- Network connectivity (Neutron)
- Metering service (Ceilometer)
- Roles and Rights Management
- Workflow management (Mistral)

Public Cloud scope	Product name	ovhcloud.com page	Commercial offers
Public cloud Compute	Public Cloud Instance	https://www.ovhcloud.com/fr/public-cloud/compute/ https://www.ovhcloud.com/fr/public-cloud/metal-instances/	Instances: Guaranteed resources, GPU, IOPS, discovery VPS: Starter, value, comfort, essential, elite Metal Instances
Object Storage	Object Storage	https://www.ovhcloud.com/fr/public-cloud/object-storage/	Object storage, high performance object storage, cloud archive
	Cold Storage	https://www.ovhcloud.com/fr/public-cloud/cold-archive/	Cold Archive
Block Storage	Block Storage	Dedicated : https://www.ovh.com/fr/cloud-disk-array/	Cloud disk Array, Block Storage

		Public: https://www.ovhcloud.com/fr/public-cloud/block-storage/	
Kubernetes	Managed Orchestration	https://www.ovhcloud.com/fr/public-cloud/kubernetes/ https://www.ovhcloud.com/en/public-cloud/managed-rancher-service/	Managed Kubernetes Service, Managed Rancher Service
	Managed OCI artifact Registry	https://www.ovhcloud.com/fr/public-cloud/managed-private-registry/	Managed Private Registry
Data / Cloud Databases	Managed Search Engine Software Platform	https://www.ovhcloud.com/fr/public-cloud/opensearch/	Managed Opensearch
	Managed Timeseries	https://www.ovhcloud.com/fr/public-cloud/m3db/	Managed M3DB
	Managed In-Memory Database	https://www.ovhcloud.com/fr/public-cloud/redis/	Managed Redis
	Managed Document Database	https://www.ovhcloud.com/fr/public-cloud/mongodb/	Managed MongoDB
	Managed Relational Database	https://www.ovhcloud.com/fr/public-cloud/mysql/ https://www.ovhcloud.com/fr/public-cloud/postgresql/	Managed MySQL, Managed PostGreSQL
	Managed Column-Oriented Database	https://www.ovhcloud.com/fr/public-cloud/apache-cassandra/	Managed Cassandra
	Managed Message Broker	https://www.ovhcloud.com/fr/public-cloud/apache-kafka/	Managed Kafka
	Managed Data Visualisation	https://www.ovhcloud.com/fr/public-cloud/grafana/	Managed Grafana

Data / AI Products	Managed Containers	https://www.ovhcloud.com/fr/public-cloud/ai-deploy/ https://www.ovhcloud.com/fr/public-cloud/ai-training/	AI Deploy, AI Training
	Notebook Interface	https://www.ovhcloud.com/fr/public-cloud/ai-notebooks/	AI Notebooks, Quantum Notebooks

The following business processes are considered to be part of the scope:

- The provision, connectivity, maintenance in operational conditions and decommissioning of the infrastructure allocated to the customer.
  - Provision of the infrastructure allocated to the customer
  - Connectivity of the infrastructure allocated to the customer
  - Maintaining the infrastructure allocated to the customer in operational and security conditions
  - Decommissioning of the infrastructure allocated to the customer at the end of the service
- The means provided to the client for the configuration, use and monitoring of the allocated platform.
  - Configuration of the infrastructure and options by the customer
  - Use and administration of the infrastructure by the customer
  - Monitoring of the infrastructure by the customer

2. Principal Service Commitments and System Requirements

OVHcloud establishes policies and procedures for the Public Cloud Service System to meet its objectives for providing cloud and data services. Those objectives are based on: (i) principal service commitments and requirements made to user entities; (ii) laws and regulations governing the provision of such services; and (iii) other financial, operational, and compliance requirements that OVHcloud has established for these services.

The principal service commitments and system requirements for the Public Cloud Services System include but are not necessarily limited to:

- Security practices within the design, implementation and operation of the Public Cloud Services System are adopted to secure data from unwanted access through access control, technical infrastructure control, encryption, monitoring, and policies and procedures.
- Availability practices within the design, implementation and operation of the Public Cloud Services System are adopted to reduce the likelihood and impact of system inaccessibility through capacity management, backup strategies, and business continuity planning.
- Confidentiality practices within the design, implementation, and operation of the Public Cloud Services System are adopted to identify confidential information classified according to the TLP protocol and apply protection against unauthorized disclosure, through policies and procedures, data classification, security controls, and data destruction.
- Privacy practices within the design, implementation and operation of the Public Cloud Services System are adopted to put in place protection controls to protect Personally Identifiable Information (PII) as a cloud PII processor considering 3 main sources of requirements:
    - Legal, statutory, regulatory and contractual requirements;
    - Risks;
    - Corporate policies.
- Cloud Security Alliance (CSA): OVHcloud has put in place security practices within the design, implementation, and operation of the Storage Services System. OVHcloud has adopted CSA best practices and industry-accepted standards.
- C5: OVHcloud has put in place security practices within the design, implementation, and operation of the Public Cloud Services System. OVHcloud has adopted German sovereignty requirements included within the C5 standard.

OVHcloud establishes operational requirements that support the achievement of its security and availability commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in the company's policies and procedures, design documentation, and contracts with customers. Information security and availability policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained.

In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Storage Services System.

3. Components of the System Used to Provide the Services

Public Cloud Services System is comprised of the following components:

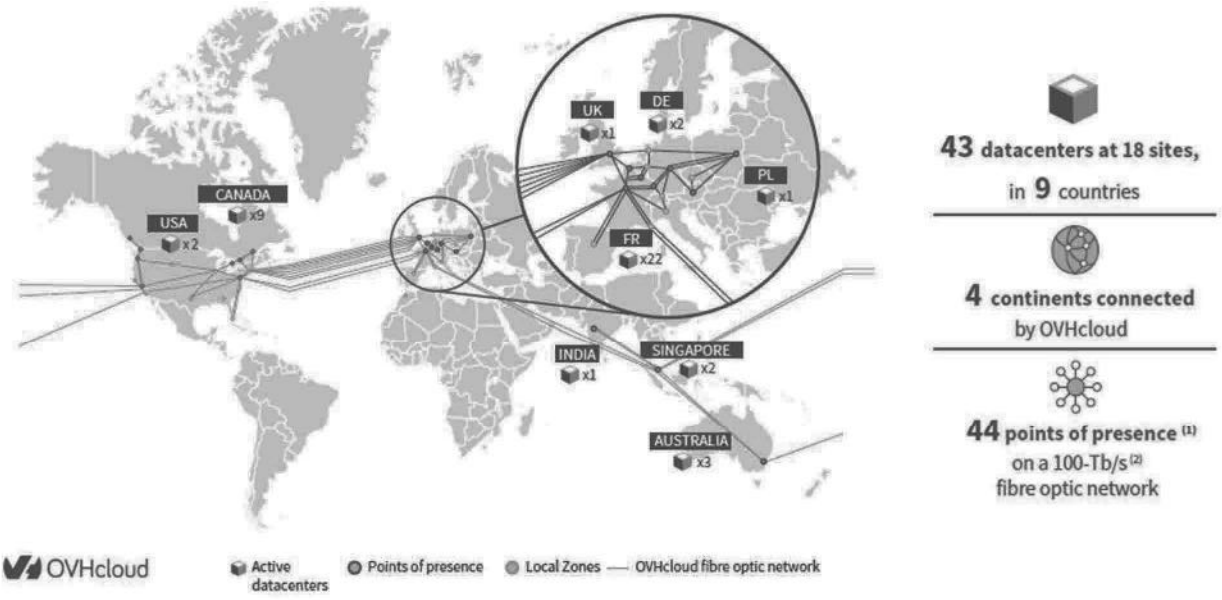
- **Infrastructure:** computer equipment (e.g., servers, network and storage devices) and physical technology upon which the system is hosted.
- **Software:** application programs and system software used to deliver the services.
- **People:** personnel involved in the governance, operation, and use of the system and delivery of services.
- **Procedures:** automated and manual procedures to operate, maintain, and secure the services.
- **Data:** transaction streams, files, databases, tables, and output used or processed by the system.

These components are described in further detail below.

3.1. Infrastructure

OVHcloud has multiple clouds around the world, each operating from a Point of Delivery (POD). A POD is a standardized design of equipment and software that provides the in-scope cloud services. A POD consists of servers, storage and network devices and may vary in size, but the design architecture is similar from site to site.

OVHcloud operates 43 datacenters in 18 locations in Europe, North America, and Asia-Pacific. OVHcloud manufactures its servers in-house and is not dependent on a third-party manufacturer, except for DC tape datacenters and Cold Archive service.



Source: At 31 August 2024, Company.
(1) A point of presence is a point at which the network establishes a connection with the internet.
(2) Tera bits per second.

Figure 10: OVHcloud geographical representation

For Public Cloud products, the following datacenters are used to deliver the service:

Geographical Area	City	Code	Address	Type
France	Roubaix	RBX	2 rue Kellermann 59100 ROUBAIX	OVH DC
	Gravelines	GRA	ZI des Huttes - Route de la ferme Masson 59820 GRAVELINES	OVH DC
	Strasbourg	SBG	9 rue du Bassin de l'Industrie 67000 STRASBOURG	OVH DC
	DC tape Croix	CRX03	155 avenue Georges Hannart 59170 CROIX	OVH DC
	DC tape Bordeaux	VDO01	Bordeaux	Shell & Core
	DC tape Grenoble	EYN01	Grenoble	Shell & Core
	DC tape Saint-Pierre-des-Corps	SDP01	Saint-Pierre-des-Corps	OVH DC
	3-AZ Paris / Marcoussis	MR901	15 rue Marin Angiboust, 91460 Marcoussis	Colocation SOC report managed by suppliers
	3-AZ Paris / Ferrières-en-Brie	IEB01	16 Av. Joseph Froelicher, 77600 Ferrières-en-Brie	Colocation SOC report managed by suppliers
	3-AZ Paris / Clichy	CCH01	7-9 Rue Petit 92582, Clichy	Colocation
Canada	Beauharnois	BHS	50, rue de l'Aluminerie, Beauharnois QC J6N OC2	OVH DC
United Kingdom	Erith	ERI	Viking Way 14, Belvedere Link Industrial Estate - ERITH DA8 1EW	OVH DC

Germany	Limburg	LIM	LIMBURG: Limburger Straße 45, 65555 Limburg-Offheim Germany	OVH DC
Poland	Ozarow	WAW	UL. KAZIMIERZA KAMINSKIEGO 6 – 05-850 OZAROW MAZOWIECKI - POLSKA	OVH DC
Australia	Sydney	SYD1	Data Centre SYDNEY - 639 Gardeners Road, MASCOT NSW 2020	Colocation SOC report managed by suppliers
		SYD2	Next DC 6-8 Giffnock Avenue, Macquarie Park NSW 2113	Colocation SOC report managed by suppliers
India	Mumbai	MUM	Yotta Datacenter Park - Panvel Hiranandani Fortune City. Survey No. 30, MH SH 76, Panvel, Navi Mumbai, Maharashtra 410206, India	Colocation SOC report managed by suppliers
Singapore	Singapore	SGP1	ALTIMAT Data Center Singapore Pte Ltd - 110 Paya Lebar Road - SINGAPORE 409009	Colocation
		SGP2	23 Tai Seng Drive #06-00, Singapore 535224	Colocation

3.2. Software

	System				Application	Monitoring and Auditing
	Management tools	*Virtualization and management tools*	*Server operating systems*	*Backup systems*		
Public Cloud-Compute	Puppet Terraform Deployment-as-a-Service (DaaS) MariaDB RabbitMQ	Openstack Nova Qemu (KVM) Kubernetes Docker	Ubuntu	Swift S3	Octavia (HAProxy)	OVH Logs Data Platform Prometheus / Thanos
Public Cloud-Block Storage	Admin servers Puppet	VMs on OVH Private Cloud (PCC - vSphere)	Multiple admins deployed in geographically independent locations with the same accesses so no failover needed Multiple puppet hosts in geographically independent locations. VM disk on PCC datastores which are redundant by design	Code is hosted on stash.ovh.net, database backups hosted on PCS (Swift)	N/A	Icinga2 Opsgenie OVH Logs Data Platform
Public Cloud-Object Storage	Internally developed orchestrators (Mozg) to manage overall infrastructure puppet	VMs on OVH Private Cloud (PCC - vSphere)	Ubuntu Debian	MySQL dump stored in Swift in another DC VM Managed Backup service provided by PCC	N/A	Icinga2, Opsgenie, OVH Logs Data Platform Prometheus, Grafana, Mimir Tenable, Sonarqube, REVmon

	prefect admin servers					
Data	Ansible MongoDB OpsManager Terraform Aiven (Aiven is a supplier that provides managed services for databases. SOC controls for this provider are covered by its own SOC2 report)	N/A	Ubuntu running Kubernetes clusters and debian	MongoDump for MongoDB sercices block storage disk snapshot etcd is backuped upon each deployment on a given region, backup is sent to PCS swift	Postgresql, MySQL, MongoDB,Redis, OpenSearch, Apache Kafka, apache MirrorMaker 2, Kafka Connect, Grafana, Cassandra, M3DB, M3 Aggregator AI products (models training jobs, VSCode/Jupyter notebooks, Inference APIs deployments) Apache Spark / Jupiyter	Prometheus and Mimir internal offer for metrics LDP for logs Revmon, Jfrog Xray, CVEmon, Tenable for CVE, sentry
Kubernetes	Ansible Terraform	Openstack Docker Kubernetes	Debian	Etcdctl-backup Internal CriticalDB backup management	N/A	Warp10 Mimir OpsGenie LDP Sentry

3.3. People

OVHcloud's mission and core values are carried out by OVHcloud people with respect to integrity, ethical values, management's operating style, delegation of authorities, as well as overall the organization processes set by the Governance.

All personnel are provided with the legally binding Code of Ethics and IT Charter before following onboarding and awareness training. OVHcloud made available an Ethics and Compliance hotline for personnel to anonymously report on possible violations or misconduct. All contracts include non-disclosure requirements and personnel are made aware that any confidentiality breach, violation or misconduct may lead to a disciplinary action which might cause an immediate dismissal. Throughout the hiring process, a staff screening is performed ensuring new hires would fit their role based on knowledge and experience proportionally to the position they would take at OVH-cloud. Staff screening also includes background checks in line with local laws and regulations.

Management distributes roles and responsibilities based on the skillset appropriateness to best combine the skills and experiences of key staff between management, system and software development and maintenance skills. As part of their onboarding, new personnel are trained on OVH-cloud security and control measures that have been defined by management. Regular management and one-to-one meetings are held ensuring continuous feedback and team development in order to support OVHcloud objectives and security measures.

3.3.1. Organizational Structure

The following organization chart illustrates OVHcloud's organizational structure:

- The BU Commerce is responsible for selling OVHcloud solutions to customers, providing them support, animating an ecosystem of offers and partners.
- The BU Product is responsible for developing, automating and operating the cloud infrastructures and platform, relying on industrial standards and based on customer and market feedback.
- The BU Industry is the infrastructure architect and operator of OVHcloud from engineering to server manufacturing, from infrastructure design to data centre management ensuring the level of quality and availability of the infrastructures adapted to the services expected by OVHcloud customers.
- The BU Ops is responsible for coordinating and ensuring that the company's resources are aligned with its objectives by streamlining the organization, providing information systems, automating processes via lean management, and facilitating cooperation between the BUs.
- The BU Corporate consists of the Finance, HR and Legal management functions.

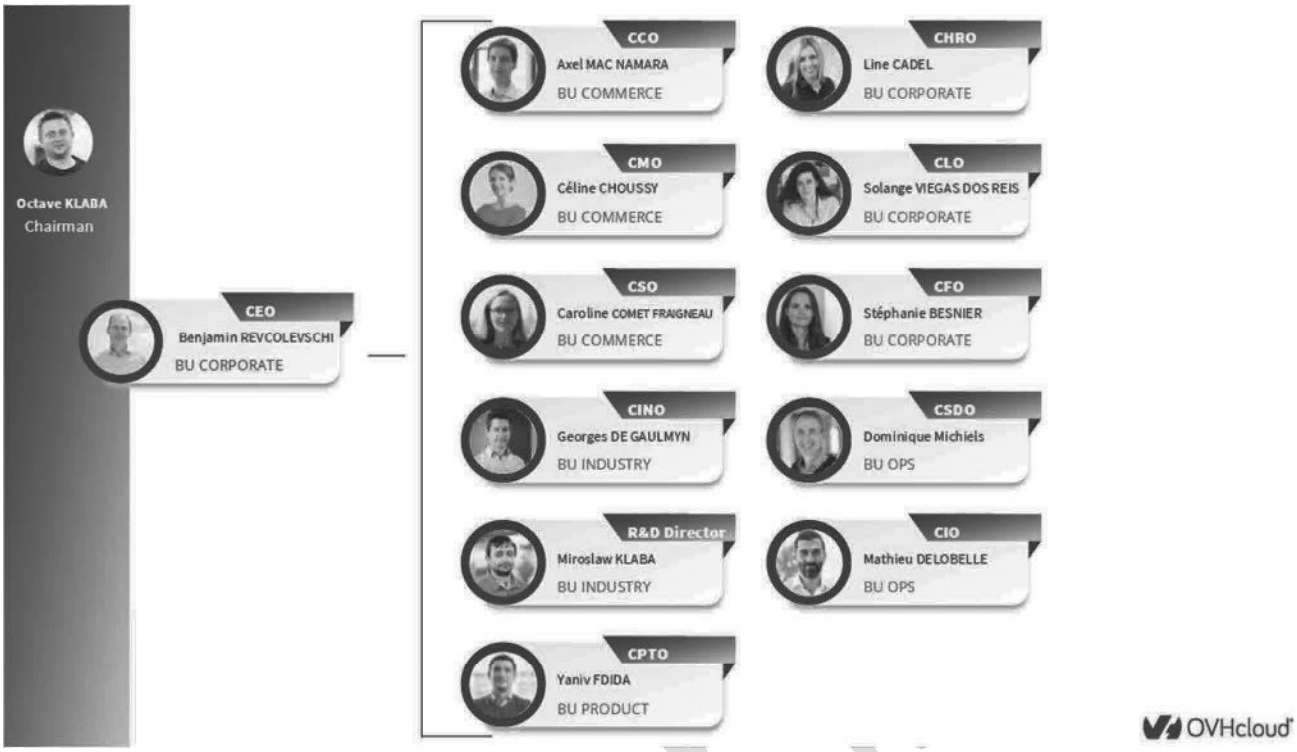


Figure 11: OVHcloud organizational structure

3.3.2. Governance

Governance sets the tone at the top as a foundation of OVHcloud's mission and core values. OVHcloud operates under the management of an Executive Committee committed to the Group's mission to provide customers around the world with secure, trusted, open, sustainable cloud solutions. In addition, the Group is overseen by a Board of Directors composed of independent *administrateurs*. An overview of the members can be found here: https://corporate.ovhcloud.com/en-ie/company/governance/.

OVHcloud corporate governance has established, maintains and monitors standards for integrity, ethical values, management's operating style, delegation of authorities, as well as overall organizational processes. For that purpose, OVHcloud governance has distributed appropriate roles and responsibilities within the organization:

- The Chief Information Security Officer (CISO) to oversee the information security program and who is supplemented by a security team responsible for centralizing the global coordination of information security within OVHcloud including:
  - Dedicated Security Managers responsible for determining, implementing, maintaining and monitoring appropriate and relevant state-of-the-art security measures;
  - A Risk Manager who coordinates the management of security risks and the associated action plans;
- The Data Protection Officer to oversee all topics related to privacy;

- A network of Security and Privacy referents within the different BUs responsible for security and privacy topics within their scope; they ensure the link between the security and privacy teams with the Product and IT teams;
- An Ethics and Compliance team to oversee the ethics and compliance topics.

3.4. Procedures

3.4.1. Policies and Procedures

OVHcloud has developed and maintains its Information Systems Security Policy made publicly available on OVHcloud website: https://docs.ovh.com/gb/en/security/issp/. The ISSP provides the security reference framework to which OVHcloud management is committed towards all OVHcloud stakeholders.

Beyond the main policy setting the security concepts and approach, OVHcloud is organized by security themes adapted to OVHcloud organization and operations with dedicated security procedures and controls:

During the year 2023, the 28 security themes were redesigned:

1	Define and maintain security governance (Security governance)
2	Maintain consistent security principles and documentation (Security model)
3	Provide to customer appropriate security features to manage their risks (Customer Security Features)
4	Implement appropriate data protection for any data managed or hosted (Data Protection)
5	Demonstrate compliance with OVHcloud commitments (Security compliance)
6	Promote risk-based decisions (Security risks management)
7	Build, develop and maintain relationship with security ecosystem (Security ecosystem)
8	Protect customer's cloud usage (Security Protection for Customer)
9	Protect OVHcloud technical reputation (External technical reputation)
10	Assess security and implement continuous improvement (Audits and controls)
11	Assets management
12	Ensure alignment of resources with security objectives and develop a security culture (Human resources, Awareness and Training)
13	Identity, Authentication and Access Management
14	Protect end-user information system (End user information system)
15	Supply Chain and Service Provider Management
16	Support IT and product developments (Project management)
17	Manage security in IS evolution (Change management)
18	Secure continuous delivery

19	Use strong Cryptography (Cryptography)
20	Deploy and maintain secure configuration and hardening (Configuration and hardening)
21	Ensure Network security (Network security)
22	Operations and Maintenance in Security Conditions
23	Logging, security monitoring and detection
24	Vulnerability and patch management
25	Security incident management
26	Datacenter security
27	Office security
28	Resilience

In a fast-moving world where change is the only constant, security practices must constantly evolve to remain relevant and adapted to its environment. As a result, OVHcloud security policies, procedures and controls are subject to a constant evolution to maintain state-of-the-art security practices.

3.4.1.1. Automated Procedures

The automated procedures consist of programmatic controls developed and incorporated into the system, as well as network, infrastructure, server and system software support and monitoring tools. The key automated processes and tools include:

- User authentication and access controls
- Scheduled system and infrastructure backup processes
- Automated system monitoring and logging
- Automatic alerting (for security and availability)

3.4.1.2. Manual Procedures

Manual processes (supported by policies, procedures, and guidelines) for operating and maintaining the system, including processes for:

- User administration processes
- Security and vulnerability management processes
- Service desk processes
- Client delivery, onboarding and system configuration processes
- Client decommissioning processes
- Change management processes
- Security Monitoring
- Patch updates and change control processes
- Physical security processes
- Technical configuration baselines
- Incident and problem management processes
- HR procedures, including background checks and performance reviews
- Business Continuity and Disaster Recovery procedures

3.5. Data

The key types of data collected, processed, and stored by the Public Cloud Services System include:

- Server and network configurations
- Custom parameters for client configurations
- Client information specific to access control, including usernames
- Client personal data specific to support and billing
- Logs of all infrastructures, including customers infrastructures

This data is collected, processed and stored to guarantee the provision, connectivity and maintenance in operating condition.

4 Relevant aspects of the Control Environment, Risk Assessment, Monitoring and Information and Communication

4.1 Control Environment

Management Philosophy

OVHcloud's control environment reflects the philosophy of executive management and other stakeholders concerning the importance of security for its customers. The importance of security is emphasized within OVHcloud through the establishment of policies, procedures and awareness, as well as investment in resources and people to implement them. Management places importance on controls and security in its processes, policies, procedures and organizational structure.

Code of Conduct, Integrity and Ethical Values

OVHcloud is committed to acting with the highest ethical and integrity standards and requires its employees to behave likewise. For this purpose, OVHcloud has established several controls to promote and ensure integrity and ethical values, including:

- An employee handbook is in place and is provided to employees as part of the onboarding process.
- All employees are bound by confidentiality clauses and are required to abide by all internal policies.
- A set of policies addressing anti-corruption, anti-bribery, anti-discrimination, anti-harassment and whistleblowing are in place.
- A disciplinary procedure is in place and documented, communicating that an employee may be sanctioned for noncompliance with a policy, including security policies or misconduct.
- Employees are required to sign a confidentiality statement upon hire agreeing not to disclose proprietary or confidential information, including customer information, to unauthorized parties.
- Background checks are performed for employees as a component of the recruitment process, including a criminal record check for sensitive positions.

Organizational Structure and Assignment of Authority and Responsibility

OVHcloud has a board of directors which provides oversight and is involved in significant business decisions. In accordance with Article 2 of the Board of Directors' internal regulations, the Board meets at least four times a year, and the majority of board members are independent from executive management.

OVHcloud's organizational structure is managed by an Executive committee. The organizational structure is designed to support the achievement of the Company objectives. Key areas of authority, responsibility and reporting lines are defined. Management continuously evaluates the

organizational structure and makes changes as necessary. The organizational structure is described in an organizational chart, available to all OVHcloud employees and updated as necessary.

Responsibilities related to information security are defined in a set of policies. These policies are updated as required and are available to all employees on the intranet.

Human Resources and Commitment to Competence

OVHcloud has a recruitment process to evaluate applicants' abilities to perform the duties outlined in their job description. Each applicant must participate in several interviews with different stakeholders, depending on the targeted position and applicant's seniority. Throughout the process, interview feedback is collected. For applicants to whom an offer of employment is made and is accepted, a background check is performed. Upon arrival in the company, newcomers follow an onboarding process which includes a security awareness session to increase their understanding of security policies as well as their responsibilities to comply with these policies. In addition, people hired in the Software engineering team participate in a secure software development training, which includes recognized standards like the OWASP Top 10 and which also considers the technical specificities of OVHcloud environment, to help ensure they are aware of web vulnerabilities and how to avoid them.

For each position, a job description is documented and updated as needed. The job description outlines the role as well as the responsibilities for the position and serves as a basis for assessing employees' performance.

Management performs a bi-annual performance review of employees to evaluate their performance, review their contribution to OVHcloud success, set the objectives for the upcoming period, provide feedback and identify the needs for training.

Information Security Management

OVHcloud has a dedicated Security team, led by the Chief Information Security Officer, that is responsible for the management and monitoring of information security throughout the Organization. OVHcloud has developed, documented, approved and ISO27001 certified an Information Security Management System that includes a set of policies and procedures.

OVHcloud's top management, through the CEO, defines the information security objectives and the Executive committee monitors the progress towards meeting those objectives.

On an annual basis, OVHcloud management reviews the additional needs identified by security management to achieve security and compliance business objectives. This includes potential new hires in the Security Team, tools, training and consultancy.

Access Control

OVHcloud internal access

OVHcloud has developed and maintains an access control policy that governs the granting of access to internal systems.

User access provisioning

Access to the systems is managed based on the role the individual has within the company, using the least privilege and need-to-know principles. Access rights for new employees are created based on predefined roles, their team and their role in the team. Access or privileges granted in addition to the standard role are validated by management.

User access revocation

A checklist is in place to guide and track the offboarding of staff members, including termination of employees. Management notifies the Human Resources (HR) Team of changes or terminations of employees or contractors to review their access privileges and revoke them as appropriate, in a timely manner. High risk permissions and accounts are revoked first to help ensure that the most sensitive systems can no longer be accessed.

Periodic user access review

User accounts and permissions to critical systems are reviewed on a bi-annual basis, to ensure that access is based on current job activities and identify the existence of accounts that are no longer valid (e.g., belong to the leavers) or unauthorized.

User authentication

To help ensure that only authenticated and authorized users can access the systems, OVHcloud has established an access control policy and requirements for user authentication in a password policy. Access to in-scope system components requires a unique username and password or key, prior to authenticating users. In addition, multi-factor authentication is enforced on critical systems and services, depending on the technical possibilities. Passwords for in-scope system components are configured according to the requirements mentioned in the password policy. A combination of parameters is in place, including but not limited to:

- Password minimum length;
- Password complexity;
- Password renewal frequency;
- Password history limitations;
- Account lockout threshold.

OVHcloud customer access

Access to the OVHcloud solution requires authentication and appropriate authorization. By default, on the OVHcloud solution, a login / password authentication mechanism is provided to user organizations (i.e., Customer). A password complexity policy is enforced using a combination of parameters, including but not limited to:

- Password minimum length;
- Password complexity;

- Password history limitations;
- Account lockout threshold.

Two-factor authentication can be set up on the Customer's instance. The two-factor authentication mechanism requires the use of a One-time password (OTP), in addition to the login and password. Otherwise, user organizations (i.e., Customers), depending on the Service offer, have the option of integrating via SAML, their OVHcloud instance and their SSO.

Various roles are provided and available in the solution, and can be assigned to end-user accounts, according to user organization's needs.

Encryption

Encryption is leveraged to protect confidential data, at rest and in transit. In particular:

- Communication sessions between the OVHcloud solution and end-users are secured via the Transport Layer Security (TLS) protocol that ensures data encryption, integrity, and server authentication.
- Confidential customer data is encrypted at rest.
- OVHcloud utilizes a mobile device management tool to manage and encrypt employee workstations.

Configuration Management

OVHcloud uses the infrastructure-as-code approach to automate the deployment, configuration and destruction of systems. This is to help avoid configuration drifts and ensure baseline configuration is consistently applied across tenants. Changes to the configuration are peer-reviewed and tracked in the code management software.

Software Development Lifecycle and Change Management

To maintain stability of production environments, OVHcloud maintains a Software Development Lifecycle and change management process, which governs how software and infrastructure changes are introduced. The process is based on Agile principles and security best practices. Changes are documented, tracked and monitored thanks to a ticketing system.

To control access to the source code library, maintain history of code changes and manage versions, source code management software is used. A continuous integration pipeline is utilized to automate build, test and tagging of new software releases. When a new change is committed in the repositories, unit and integration tests are automatically performed and the code is scanned by a Static Application Security Testing (SAST) tool to help detect known vulnerabilities, insecure coding practices and security sensitive pieces of code. The outcomes of the tests are documented in the pull request. Change requests are peer-reviewed via a pull request and approved by someone who did not authorize the code, before being merged with the main branch.

At the end of each sprint, end-to-end tests are performed to help ensure that regressions are not introduced in the new release, before it is rolled out in production environments. Hotfixes can be

performed between two standard releases to introduce minor changes, fix a bug or deploy a security patch. Emergency changes follow the standard change management, with the exception that approval is not required in advance but can be obtained retrospectively.

To ensure that unauthorized changes are not introduced in production environments, only authorized users can deploy changes in production environments.

Network Security

The network is logically segmented to help ensure that Customer data is isolated from other networks and protected from unauthorized access. Specifically, the production environments are logically segmented from test and development environments. Firewalls are in place to filter unauthorized network traffic from the internet and protect production systems. Firewalls are configured to deny inbound connections which are not explicitly authorized.

To further protect production systems from external threats, traffic from the internet passes through a load balancer which includes a network and transport layer denial of service protection. In addition, a Web Application Firewall (WAF) is utilized to filter web traffic.

A threat detection service, with network intrusion detection (IDS) capabilities, continuously monitors production environments for suspicious or malicious activities and is operated by OVHcloud.

Access to production networks is granted using the least privilege principle. Remote access to OVHcloud production networks is restricted through VPN or bastion hosts that enforce multi-factor authentication (MFA) and encrypted communications.

Mobile Devices

OVHcloud laptops are enrolled in a Mobile Devices Management which enables them to enforce security controls such as disk encryption, system hardening, application control and lock screen. Laptops are protected by an antivirus solution that is automatically updated.

Vulnerability & Patch Management

OVHcloud has established a vulnerability process to identify, evaluate and treat vulnerabilities in a timely manner. The process includes a combination of scans and penetration tests to identify vulnerabilities as well as procedures to manage vulnerabilities throughout their lifecycle. The vulnerability management process is supported by a patch management process to help ensure that systems are up-to-date and reduce the risk of compromise.

Vulnerability scans

To identify vulnerable components, several types of scans are performed to cover the different systems and layers of the platform. It includes scans of public facing components, scans of internal systems and scans of code repositories to detect vulnerable open-source software dependencies. Outcomes of the scans are reviewed and analyzed by the production teams, that can request the assistance of OVHcloud Computer Emergency Response Team (CERT) and are managed as part of the vulnerability management process.

Penetration testing

To validate the security posture and identify potential vulnerabilities in the platforms, OVHcloud works either with its own pentest team or with third parties to perform penetration tests at least on an annual basis. The scope of the test includes the platform and an assessment of the OWASP top 10 vulnerabilities or specific designed tests adapted to the situation. Additional scenarios can be added to focus on areas presenting a higher degree of risk or new functionalities. In addition, depending on the Service offer, customers can perform their own penetration tests on the platform, under the conditions described in the Master Service Agreement The results of the tests are reviewed, the risks induced by the findings are assessed and a treatment plan is defined, tracked and executed.

Vulnerability management

OVHcloud has established a vulnerability management policy defining the scale and methodology to assess the severity of the identified vulnerabilities and treatment time frames depending on the severity levels. To assess the severity of vulnerabilities, OVHcloud security team uses the CVSS score (Common Vulnerability Scoring System) for the initial assessment and then assesses the risk involved, by considering the specificities of the infrastructure and the platform. Based on this assessment, a treatment plan is defined and documented in a ticketing system to be tracked until resolution.

Patch management

To help ensure that the supporting cloud infrastructure is hardened, systems are automatically patched as part of routine maintenance or because of the vulnerability management process. Servers and containers are configured to use the most up-to-date stable version of the operating system and install security patches during each release or hotfix.

Replication, Backups and Disaster Recovery

Replication

In production environments, the services are replicated across several zones, according to need and the responsibility model for each product.

Backup

Data is automatically backed up on a regular basis and at least once a day. Backup jobs are monitored, and a notification is sent to IT teams in the event of a failure for triage, investigation and resolution. Database restoration from backup is regularly tested by the team as a component of business operations. To help ensure the resumption of operations in the event of a disaster, production data and backups are stored within several Datacenters.

Disaster recovery

OVHcloud has a Business Continuity and Disaster Recovery Plan to help ensure availability of services following a disaster or other adverse events. The plan details in which cases it shall be activated, the response structure to cope with the adverse event, the roles and responsibilities

as well as the overall process to follow. The plan is documented, updated, tested annually, and complemented by several procedures. To maintaining an up-to-date plan, a Business Impact Analysis is performed on a yearly basis to determine business continuity priorities and requirements. Based on the outputs from the risk assessment and the Business Impact Analysis, BCDR strategies are Identified, and an action plan defined.

System Monitoring Detection

The Service and production environments are continuously monitored to help detect suspicious activities which could be an indication of a security incident, an unauthorized access, or an availability related issue. To this end, a wide variety of logs and metrics are collected, that includes, application logs, infrastructure logs, system availability, systems performance, database capacity, access logs and security events.

OVHcloud leverages automated tools and manual reviews to analyze the collected logs and metrics. Moreover, automated notifications and alerts are configured to notify appropriate personnel when certain thresholds or events are detected, so that additional analysis can be carried out and proactive or remedial actions may be taken if necessary.

Security Incidents Management

OVHcloud maintains a Security Incident Management Policy that is triggered once a security incident is confirmed. It includes roles and responsibilities along with the steps to follow, from detection to response. Security incidents are logged, tracked, and reported to management and a root cause analysis is performed.

4.2 Risk Assessment

OVHcloud maintains an information security risk management process initiated as part of the Information Security Management System (ISMS) implementation as part of the ISO 27001 certification. The risk management process serves as a decision-making process combining OVHcloud mission objectives together with security activities for enlightened decisions based on a risk-based approach.

OVHcloud information security risk management is based on the ISO 27005 industry standard and consists in the following phases:

- **Context Establishment**: OVHcloud sets the purpose of the information security risk management process together with the basic criteria revolving around the risk evaluation criteria, impact criteria and risk acceptance criteria. OVHcloud then establishes the scope and boundaries of the ISMS perimeter considering relevant assets to be considered. The following steps consist of gathering information around the ISMS context and environment in which it operates considering internal and external factors through workshops.
- **Risk Assessment**: OVHcloud considers the following activities:
- **Risk Identification**: OVHcloud assesses the consequences triggered by potential loss events on the identified assets according to their criticality, related threat sources and vulnerabilities. The risk scenario is then evaluated against OVHcloud security controls that could mitigate the risk and relevant industry controls and frameworks such as the NIST Cybersecurity Framework.

- **Risk Analysis**: For each risk, OVHcloud carries on a risk level estimation including impact and likelihood together with the determination of level of risk.
- **Risk Evaluation**: Based on the defined methodology, OVHcloud compares the risk against the risk evaluation and acceptance criteria for treatment actions prioritized according to criticality.
- **Risk Treatment and Acceptance**: Specific risk treatment plans are defined to mitigate the risks and residual risks subject to acceptance decisions are calculated. Based on the overall risk information consolidated, risk treatment plans are prioritized and integrated with objectives.
- **Risk Communication and Review**: As a continuous process, OVHcloud reviews and monitors the risks and risk treatment plans on a regular basis with the related risk owners ensuring continuous alignment with the organization's business objectives and risk acceptance criteria and maintaining a continuous relevance of the information security risk management process.

4.3 Monitoring

OVHcloud has implemented and maintains continuous monitoring of its Information Security Management System ensuring internal controls are designed in an appropriate and effective manner and internal controls operate as intended. Monitoring activities then enables OVHcloud management to assess the quality of the Information Security Management System performance over time.

Monitoring operates at the entity level as well as at the process level and is accomplished through both ongoing monitoring activities as well as periodic, separate evaluations.

Overall monitoring results are communicated to management on a regular basis during dedicated management meetings to review the major risks including the main threats under surveillance, the monitoring metrics, the progress of the ongoing actions and the updated roadmap. Management meetings with the Executive Committee also ensure that the ISSP is aligned with OVHcloud's strategic and operational objectives.

4.3.1 Ongoing Monitoring

OVHcloud has implemented entity level Information Security Management System monitoring activities supplemented by perimeter process level monitoring activities. OVHcloud distinguishes different perimeters for each of its certified Information Security Management System as part of the ISO 27001 certification: datacenters as a whole and individual products would be considered as perimeters with specific processes when required by the nature of its operations.

On the one hand, transversal activities related to governance, human resources, privacy, security with third parties and customers are therefore monitored as part of entity level Information Security Management System monitoring activities. On the other hand, specific activities which can differ per perimeter depending on the nature of their operations and the technologies in use such as physical and logical security, identity and access management, backup and restoration, network security, logging and monitoring activities, change and incident management are monitored as part of perimeter process level Information Security Management System monitoring activities.

Ongoing monitoring activities are overseen by the Security Managers in coordination with the perimeter management and security personnel within the teams in respect of security best practices defined by the Security team, standards requirements, SLAs for technical processes and ongoing monitoring is directly supervising the running and maintenance of the infrastructure on a day-to-day basis.

OVHcloud uses a wide variety of monitoring systems to:

- prevent and detect production and security incidents;
- monitor critical features, with any alerts being escalated to the monitoring system;
- inform the responsible persons and trigger the appropriate procedures;
- ensure continuity of service in the performance of automated tasks;
- ensure the integrity of the resources monitored.

Technical incidents and issues such as breakdown, disruption of service, slowdown, bugs, etc. are subject to analysis and review in management meetings following the event to be disclosed to customers when applicable for transparency purposes.

4.3.2 Separate Evaluations

As part of its Information Security Management System, OVHcloud has implemented an audit process assessing security controls are properly designed and operating effectively in order to ensure continuous improvement and compliance. OVHcloud considers five types of security audits:

- external audits (certifications, attestations, customers) – see below;
- internal audits, carried out internally or by external auditors;
- technical audits (intrusion tests, vulnerability scans, code reviews), carried out internally or by external auditors;
- audits of the activities of third parties, carried out by the person responsible for managing third parties;
- datacenter audits, carried out by internal auditors. The nature and frequency of the audits carried out will depend on the solutions and the perimeters. Whenever non-compliance is identified, a corrective measure is applied and added to the action plans. All these measures are covered by a formal, tracked follow-up, as well as a regular review, where their effectiveness is re-examined.

As part of the external audits, OVHcloud maintains several key certifications issued by independent audit reports to provide solutions with the highest security standards, including amongst others:

- **ISO/IEC 27001**: This security certification standard evaluates an organization's compliance with the standards released by the International Organization for Standardization (ISO), which establishes best practices for the management system for information security within an organization. The certification is performed by an independent third party and assesses the information security for a range of information assets, including financial information, intellectual property and employee information.

- **ISO/IEC 27701**: ISO/IEC 27701 can be considered as an extension of ISO/IEC 27001 and ISO/IEC 27002, to incorporate the notion of managing personal data protection. This standard specifies requirements and provides guidance for the setup, implementation, maintenance and continuous improvement of a Personal Data Protection Information Management System (PIMS). This international standard considers the GDPR and allows organizations that adopt it to demonstrate their approach to protecting personal data.
- **SecNumCloud**: This is the highest French security certification for cloud providers, released by the French National Cybersecurity Agency (ANSSI) to guarantee data security
and sovereignty. The certification aims at guiding public/administrative authorities, vital organizations and all French and European economic entities towards trusted cloud providers to store sensitive data. It is based on an extensive security audit.
- **PCI DSS**: The Payment Card Industry Data Security Standard is a security certification administered by the PCI Security Standards Council (PCI SSC). It certifies that a business
conforms with the PCI SSC standards on the storage, transmission and processing of cardholder data when processing card payments to reduce card fraud.
- **HDS**: The "*Hébergeur de Données de Santé*" (HDS) security certification reflects standards
determined by the French *Agence du Numérique en Santé (ANS)* with respect to health information security measures. It is required for organizations that host personal health data under French law and certifies that such organizations meet the required security standards to handle this sensitive information. The assessment of compliance is made by
an independent third-party through both a documentary and on-site audit.

An overview of OVHcloud's overall certifications can be found here: https://www.ovhcloud.com/en-ie/enterprise/certification-conformity/.

A combination of automated and manual processes is used to operate the Public Cloud Services System.

4.4 Information and Communication

OVHcloud has established an internal and external information and communication process ensuring the relevant information is identified, captured and communicated to the interested parties.

4.4.1 Internal Communication

Effective communication also must occur in a broader sense, flowing down, across and up the OVHcloud organization. Information systems deal not only with internally generated data, but also information about external events, activities and conditions necessary for informed business decision making and external reporting.

As from their onboarding, OVHcloud ensures that employees have a clear understanding of their defined roles and responsibilities ensuring that they can properly carry out their responsibilities and report significant events in a timely and effective manner upstream. In addition, newly hired employees follow onboarding training introducing them to OVHcloud environment and procedures.

Internal communications may take the form of policies, procedures, global communications (via email and the Intranet), regular management meetings at various levels covering from top management to middle management to operational teams. Key communications related to OVHcloud mission, strategy, new product releases, financials, partnerships but also major incidents are communicated through global channels internally. New procedures, projects, infrastructures or software applicable to specific teams are communicated to the relevant groups pointing towards the related resources on the collaborative internal tools and points of contact.

Security policies and related procedures are formalized and controlled with the Security team who ensure that the relevant teams receive the appropriate information. Security controls then enable the Security team to monitor the application of security policies and related procedures.

4.4.2 External Communication

External communication is managed by a dedicated team together with Senior Management through multiple public interactive communication channels to effectively communicate on OVHcloud mission, strategy, new product releases, financials, partnerships but also major incidents. Specific communications towards external parties, such as customers, suppliers, regulators and shareholders are handled by specific teams with the appropriate level of expertise within OVHcloud.

To be transparent towards its customers, OVHcloud makes available a dedicated status page for all interested parties regarding OVHcloud products status: https://www.status-ovhcloud.com/. This status page allows internal teams communicate on all incidents, from critical incidents that can impact many customers to localized incidents that can impact only a few customers; this is what we call "1 to many" and "1 to few" communications. In addition, OVHcloud maintains an incident management process to follow-up on customer reported issues to ensure they are investigated and resolved.

OVHcloud also maintains a web page with customer-oriented documentation and tutorials to provide customers guidance in the deployment and day-to-day use of their OVHcloud solutions: https://docs.ovh.com/ie/en/.

5 Description of Complementary User Entity Controls

OVHcloud services were designed with the assumption that certain policies, procedures and controls are implemented by its customers in a principle of shared responsibility between OVHcloud and its customers. While OVHcloud achieves the objectives described in Section III, the overall achievement of the control objectives also depends on the policies, procedures and controls implemented by user organizations. As such, user organizations are responsible for the design, implementation and operation of their OVHcloud environment according to the level of service they have chosen. Therefore, user organizations are responsible for evaluating their own internal control to determine whether the identified Complementary User Entity Controls have been appropriately designed and operating effectively, where applicable.

The list of Complementary User Entity Controls presented below does not represent all control considerations required by user organizations as other controls may be required in line with the user organization's characteristics.

	Complementary User Entity Control Considerations	Associated Criteria
	General	
1	User organizations should maintain formal policies that provide guidance for information security within the user organization and the supporting IT environment.	CC1.5, CC5.3
2	User organizations are responsible for identifying and establishing adequate controls in line with responsibilities defined as per the contractual agreement and the Data Protection Agreement signed with OVHcloud.	CC1.1, CC1.3, CC1.5
3	User organizations should assess whether the security control objectives applied by OVHcloud are relevant to the risks associated with the way they use their OVHcloud infrastructure. Therefore, user organizations are responsible for identifying the risk and corresponding controls to be implemented to address those risks when using OVHcloud services, software and implementing OVHcloud operational controls.	CC3.1, CC3.2, CC3.3
	Access	
4	User organizations are responsible for establishing appropriate controls and measures allowing relevant access to the environment provided by OVHcloud.	CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7
5	User organizations are responsible for using strong authentication methods to their OVHcloud environments such as multi-factor authentication or strong passwords.	CC6.6
6	User organizations are responsible for establishing appropriate access controls over the use of their OVHcloud environments such as security groups, Identity Access Management and/or Access Controls Lists and Segregation of Duties.	CC6.1, CC6.2, CC6.3, CC6.4,

		CC6.5, CC6.6, CC6.7
7	User organizations are responsible for reviewing the access rights and logs associated with their OVHcloud accounts.	CC6.1, CC6.3
8	User organizations are responsible for granting and disabling access to their OVHcloud services when necessary.	CC6.3, CC6.5
9	User organizations are responsible for ensuring the supervision, management and control for access to key systems hosted in the OVHcloud environment.	CC6.1, CC6.3, CC7.2
10	User organizations must ensure that their workstations and mobile equipment are secure to enable the administration tasks of their OVHcloud service and related systems in line with the criticality of their environment.	CC6.1, CC6.6, CC6.8
	Security events, backup and patching	
11	User organizations are responsible for monitoring security related events and logging appropriate diagnostic information of their systems in their OVHcloud environment.	CC7.1, CC7.2, CC7.3
12	User organizations are responsible for identifying and patching vulnerabilities as well as ensuring periodic maintenance on their OVHcloud environment in line with responsibilities defined as per the contractual agreement.	CC7.1, CC7.2
13	User organizations are responsible for establishing their own backup and restoration processes in the event of loss or damage to their OVHcloud environment. User organizations may subscribe to OVHcloud additional services for this purpose.	A1.2, A1.3
14	User organizations are responsible for implementing their own Disaster Recovery and Business Continuity Plans that address the inability to access or utilize their OVHcloud environment. User organizations may subscribe to OVHcloud additional services for this purpose.	CC9.1, A1.2, A1.3

15	User organizations are responsible for ensuring that their OVHcloud resources have the appropriate levels of redundancy and isolation; redundancy can be achieved using multiple locations.	CC9.1, A1.1, A1.2
16	User organizations are responsible for implementing appropriate incident response processes.	CC7.4, CC7.5
	Change management	
17	User organizations are responsible for following appropriate security practices during development and deployment of their systems in the OVHcloud environment.	CC8.1
18	User organizations are responsible for appropriately testing and approving changes on their systems before being deployed in their OVHcloud environments.	CC8.1
	Data and Privacy	
19	User organizations are responsible for managing compliance with applicable laws and regulations (including the General Data Protection Regulation).	P1.1, P2.1, P4.2, P6.6
20	User organizations are responsible for the integrity and the content of the data stored in their OVHcloud environment and the data transfers from their OVHcloud environment to an external environment. User organization should establish adequate controls for ensuring data integrity and compliance with applicable regulatory requirements.	CC6.7
21	User organizations are recommended to use encrypted (TLS/SSL) connections for all their interactions with OVHcloud. User organizations are responsible for determining, implementing and managing encryption requirements in their OVHcloud environment when it is not enabled by default and / or can be controlled by user organizations.	CC6.7, CC6.8
22	User organizations are responsible for managing IP resources in an appropriate and sufficient manner to ensure the proper functioning of the OVHcloud services they subscribed to.	CC6.7, CC6.8

	Public Cloud specifics		
23	Compute	User organizations are responsible for installing and managing operating systems and applications on their instances.	CC6.1, CC5.1
24		User organizations are responsible for their use of the Service, in particular allocated processing capability and storage resources: User organizations are responsible for ensuring that instances have sufficient resources to function correctly.	A1.1, A1.3
25		User organizations are responsible for allocating appropriate storage assets to their instances, managing data lifecycle, including backups and encryption.	A1.2, A1.3, CC6.7, CC6.8
26	Block Storage	User organizations are responsible for allocating appropriate storage assets to their instances, managing data lifecycle, including backups and encryption.	A1.2, A1.3, CC6.7, CC6.8
27	Object Storage	User organizations are responsible for allocating appropriate storage assets to their instances, managing data lifecycle, including backups and encryption.	A1.2, A1.3, CC6.7, CC6.8
28	Managed Kubernetes	User organizations are responsible for their use of the Service, in particular allocated processing capability and storage resources: User organizations are responsible for ensuring that instances have sufficient resources to function correctly.	A1.1, A1.3
29		User organizations are responsible for not altering the pre-configured systems that operate the Kubernetes cluster.	CC5.1, CC5.2, CC6.1
30	Private Registry	User organizations are responsible for the lifecycle of the images stored in their private registry; user organizations are responsible for ensuring their images are devoid of security vulnerabilities or malware.	CC5.1, CC6.6, CC7.2
31	Data	User organizations are responsible for their use of the Service, managing data lifecycle and encryption.	CC6.7

Public Cloud Specifics

Computer

Further details on user organizations responsibilities are detailed on https://help.ovhcloud.com/csm/en-gb-public-cloud-instances-raci?id=kb_article_view&sysparm_article=KB0054604.

Block Storage

Further details on user organizations responsibilities are detailed on https://help.ovhcloud.com/csm/en-gb-public-cloud-block-storage-raci?id=kb_article_view&sysparm_article=KB0054797.

Object Storage

Further details on user organizations responsibilities are detailed on https://help.ovhcloud.com/csm/en-gb-public-cloud-storage-shared-responsibility?id=kb_article_view&sysparm_article=KB0057223.

Managed Kubernetes

Further details on user organizations responsibilities are detailed on : https://help.ovhcloud.com/csm/en-gb-public-cloud-kubernetes-responsibility-model?id=kb_article_view&sysparm_article=KB0058751.

Private Registry

Further details on user organizations responsibilities are detailed on https://help.ovhcloud.com/csm/en-gb-public-cloud-private-registry-responsibility-model?id=kb_article_view&sysparm_article=KB0058675.

Data

Further details on user organizations responsibilities are detailed on https://help.ovhcloud.com/csm/en-gb-public-cloud-databases-responsibility-model?id=kb_article_view&sysparm_article=KB0036388.

6 System Incidents

There was no identified significant system incident that were the results of controls that were a) not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements from January 1, 2024 to December 31, 2024.

7 Changes to the System

There was no significant change that is likely to affect report users' understanding of Public Cloud system and service provided from January 1, 2024 to December 31, 2024.

8 CCM Criteria and C5 controls that are not applicable to OVHcloud's Public Cloud system, with the relevant justification.

8.1 Not applicable CCM Criteria

Control Domain	CCM Control ID	Justification
Application & Interface Security Data Integrity	AIS-02	Processing integrity controls are not included in the scope of this report because OVHcloud's Public Cloud solution is an IaaS solution and does not process customer's data. OVHcloud is not responsible of customer data integrity.
Application & Interface Security Data Integrity	AIS-03	Processing integrity controls are not included in the scope of this report because OVHcloud's Public Cloud solution is an IaaS solution and does not process customer data. OVHcloud is not responsible of customer data integrity.
Application & Interface Security Data Security / Integrity	AIS-04	Processing integrity controls are not included in the scope of this report because OVHcloud's Public Cloud solution is an IaaS solution and does not process customer data. OVHcloud is not responsible of customer data integrity.
Change Control & Configuration Management Outsourced Development	CCC-02	This requirement is not applicable because OVHcloud does not outsource development and change management processes on the Public Cloud perimeter.
Data Security & Information Lifecycle Management Ecommerce Transactions	DSI-03	This requirement is not applicable because the Public Cloud offer does not provide e-commerce solutions.
Encryption & Key Management Storage and Access	EKM-04	This requirement is not applicable because OVHcloud does not encrypt customers' data hosted on its servers. Data encryption is the customer's responsibility. The customer manages their own key usage.

8.2 Not applicable C5 Criteria

Criteria title	C5 Criteria ID	Justification
Outsourcing of the development	DEV-02	This requirement is not applicable because OVHcloud does not outsource development and change management processes on the Public Cloud perimeter.
Encryption of sensitive data for storage	CRY-03	This requirement is not applicable as the encryption of customer data hosted on the Public Cloud products is under the customer's responsibility.

9 Additional information about Management's description

The controls supporting the service organisation's service commitments and system requirements based on the applicable trust services criteria are included within section IV of this report, «Management's Description of its Relevant Criteria and Related Controls, and Independent Service Auditors' Description of Tests of Controls and Results». Although the applicable trust services criteria and related control activities are presented within Section IV, they are an integral part of OVHcloud's description of its system.

SECTION IV Management's Description of its Relevant Criteria and Related Controls, and Independent Service Auditors' Description of Tests of Controls and Results

1. Description of testing procedures performed

We performed a variety of tests relating to the controls listed in this section throughout the period from January 1, 2024, to December 31, 2024. Our tests of controls were performed on controls as they existed during the period from January 1, 2024, to December 31, 2024, and were applied to those controls specified by OVH Groupe S.A.

In determining the nature, timing and extent of tests, we considered (a) the nature and frequency of the controls tested, (b) the types of available evidential matter, (c) the assessed level of control risk, (d) the expected effectiveness of the test, and (e) our understanding of the control environment.

In addition to the tests listed below, we ascertained through multiple inquiries with management and the control owner that each control activity listed below operated as described throughout the period. Tests performed are described below:

Test Procedure	Description
Inspection	Inspecting documentation subject to the control. This includes, among other things, reading (management) reports to assess whether the specific control is properly monitored, controlled and resolved on a timely basis.
Observation	Observing of the performance of the control by OVHcloud.
Inquiries	Interviewing appropriate OVHcloud personnel about the operation of the controls.
Re-performance	Re-performing the operation of a control to ascertain that it was performed correctly.

Information produced by the entity

For tests of controls requiring the use of information produced by the entity (IPE), including electronic information (for example, controls requiring system-generated populations for sample-based testing), we performed a combination of the following procedures where possible - based on the nature of the IPE - to address the completeness, accuracy, and data integrity of the data or reports used:

- Inspected the source of the IPE
- Inspected the query, script, or parameters used to generate the IPE
- Tied data between the IPE and the source
- Inspected the IPE for anomalous gaps in sequence or timing to determine that the data is complete, accurate, and maintains its integrity

For tests of controls requiring management's use of IPE in the execution of the controls (for example, management's monitoring of alerts generated by its intrusion prevention system [IPS]), we performed additional procedures including, but not limited to, inspecting evidence of authorization for users with access to administer and modify IPS configurations, a selection of changes to configurations, and updates applied to the IPS during the examination period. We inspected evidence of management's procedures, as applicable, to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Reporting on results of testing

The concept of materiality is not applied when reporting the results of control tests because we do not have the ability to determine whether an exception will be relevant to a particular user entity. Consequently, we report all exceptions.

Results of Testing Performed

The information regarding the tests of operating effectiveness is explained below in four parts:

Part A: Mapping between applicable Trust Services Criteria and OVHcloud Controls

Part B: Mapping between applicable CCM Criteria and OVHcloud Controls

Part C: Mapping between the applicable objectives set forth in C5 and OVHcloud Controls

Part D: OVHcloud's Control Description, KPMG's Tests of Controls and KPMG's Results of Tests

The applicable trust services criteria, CCM criteria, objectives set forth in C5, and control activities in Part A, B, C and D are provided by OVHcloud.

OVHcloud's controls within its control environment have been categorized in the following categories:

- GOV: Governance
- PHY: Physical security
- CHG: Change management
- IAM: Identity and access management
- HR: Human resources
- BAC: Backup and restoration
- NET: Network security
- MON: Logging and monitoring activities
- IM: Incident management
- SEC: Logical security
- PCY: Privacy
- THP: Security with third parties
- CUS: Security with customers

2. Part A: Mapping between Applicable Trust Services Criteria and OVHcloud Controls

CONTROL ENVIRONMENT

Ref.	Trust Criteria	OVHcloud Control
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	**HR-01.** OVHcloud has documented an Information and Communication Charter, a Code of Ethics and depending on geographic locations, an Employee Handbook which are reviewed, updated when necessary, and approved by management. Personnel are required to read and accept these documents upon their recruitment. Acceptance of information security policy is formally reaffirmed annually through perimeter membership renewal. Disciplinary measures and sanctions are established for employees who have violated security policies and procedures, internal regulations or the IT charter.
		HR-02. OVHcloud management performs annual performance evaluations of employees where past performance and future developments are assessed and discussed. Annual performance evaluations also include review of skills to be further developed and actions to perform such as training to follow, specific projects to participate in or roles to take up. The performance evaluation is validated by the employee's manager.
		HR-04. Prior to recruitment, a background screening of personnel is performed. Personnel are verified against regulatory screening databases and their experience as well as training are evaluated (if applicable, depending on the country). For third parties, OVHcloud performs a background check of the enterprise during the third parties' audit. Moreover, the third party undertakes the contract signature to perform a background check of its employees.
		IM-04. OVHcloud has a whistle blowing platform available to employees and customers. Management monitors customers and employees' complaints reported via the platform
		THP-01. OVHcloud annually monitors the compliance of service providers with its security requirements and internal policies through annual audits. These audits include: • The review and renewal of service agreements; • Background check on the company providing the service; • Review of provided services and activities; • Review of certificates of the management systems' compliance with international standards (when applicable); Identified violations and deviations are subjected to analysis, evaluation and treatment.

Ref.	Trust Criteria	OVHcloud Control
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	**GOV-04.** Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.
		GOV-07. A procedure for planning and conducting audits is documented and communicated through the intranet. OVHcloud has established a formal audit plan that includes internal and external assessments to validate the implementation and operating effectiveness of OVHcloud control environment and to assess compliance with the relevant and applicable legal, regulatory or contractual requirements as well as compliance with the policies and procedures. The audit results are reviewed during the monthly ISMS meetings for monitoring corrective actions.
		GOV-15. Reporting relationships and organizational structures are defined and reviewed periodically by senior management and adjusted as needed based on changing entity commitments and requirements relevant to security, availability, confidentiality and privacy.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	**GOV-04.** Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.
		GOV-15. Reporting relationships and organizational structures are defined and reviewed periodically by senior management and adjusted as needed based on changing entity commitments and requirements relevant to security, availability, confidentiality and privacy.

Ref.	Trust Criteria	OVHcloud Control
		GOV-17. OVHcloud management has adopted a global information security policy that is communicated to employees, third parties and customers as appropriate. The information security policy describes OVHcloud's objectives, requirements and commitments to information security and refers to specific and detailed security policies that are used as a reference in the implementation of the operational security management system.

Ref.	Trust Criteria	OVHcloud Control
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	**HR-02.** OVHcloud management performs annual performance evaluations of employees where past performance and future developments are assessed and discussed. Annual performance evaluations also include review of skills to be further developed and actions to do so such specific projects or roles to take up or training to follow. The performance evaluation is validated by the manager and the employee. Corrective actions, including training, when necessary, are planned.
		HR-03. OVHcloud provides continued training about its security commitments and requirements for personnel to support the achievement of objectives. Security training includes: • Handling system components and information assets. • Correct behavior in the event of security incidents. Regarding third parties, service providers undertake on the contract signature to train their employees with the training materials provided by OVHcloud.
		HR-04. Prior to recruitment, a background screening of personnel is performed. Personnel are verified against regulatory screening databases and their experience as well as training are evaluated (if applicable, depending on the country). For third parties, OVHcloud performs a background check of the enterprise during the third parties' audit. Moreover, the third party undertakes the contract signature to perform a background check of its employees.
		HR-08. OVHcloud provides security and awareness training to employees based on identified needs and security hot topics. Target group-oriented awareness and training are addressed on a regular basis providing: - best security practices including references to applicable policies and instructions such as programming good practices, training on internal practices for secure infrastructure and on advanced security including current threat situation. - regular security communications and updates on security news as needed. - secure development communications and training.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	**GOV-04.** Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.

Ref.	Trust Criteria	OVHcloud Control
		HR-01. OVHcloud has documented an Information and Communication Charter, a Code of Ethics and depending on geographic locations, an Employee Handbook which are reviewed, updated when necessary, and approved by management. Personnel are required to read and accept these documents upon their recruitment. Acceptance of information security policy is formally reaffirmed annually through perimeter membership renewal. Disciplinary measures and sanctions are established for employees who have violated security policies and procedures, internal regulations or the IT charter.
		HR-02. OVHcloud management performs annual performance evaluations of employees where past performance and future developments are assessed and discussed. Annual performance evaluations also include review of skills to be further developed and actions to do so such specific projects or roles to take up or training to follow. The performance evaluation is validated by the manager and the employee. Corrective actions, including training, when necessary, are planned.
		GOV-21. Information Security and Operations teams hold periodic meetings to monitor and manage respective department's progress or lack thereof as it relates to their achievement of department's responsibilities.
		GOV-15. Reporting relationships and organizational structures are defined and reviewed periodically by senior management and adjusted as needed based on changing entity commitments and requirements relevant to security, availability, confidentiality and privacy.
		HR-06. Employees and service providers have been informed about which responsibilities related to confidentiality, will remain in place when their employment is terminated or changed and for how long.
		GOV-11. OVHcloud's confidentiality commitments and the associated system requirements are documented and reviewed when necessary. These commitments and system requirements as well as their changes are communicated to employees, customers and providers, as appropriate, which must accept them.

Ref.	Trust Criteria	OVHcloud Control
		THP-01. OVHcloud annually monitors the compliance of service providers with its security requirements and internal policies through annual audits. These audits include: • The review and renewal of service agreements; • Background check on the company providing the service; • Review of provided services and activities; • Review of certificates of the management systems' compliance with international standards (when applicable); Identified violations and deviations are subjected to analysis, evaluation and treatment.
		GOV-07. A procedure for planning and conducting audits is documented and communicated through the intranet. OVHcloud has established a formal audit plan that includes internal and external assessments to validate the implementation and operating effectiveness of the OVHcloud control environment and to assess compliance with the relevant and applicable legal, regulatory or contractual requirements as well as compliance with the policies and procedures. The audit results are reviewed during the monthly ISMS meetings for monitoring corrective actions.

COMMUNICATION AND INFORMATION

Ref.	Trust Criteria	OVHcloud Control
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-03. During its ongoing and periodic business planning and budgeting process, management evaluates the need for additional tools and resources to achieve business objectives.
		GOV-07. A procedure for planning and conducting audits is documented and communicated through the intranet. OVHcloud has established a formal audit plan that includes internal and external assessments to validate the implementation and operating effectiveness of the OVHcloud control environment and to assess compliance with the relevant and applicable legal, regulatory or contractual requirements as well as compliance with the policies and procedures. The audit results are reviewed during the monthly ISMS meetings for monitoring corrective actions.
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements;

Ref.	Trust Criteria	OVHcloud Control
		• risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • • backup, business continuity and disaster recovery.
		GOV-17. OVHcloud management has adopted a global information security policy that is communicated to employees, third parties and customers as appropriate. The information security policy describes OVHcloud's objectives, requirements and commitments to information security and refers to specific and detailed security policies that are used as a reference in the implementation of the operational security management system.

Ref.	Trust Criteria	OVHcloud Control
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	**GOV-11.** OVHcloud's confidentiality commitments and the associated system requirements are documented and reviewed when necessary. These commitments and system requirements as well as their changes are communicated to employees, customers and providers, as appropriate, which must accept them.
		GOV-03. During its ongoing and periodic business planning and budgeting process, management evaluates the need for additional tools and resources to achieve business objectives.
		IM-03. Employees, customers and providers have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel. OVHcloud also provides user guides, security alerts and known issues on its websites and client portals with information to improve security knowledge and awareness.
		IM-04. OVHcloud has a whistle blowing platform available to employees and customers. Management monitors customers and employees' complaints reported via the platform.
		GOV-04. Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.
		GOV-17. OVHcloud management has adopted a global information security policy that is communicated to employees, third parties and customers as appropriate. The information security policy describes OVHcloud's objectives, requirements and commitments to information security and refers to specific and detailed security policies that are used as a reference in the implementation of the operational security management system.
		HR-01. OVHcloud has documented an Information and Communication Charter, a Code of Ethics and depending on geographic locations, an Employee Handbook which are reviewed, updated when necessary, and approved by management. Personnel are required to read and accept these documents upon their recruitment. Acceptance of information security policy is formally reaffirmed annually through perimeter membership renewal. Disciplinary measures and sanctions are established for employees who have violated security policies and procedures, internal regulations or the IT charter.

Ref.	Trust Criteria	OVHcloud Control
		GOV-10. OVHcloud posts a description of its system, system boundaries, and system processes on its intranet for employees. Moreover, OVHcloud posts the documentation for the use and configuration of its services on its website for its customers
		HR-03. OVHcloud provides continued training about its security commitments and requirements for personnel to support the achievement of objectives. Security training includes: • Handling system components and information assets; • Correct behavior in the event of security incidents. Regarding third parties, service providers undertake on the contract signature to train their employees with the training materials provided by OVHcloud.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	**GOV-11.** OVHcloud's confidentiality commitments and the associated system requirements are documented and reviewed when necessary. These commitments and system requirements as well as their changes are communicated to employees, customers and providers, as appropriate, which must accept them.
		THP-04. Third-party relationships are formalized with agreements that identify the critical business activities performed by the third party and the security requirements. Moreover, OVHcloud keeps a file for the monitoring of third parties that includes: • Company name; • Address; • Date of contract signature and contract end; • Description of the service; • Responsible contact person at OVHcloud and at the service provider.
		IM-03. Employees, customers and providers have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel. OVHcloud also provides user guides, security alerts and known issues on its websites and client portals with information to improve security knowledge and awareness.
		GOV-17. OVHcloud management has adopted a global information security policy that is communicated to employees, third parties and customers as appropriate. The information security policy describes OVHcloud's objectives, requirements and commitments to information security and refers to specific and detailed security policies that are used as a reference in the implementation of the operational security management system.

Ref.	Trust Criteria	OVHcloud Control
		IM-04. OVHcloud has a whistle blowing platform available to employees and customers. Management monitors customers and employees' complaints reported via the platform.
		GOV-10. OVHcloud posts a description of its system, system boundaries, and system processes on its intranet for employees. Moreover, OVHcloud posts documentation for the use and configuration of its services on its website for its customers.
		HR-03. OVHcloud provides continued training about its security commitments and requirements for personnel to support the achievement of objectives. Security training includes: • Handling system components and information assets; • Correct behavior in the event of security incidents. Regarding third parties, service providers undertake on the contract signature to train their employees with the training materials provided by OVHcloud.
		GOV-14. OVHcloud's security and privacy commitments and changes to these commitments are communicated to customers and are available on OVHcloud's website.
		CHG-06. Planned changes to system components that affect the service availability are communicated to customers through OVHcloud's website. This communication is made 72 hours before the change implementation.

RISK ASSESSMENT

Ref.	Trust Criteria	OVHcloud Control
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-03. During its ongoing and periodic business planning and budgeting process, management evaluates the need for additional tools and resources to achieve business objectives.
		GOV-07. A procedure for planning and conducting audits is documented and communicated through the intranet. OVHcloud has established a formal audit plan that includes internal and external assessments to validate the implementation and operating effectiveness of the OVHcloud control environment and to assess compliance with the relevant and applicable legal, regulatory or contractual requirements as well as compliance with the policies and procedures. The audit results are reviewed during the monthly ISMS meetings for monitoring corrective actions.
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.

Ref.	Trust Criteria	OVHcloud Control
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-03. During its ongoing and periodic business planning and budgeting process, management evaluates the need for additional tools and resources in order to achieve business objectives.
		GOV-07. A procedure for planning and conducting audits is documented and communicated through the intranet. OVHcloud has established a formal audit plan that includes internal and external assessments to validate the implementation and operating effectiveness of the OVHcloud control environment and to assess compliance with the relevant and applicable legal, regulatory or contractual requirements as well as compliance with the policies and procedures. The audit results are reviewed during the monthly ISMS meetings for monitoring corrective actions.
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.

Ref.	Trust Criteria	OVHcloud Control
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		GOV-07. A procedure for planning and conducting audits is documented and communicated through the intranet. OVHcloud has established a formal audit plan that includes internal and external assessments to validate the implementation and operating effectiveness of the OVHcloud control environment and to assess compliance with the relevant and applicable legal, regulatory or contractual requirements as well as compliance with the policies and procedures. The audit results are reviewed during the monthly ISMS meetings for monitoring corrective actions;

Ref.	Trust Criteria	OVHcloud Control
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		GOV-12. OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedures for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.

MONITORING ACTIVITIES

Ref.	Trust Criteria	OVHcloud Control
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	**SEC-02**. Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		GOV-01. A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		GOV-07. A procedure for planning and conducting audits is documented and communicated through the intranet. OVHcloud has established a formal audit plan that includes internal and external assessments to validate the implementation and operating effectiveness of the OVHcloud control environment and to assess compliance with the relevant and applicable legal, regulatory or contractual requirements as well as compliance with the policies and procedures. The audit results are reviewed during the monthly ISMS meetings for monitoring of corrective actions

Ref.	Trust Criteria	OVHcloud Control
		GOV-21. Information Security and Operations teams hold periodic meetings to monitor and manage respective department's progress or lack thereof as it relates to their achievement of department's responsibilities.
		THP-01. OVHcloud annually monitors the compliance of service providers with its security requirements and internal policies through annual audits. These audits include: • The review and renewal of service agreements; • Background check on the company providing the service; • Review of provided services and activities; • Review of certificates of the management systems' compliance with international standards (when applicable); Identified violations and deviations are subjected to analysis, evaluation and treatment.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	**SEC-02.** Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		GOV-01. A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-07. A procedure for planning and conducting audits is documented and communicated through the intranet. OVHcloud has established a formal audit plan that includes internal and external assessments to validate the implementation and operating effectiveness of the OVHcloud control environment and to assess compliance with the relevant and applicable legal, regulatory or contractual requirements as well as compliance with the policies and procedures. The audit results are reviewed during the monthly ISMS meetings for monitoring corrective actions;

Ref.	Trust Criteria	OVHcloud Control
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on a need-to-know basis.
		GOV-21. Information Security and Operations teams hold periodic meetings to monitor and manage respective department's progress or lack thereof as it relates to their achievement of department's responsibilities.

CONTROL ACTIVITIES

Ref.	Trust Criteria	OVHcloud Control
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	**IAM-06.** Business roles are reviewed on a bi-annual basis by the business role owners, ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities.
		GOV-01. A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-03. During its ongoing and periodic business planning and budgeting process, management evaluates the need for additional tools and resources in order to achieve business objectives.
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		GOV-12. OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedures for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program

Ref.	Trust Criteria	OVHcloud Control
		that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	**IAM-08.** Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		IAM-02. Perimeter entrance requires a documented access request and manager approval prior to access being provisioned. Logical access rights within a perimeter are granted by authorized and approved granters based on rules of need to know and least privilege.
		IAM-01. Logical access is revoked in a timely manner as part of the termination process and any assets handed over are provably returned upon termination of employment.
		IAM-06. Business roles are reviewed on a bi-annual basis by the business role owners, ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities.
		GOV-01. A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management;

Ref.	Trust Criteria	OVHcloud Control
		• Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		GOV-12. OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedures for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security;

Ref.	Trust Criteria	OVHcloud Control
		• • backup, business continuity and disaster recovery.
		GOV-17. OVHcloud management has adopted a global information security policy that is communicated to employees, third parties and customers as appropriate. The information security policy describes OVHcloud's objectives, requirements and commitments to information security and refers to specific and detailed security policies that are used as a reference in the implementation of the operational security management system.
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
		MON-05. OVHcloud has documented policies and procedures regarding the logging and monitoring of events on system components, that include: • Operational aspects of logging and monitoring (logs generation, lifecycle, retention, review and alerting); • Time synchronization of system components; and • Compliance with legal and regulatory frameworks.
		MON-06. OVHcloud has documented policies and procedures regarding protection requirements, lifecycle and retention of logs on its systems, that include: • Access only to authorized users and systems; • Backup and retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.
		MON-07. Users access and activities on the production environment are logged by a bastion. Logged information is used to detect events that may indicate misuse. When such an event is identified, the personnel responsible are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.

Ref.	Trust Criteria	OVHcloud Control
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-04. Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		GOV-12. OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedures for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security;

Ref.	Trust Criteria	OVHcloud Control
		• acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.
		GOV-15. Reporting relationships and organizational structures are defined and reviewed periodically by senior management and adjusted as needed based on changing entity commitments and requirements relevant to security, availability, confidentiality and privacy.

LOGICAL AND PHYSICAL ACCESS CONTROLS

Ref.	Trust Criteria	OVHcloud Control
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	**NET-01.** End user and server workload network traffic is segmented to support isolation. Moreover, there are dedicated networks for the administrative management of the infrastructure. These networks are separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication.
		NET-02. Firewall configuration files are automatically promoted to production firewall devices. Thus, firewall rules are regularly reviewed by peers before approving any change in the corresponding configuration files in production, thanks to CI/CD processes and tools.
		NET-03. Intrusion detection systems and other technical measures are implemented to detect and response to network-based attacks, including network monitoring and traffic filtering.
		IAM-04. In-scope system components require unique username, passwords or authorized SSH keys prior to user authentication.
		IAM-01. Logical access is revoked in a timely manner as part of the termination process and any assets handed over are provably returned upon termination of employment.
		IAM-02. Perimeter entrance requires a documented access request and manager approval prior to access being provisioned. Logical access rights within a perimeter are granted by authorized and approved granters based on rules of need to know and least privilege.
		IAM-06. Business roles are reviewed on a bi-annual basis by the business role owners, ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities.
		IAM-07. OVHcloud permits remote access to production systems by authorized employees, using authorized devices, with multi-factor authentication (MFA) and over encrypted virtual private network (VPN) connection.
		IAM-08. Privileged access rights are assigned in accordance with the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.

Ref.	Trust Criteria	OVHcloud Control
		MON-07. Users access and activities on the production environment are logged by a bastion. Logged information is used to detect events that may indicate misuse. When such an event is identified, the personnel responsible are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
		GOV-06. A complete inventory of assets located at all geographical locations is maintained and updated regularly. Moreover, during its risk assessment process, OVHcloud identifies the list of assets which may be impacted by each risk scenario. A Business Impact Assessment (BIA) is performed to quantify the consequences of confidentiality, integrity, or availability loss on the assets impacted by the risk scenario analyzed. The asset's criticality depends on the result of the assessment.
		NET-06. OVHcloud has deployed Transport Layer Security (TLS) for the transmission of confidential and/or sensitive information.
		NET-07. Incoming and outgoing traffic is formally identified and limited to what is strictly necessary according to the firewall rules. System firewalls are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined and validated by the Information Security Operational Referent (ROSI) or appropriate validator.
		SEC-03. Storage for laptops and workstations having access to the production environment is encrypted.
		SEC-04. The use of removable media on workstations is disabled.
		SEC-09. Policies and procedures for data encryption are documented and include: • Usage of strong and trusted encryption procedures and secure network protocols that correspond to the state-of-the-art, such as trusted symmetric encryption algorithms, trusted hashing algorithms, trusted one-way password encryption algorithms, trusted key exchange algorithms, trusted SSL/TLS Protocols and certificates... etc. • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys.
		SEC-10. OVHcloud has documented a key management policy that describes the process of secure key management that includes:

Ref.	Trust Criteria	OVHcloud Control
		• Keys generation in a secure Locker / Vault using trusted and secure algorithms; • Key storage and communication over secure channels; • Key lifecycle and disposal.
		IAM-10. Passwords for in-scope system components are configured according to OVHcloud's password policy.
		NET-09. Virtual hosts are behind software firewalls which are configured to prevent TCP/IP spoofing, packet sniffing, and restrict incoming connections to customer-specified ports.
		IAM-03. Generic accounts are used on OVHcloud servers used to manage the cloud service. Access to and use of the generic accounts is traced in the bastions and users are clearly identifiable. Logs of the usage of generic accounts contain the following information: source IP address, username of the accessor, type of access, request made. In addition, a capture of the session is made and can be replayed. Bastion logs are saved for at least one year.
		IAM-12. OVHcloud has established a secure password configuration policy for in-scope system components that includes: · Restriction on password length and complexity (use of alphanumeric, upper- and lower-case characters); · Password age must not exceed 90 days; · The server-side storage takes place using cryptographically strong hash functions; · Guidelines and instructions on the secure handling and protection of passwords.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	**IAM-03.** Generic accounts are used on OVHcloud servers used to manage the cloud service. Access to and use of the generic accounts is traced in the bastions and users are clearly identifiable. Logs of the usage of generic accounts contain the following information: source IP address, username of the accessor, type of access, request made. In addition, a capture of the session is made and can be replayed. Bastion logs are saved for at least one year.
		IAM-01. Logical access is revoked in a timely manner as part of the termination process and any assets handed over are provably returned upon termination of employment.
		IAM-02. Perimeter entrance requires a documented access request and manager approval prior to access being provisioned. Logical access rights within a perimeter are granted by authorized and approved granters based on rules of need to know and least privilege.

Ref.	Trust Criteria	OVHcloud Control
		IAM-06. Business roles are reviewed on a bi-annual basis by the business role owners, ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities.
		IAM-08. Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		MON-07. Users access and activities on the production environment are logged by a bastion. Logged information is used to detect events that may indicate misuse. When such an event is identified, the personnel responsible are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	**IAM-08.** Privileged access rights are assigned in accordance with the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		IAM-01. Logical access is revoked in a timely manner as part of the termination process and any assets handed over are provably returned upon termination of employment.
		IAM-02. Perimeter entrance requires a documented access request and manager approval prior to access being provisioned. Logical access rights within a perimeter are granted by authorized and approved granters based on rules of need to know and least privilege.
		IAM-06. Business roles are reviewed on a bi-annual basis by the business role owners, ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities.
		MON-07. Users access and activities on the production environment are logged by a bastion. Logged information is used to detect events that may indicate misuse. When such an event is identified, the personnel responsible are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example,	**PHY-05.** Access to the data center is revoked in a timely manner as part of the termination process.

Ref.	Trust Criteria	OVHcloud Control
	data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	**PHY-06.** Access to the datacenter perimeter for employees and third parties requires an access request and manager approval prior to access being provisioned. Once in the perimeter, access to the physical locations according to the person's access rights is granted by authorized and approved granters and is synchronized with the person's badge.
		PHY-07. All personnel are required to wear badges at all times. Visitor badges are clearly distinguishable from employee badges.
		PHY-08. Visitors' access to OVHcloud's datacenters requires approval by the appropriate manager in the access rights management tool before access being granted. A check is performed at the entrance to ensure that the visitor's access is approved.
		PHY-09. A card-based physical access control system is implemented at the entry and exit points of the datacenter and critical areas within the facilities. Two-factor authentication mechanism is used for access to Critical+ areas.
		PHY-14. Mantraps are used for controlling access to the datacenter. For DC Tapes, alternative access security controls are in place including the use of access badges, CCTV monitoring, security guards.
		PHY-16. The logs of access to the data centers are reviewed monthly by management to detect any unauthorized access. The necessary investigations and corrective actions are performed in a timely manner.
		PHY-17. The sharing of access badges and tailgating are prohibited by policy.
		PHY-02. A monitoring process exists to monitor entry and exit points. Measures such as surveillance cameras and trained security guards are adopted. Logs and video surveillance recordings are maintained for an agreed period of time for future reference. For DC Tape Saint-Pierre-des-Corps and DC Tape Villenave d'Ornon, there are no permanent security guards at the entrance of the datacenter. However, physical security measures are implemented, including access control systems and continuous video surveillance, as well as remote security guard who can be contacted at the entrance of the site and who is responsible of the barrier opening and remote monitoring.
		PHY-04. Access points such as delivery and loading areas where unauthorized persons could enter the premises are

Ref.	Trust Criteria	OVHcloud Control
		controlled and isolated from information processing facilities to avoid unauthorized access. For MiniDCs, physical isolation is not feasible. However, security measures such as the use of access badges are implemented to prevent unauthorized access.
		PHY-03. A security level classification system is used to define zones for access security.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	**CUS-01.** When a customer terminates his contract, a logical erasure is performed on all the servers concerned. If this logical erasure fails, the concerned hard drives are destroyed according to a defined secure destruction process.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	**NET-02.** Firewall configuration files are automatically promoted to production firewall devices. Thus, firewall rules are regularly reviewed by peers before approving any change in the corresponding configuration files in production, thanks to CI/CD processes and tools.
		NET-03. Intrusion detection systems and other technical measures are implemented to detect and response to network-based attacks, including network monitoring and traffic filtering.
		NET-06. OVHcloud has deployed Transport Layer Security (TLS) for the transmission of confidential and/or sensitive information.
		MON-01. External access by OVHcloud personnel is logged by the VPN with the following information: accessor IP address, date and event type. Logs are retained for at least 1 year.
		IAM-07. OVHcloud permits remote access to production systems by authorized employees, using authorized devices, with multi-factor authentication (MFA) and over encrypted virtual private network (VPN) connection.
		NET-07. Incoming and outgoing traffic is formally identified and limited to what is strictly necessary according to the firewall rules. System firewalls are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined and validated by the Information Security Operational Referent (ROSI) or appropriate validator.
		NET-13. OVHcloud permits the connection to its internal network via VPN and only to authorized equipment using host-based certificates.
		NET-01. End user and server workload network traffic is segmented to support isolation. Moreover, there are

Ref.	Trust Criteria	OVHcloud Control
		dedicated networks for the administrative management of the infrastructure. These networks are separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication.
		MON-03. Activity logs on the administration infrastructure are centralized on dedicated syslog servers and are automatically monitored according to defined scenarios to detect potential security events. Detected events are raised through alerts to the appropriate departments for investigation and corrective action. Access logs on the bastions are monitored automatically, and alerts are raised when suspicious events occur according to predefined patterns. Investigations and corrective actions are performed in a timely manner.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	**NET-01.** End user and server workload network traffic is segmented to support isolation. Moreover, there are dedicated networks for the administrative management of the infrastructure. These networks are separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication.
		NET-03. Intrusion detection systems and other technical measures are implemented to detect and response to network-based attacks, including network monitoring and traffic filtering.
		PHY-24. The transfer of equipment to offsite locations is tracked on the system and by the edition of transfer vouchers allowing to identify the transferred equipment. The edition of transfer vouchers is restricted to the storekeepers.
		GOV-06. A complete inventory of assets located at all geographical locations is maintained and updated regularly. Moreover, during its risk assessment process, OVHcloud identifies the list of assets which may be impacted by each risk scenario. A Business Impact Assessment (BIA) is performed to quantify the consequences of confidentiality, integrity, or availability loss on the assets impacted by the risk scenario analyzed. The asset's criticality depends on the result of the assessment.
		NET-06. OVHcloud has deployed Transport Layer Security (TLS) for the transmission of confidential and/or sensitive information.
		GOV-09. OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices;

Ref.	Trust Criteria	OVHcloud Control
		• Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.
		SEC-03. Storage for laptops and workstations having access to the production environment is encrypted.
		SEC-04. The use of removable media on workstations is disabled.
		IAM-07. OVHcloud permits remote access to production systems by authorized employees, using authorized devices, with multi-factor authentication (MFA) and over encrypted virtual private network (VPN) connection.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	**SEC-01.** OVHcloud's procedures on antivirus and anti-malware protection are documented and communicated through its intranet. An antivirus and anti-malware program is implemented and kept updated on workstations and laptops to provide for the interception or detection and remediation of malware.
		SEC-02. Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		SEC-06. OVHcloud uses CVSS (Common Vulnerability Scoring System) for the scoring of vulnerabilities and relies on the online NIST database as well as other sources for the discovery of vulnerabilities. Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities are based on a list of assets ordered by criticality that relies on product-specific criteria for each Public Cloud product. Security patches are then deployed within a timeframe based on asset criticality.
		SEC-07. Employees can only install trusted software available in defined stores for MAC, Windows and Linux workstations and laptops.
		CHG-02. OVHcloud requires all changes, including maintenance activities, to be documented and tracked from

Ref.	Trust Criteria	OVHcloud Control
		initiation through change validation and deployment. Moreover, OVHcloud has deployed a SIEM solution that allows operation teams to monitor configuration files changes and other changes in the production environment.
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on a need-to-know basis.
		SEC-05. System components used to provide the services on the Public Cloud perimeter are hardened according to generally accepted industry standards. The use of a hardened operating system known as the Hardened Debian distribution provided by Digit Core (based on CIS configuration) is encouraged. Moreover, for CI/CD, the use of collaborative tools like Puppet or Bitbucket is mandatory to ensure versioning or integrity monitoring.
		MON-03. Activity logs on the administration infrastructure are centralized on dedicated syslog servers and are automatically monitored according to defined scenarios to detect potential security events. Detected events are raised through alerts to the appropriate departments for investigation and corrective action. Access logs on the bastions are monitored automatically, and alerts are raised when suspicious events occur according to predefined patterns. Investigations and corrective actions are performed in a timely manner.

SYSTEM OPERATIONS

Ref.	Trust Criteria	OVHcloud Control
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	**SEC-02.** Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		CHG-02. OVHcloud requires all changes, including maintenance activities, to be documented and tracked from initiation through change validation and deployment. Moreover, OVHcloud has deployed a SIEM solution that allows operation teams to monitor configuration files changes and other changes in the production environment.
		SEC-05. System components used to provide the services on the Public Cloud perimeter are hardened according to generally accepted industry standards. The use of a hardened operating system known as the Hardened Debian distribution provided by Digit Core (based on CIS configuration) is encouraged. Moreover, for CI/CD, the use of collaborative tools like Puppet or Bitbucket is mandatory to ensure versioning or integrity monitoring.
		CHG-09. OVHcloud uses dedicated tools for source code management and software deployment into production. Each developer has specific access to the repositories and all changes are logged.
		SEC-06. OVHcloud uses CVSS (Common Vulnerability Scoring System) for the scoring of vulnerabilities and relies on the online NIST database as well as other sources for the discovery of vulnerabilities. Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities are based on a list of assets ordered by criticality that relies on product-specific criteria for each Public Cloud product. Security patches are then deployed within a timeframe based on asset criticality.
		CHG-07. OVHcloud has documented policies and procedures for the secure development process that include review and approval, testing, implementation and maintenance.
		MON-05. OVHcloud has documented policies and procedures regarding the logging and monitoring of events on system components, that include: • Operational aspects of logging and monitoring (logs generation, lifecycle, retention, review and alerting);

Ref.	Trust Criteria	OVHcloud Control
		• Time synchronization of system components; and • Compliance with legal and regulatory frameworks.
		MON-03. Activity logs on the administration infrastructure are centralized on dedicated syslog servers and are automatically monitored according to defined scenarios to detect potential security events. Detected events are raised through alerts to the appropriate departments for investigation and corrective action. Access logs on the bastions are monitored automatically, and alerts are raised when suspicious events occur according to predefined patterns. Investigations and corrective actions are performed in a timely manner.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	**NET-03.** Intrusion detection systems and other technical measures are implemented to detect and response to network-based attacks, including network monitoring and traffic filtering.
		SEC-01. OVHcloud's procedures on antivirus and anti-malware protection are documented and communicated through its intranet. An antivirus and anti-malware program is implemented and kept updated on workstations and laptops to provide for the interception or detection and remediation of malware.
		SEC-02. Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		PHY-11. Detection measures and alerts that are communicated to personnel are implemented to identify anomalies that could result from environmental threat events.
		IM-04. OVHcloud has a whistle blowing platform available to employees and customers. Management monitors customers and employees' complaints reported via the platform.
		IM-03. Employees, customers and providers have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel. OVHcloud also provides user guides, security alerts and known issues on its websites and client portals with information to improve security knowledge and awareness.

Ref.	Trust Criteria	OVHcloud Control
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on a need-to-know basis.
		MON-05. OVHcloud has documented policies and procedures regarding the logging and monitoring of events on system components, that include: • Operational aspects of logging and monitoring (logs generation, lifecycle, retention, review and alerting); • Time synchronization of system components; and • Compliance with legal and regulatory frameworks.
		MON-03. Activity logs on the administration infrastructure are centralized on dedicated syslog servers and are automatically monitored according to defined scenarios to detect potential security events. Detected events are raised through alerts to the appropriate departments for investigation and corrective action. Access logs on the bastions are monitored automatically, and alerts are raised when suspicious events occur according to predefined patterns. Investigations and corrective actions are performed in a timely manner.
		MON-04. As part of its monitoring processes, OVHcloud monitors the logging and monitoring components to detect any failure that could cause the logging to stop or that could alter the logs. Failures are automatically reported, and corrective actions are taken in a timely manner.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer);

Ref.	Trust Criteria	OVHcloud Control
		• Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		IM-02. On an annual basis, a crisis unit simulation is performed to ensure the incident response procedures are up-to-date and accurate. When updating the incident response plan, lessons learned are used to implement changes to ensure that incident response procedures are effective.
		IM-03. Employees, customers and providers have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel. OVHcloud also provides user guides, security alerts and known issues on its websites and client portals with information to improve security knowledge and awareness.
		IM-04. OVHcloud has a whistle blowing platform available to employees and customers. Management monitors customers and employees' complaints reported via the platform.
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on a need-to-know basis.
		IM-01. After a security incident has been identified and analyzed for root cause analysis and impact, the action plan is carried out and documented. In the case, the security incident has an impact on the cloud services, communication is sent to the affected customers. The security incident is formalized within a post-mortem detailing all security incident processing steps.

Ref.	Trust Criteria	OVHcloud Control
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	**SEC-02.** Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		IM-01. After a security incident has been identified and analyzed for root cause analysis and impact, the action plan is carried out and documented. In the case, the security incident has an impact on the cloud services, communication is sent to the affected customers. The security incident is formalized within a post-mortem detailing all security incident processing steps.
		IM-02. On an annual basis, a crisis unit simulation is performed to ensure the incident response procedures are up-to-date and accurate. When updating the incident response plan, lessons learned are used to implement changes to ensure that incident response procedures are effective.
		PCY-02. Events that resulted in unauthorized use or disclosure of personal information are communicated to the data subjects, legal and regulatory authorities, and others as required.
		GOV-04. Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; backup, business continuity and disaster recovery.

Ref.	Trust Criteria	OVHcloud Control
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on a need-to-know basis.
		CHG-06. Planned changes to system components that affect the service availability are communicated to customers through OVHcloud's website. This communication is made 72 hours before the change implementation.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	**IM-01.** After a security incident has been identified and analyzed for root cause analysis and impact, the action plan is carried out and documented. In the case, the security incident has an impact on the cloud services, communication is sent to the affected customers. The security incident is formalized within a post-mortem detailing all security incident processing steps.
		IM-02. After a security incident has been identified and analyzed for root cause analysis and impact, the action plan is carried out and documented. In the case, the security incident has an impact on the cloud services, communication is sent to the affected customers. The security incident is formalized within a post-mortem detailing all security incident processing steps.
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.

Ref.	Trust Criteria	OVHcloud Control
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on a need-to-know basis.

CHANGE MANAGEMENT

Ref.	Trust Criteria	OVHcloud Control
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	**CHG-01.** OVHcloud protects confidential and personal information during system design, development, testing, implementation and change processes to meet the OVHcloud's objectives related to confidentiality and privacy.
		CHG-02. OVHcloud requires all changes, including maintenance activities, to be documented and tracked from initiation through change validation and deployment. Moreover, OVHcloud has deployed a SIEM solution that allows operation teams to monitor configuration files changes and other changes in the production environment
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
		CHG-04. Separate environments are used for development and production. Moreover, data contained in the production environments is not used in development environments in order not to compromise their confidentiality.
		CHG-05. During the development process, all pull requests must be approved by at least one peer reviewer before being pushed to production.
		CHG-09. OVHcloud uses dedicated tools for source code management and software deployment into production. Each developer has specific access to the repositories and all changes are logged.
		HR-08. OVHcloud provides security and awareness training to employees based on identified needs and security hot topics. Target group-oriented awareness and training are addressed on a regular basis providing: • best security practices including references to applicable policies and instructions such as programming good practices, training on internal practices for secure infrastructure and on advanced security including current threat situation; • regular security communications and updates on security news as needed;

Ref.	Trust Criteria	OVHcloud Control
		• secure development communications and training.
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on a need-to-know basis.
		SEC-05. System components used to provide the services on the Public Cloud perimeter are hardened according to generally accepted industry standards. The use of a hardened operating system known as the Hardened Debian distribution provided by Digit Core (based on CIS configuration) is encouraged. Moreover, for CI/CD, the use of collaborative tools like Puppet or Bitbucket is mandatory to ensure versioning or integrity monitoring.
		CHG-07. OVHcloud has documented policies and procedures for the secure development process that include review and approval, testing, implementation and maintenance.

RISK MITIGATION

Ref.	Trust Criteria	OVHcloud Control
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.

Ref.	Trust Criteria	OVHcloud Control
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	**GOV-11.** OVHcloud's confidentiality commitments and the associated system requirements are documented and reviewed when necessary. These commitments and system requirements as well as their changes are communicated to employees, customers and providers, as appropriate, which must accept them.
		GOV-01. A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		THP-01. OVHcloud annually monitors the compliance of service providers with its security requirements and internal policies through annual audits. These audits include: • The review and renewal of service agreements; • Background check on the company providing the service; • Review of services provided and activities; • Review of certificates of the management systems' compliance with international standards (when applicable); Identified violations and deviations are subjected to analysis, evaluation and treatment.
		THP-02. OVHcloud has clauses in its agreements with providers to terminate relationships when necessary.
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		THP-05. A security policy with third parties has been implemented by OVHcloud that includes:

Ref.	Trust Criteria	OVHcloud Control
		• Signature of agreements with third parties that define business activities and security requirements; • Background check of third parties; • Audit and monitoring of third parties; • Security training and awareness of third parties.
		THP-04. Third-party relationships are formalized with agreements that identify the critical business activities performed by the third party and the security requirements. Moreover, OVHcloud keeps a file for the monitoring of third parties that includes: • Company name; • Address; • Date of contract signature and contract end; • Description of the service; • Responsible contact person at OVHcloud and at the service provider.
		THP-03. OVHcloud limits the risk related to the intervention of service providers in the perimeter of its provided services and products. Service providers do not contribute to the processes of development, change and incident management of the services provided by OVHcloud and thus do not have access to confidential information. If a third party develops software for a perimeter, a development guideline based on OWASP is provided to them and their employees must be trained accordingly.

ADDITIONAL CRITERIA FOR AVAILABILITY

Ref.	Trust Criteria	OVHcloud Control
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	**MON-02.** Use of system components is monitored against acceptable tolerance levels using dedicated tools. Moreover, provisioning and de-provisioning of cloud services are monitored continuously to adapt hardware orders and equipment availability. Actual capacity and service provision levels are monitored according to specificities of teams and products.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	**BAC-02.** Procedures for data backup and recovery are documented and include the frequency of data backup as well as the data retention duration. Backups are performed and monitored using an automated system and corrective actions are taken in a timely manner in case of anomaly.
		GOV-01. A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-02. A business continuity plan is documented for the Public Cloud perimeter that describes: • The key architecture components and systems; • The high availability, backup and recovery mechanisms for these components; • Tests of high availability, backup and recovery mechanisms when applicable. In case of major incident, the incident management process is followed, and the crisis unit is triggered.
		BAC-03. For each Public Cloud product, the redundancy model is based on risk assessment, technical specifications and operational constraints. These elements define the choices for replication locally or at remote sites and the different possible failure scales (network, room, DC).

Ref.	Trust Criteria	OVHcloud Control
		The infrastructure of Public Cloud products is based on scalability and Software Design Storage principles, meaning that the configuration of the control plane can change at will, depending on the customers' needs and the technical constraints. Moreover, as the control planes use stateless components, they can be created or modified by simply redeploying the altered components from the code repositories. Geo-redundancy of the control plane is assured for most Public Cloud products on two locations at least (Compute, Block Storage, Kubernetes and Data). On the other side, Object Storage is a mono-datacenter offer, that does not provide yet geo-redundancy of the control plane. However, resilience is assured thanks to the OpenIO and Swift software model.
		BAC-04. The ability to modify backup schedules is restricted to the authorized personnel.
		PHY-11. Detection measures and alerts that are communicated to personnel are implemented to identify anomalies that could result from environmental threat events.
		PHY-12. Environmental protection has been installed including the following: • Cooling systems, • Air conditioning units, • Redundant communications lines, • Fire extinguishers, • Smoke detectors, • Redundant electric arrival, • UPS, Diesel generator.
		PHY-13. Datacenter equipment receives maintenance on at least an annual basis. Generators are tested every 30 days and corrective action is taken by the data center manager. *The following equipment is maintained every 3 years which are: the High Voltage Cell, TGBT, the HTA/BT transformer and the fire doors.
		PHY-18. Power and telecommunications cabling carrying data or supporting information services are protected from interception, interference or damage. Where physical protection of cabling is not feasible (e.g., in some DC Tapes), logical controls and encryption are implemented as compensating measures. The 4 DC Tapes work together and are designed to compensate for the complete or partial loss of power or communication for two of them at the same time, without interrupting the service and while maintaining the protection of customer data.

Ref.	Trust Criteria	OVHcloud Control
		PHY-19. The datacenters interior layout has been designed for the purpose of maximum prevention.
		PHY-20. Security guards perform a shift round to inspect the facility and document any abnormal incidents. If not, distant security guards monitor the facility H24 7/7 through CCTV and on-site technicians make the ambiguity resolution.
		PHY-21. Datacenter staff use the monitoring system to monitor datacenter equipment such as UPS, cooling and air conditioning equipment, etc. Room temperature and humidity levels are also monitored.
		PHY-02. A monitoring process exists to monitor entry and exit points. Measures such as surveillance cameras and trained security guards are adopted. Logs and video surveillance recordings are maintained for an agreed period of time for future reference. For DC Tape Saint-Pierre-des-Corps and DC Tape Villenave d'Ornon, there are no permanent security guards at the entrance of the datacenter. However, physical security measures are implemented, including access control systems and continuous video surveillance, as well as remote security guard who can be contacted at the entrance of the site and who is responsible of the barrier opening and remote monitoring.
		PHY-15. Security perimeters are defined and used to protect areas that contain either restricted or critical information and processing facilities. The outer doors, windows and other construction elements reach a level appropriate to the security requirements. The surrounding wall constructions as well as the locking mechanisms meet the associated requirements.
		PHY-23. Measures have been implemented by OVHcloud to prevent the failure of cooling and power supplies, including: • Appropriate redundancy of power arrivals; • Appropriate redundancy of cooling and air conditioning systems; • Use of alternative power supplies such as UPS and generators; Regular maintenance of the equipment in accordance with the manufacturer's recommendations.
		PHY-22. OVHcloud has implemented structural, technical and organizational measures for protection against fire and smoke. These measures include: • Fire and smoke detection systems; • Fire extinguishers located in accessible spots and periodically checked and maintained; Regular fire protection exercises.

Ref.	Trust Criteria	OVHcloud Control
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	**BAC-01.** Backup restoration tests are performed at least annually for internal data related to the Public Cloud solution administration. Potential errors are immediately investigated and corrected during restoration tests.
		GOV-20 Business continuity mechanisms are reviewed and tested at least annually or after significant organizational or environmental changes. The tests are documented, and results are considered for future operational continuity measures.
		PHY-13. Datacenter equipment receives maintenance on at least an annual basis. Generators are tested every 30 days and corrective action is taken by the data center manager. *The following equipment are maintained every 3 years, which are: the High Voltage Cell, TGBT, the HTA/BT transformer and the fire doors.
		PHY-22. OVHcloud has implemented structural, technical and organizational measures for protection against fire and smoke. These measures include: • Fire and smoke detection systems; • Fire extinguishers located in accessible spots and periodically checked and maintained; Regular fire protection exercises.
		IM-02. On an annual basis, a crisis unit simulation is performed to ensure the incident response procedures are up-to-date and accurate. When updating the incident response plan, lessons learned are used to implement changes to ensure that incident response procedures are effective.

ADDITIONAL CRITERIA FOR CONFIDENTIALITY

Ref.	Trust Criteria	OVHcloud Control
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	**CHG-01.** OVHcloud protects confidential and personal information during system design, development, testing, implementation and change processes to meet the OVHcloud's objectives related to confidentiality and privacy.
		CUS-01. When a customer terminates his contract, a logical erasure is performed on all the servers concerned. If this logical erasure fails, the concerned hard drives are destroyed according to a defined secure destruction process.
		CUS-03. OVHcloud deletes customer data following termination of the customer's contract
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	**CUS-01.** When a customer terminates his contract, a logical erasure is performed on all the servers concerned. If this logical erasure fails, the concerned hard drives are destroyed according to a defined secure destruction process.
		CUS-03. OVHcloud deletes customer data following termination of the customer's contract.

ADDITIONAL CRITERIA FOR PRIVACY

Ref.	Trust Criteria	OVHcloud Control
P1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.	**GOV-14.** OVHcloud's security and privacy commitments and changes to these commitments are communicated to customers and are available on OVHcloud's website.
		PCY-04. A data protection agreement is provided to data subjects, which addresses the following topics: • Purpose for collecting personal information • Choice and consent • Types of personal information collected • Methods of collection • Use, retention, and disposal • Access • Disclosure to third parties • Security for privacy
		PCY-05. An objective description of the activities covered is included in OVHcloud's Privacy policy.
		PCY-06. Notice is provided by OVHcloud to data subjects before the time personal information is collected on its website.
P2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	**PCY-07.** Data subjects are informed about the choices available to them with respect to the collection, use and disclosure of personal information for which OVHcloud is controller. Moreover, OVHcloud obtains consent from data subjects before personal information is collected on its website. Documentation of explicit consent is retained in accordance with objectives related to privacy.
P3.1	Personal information is collected consistently with the entity's objectives related to privacy.	**PCY-08.** The collection, use and disclosure of personal information is limited to that necessary to meet OVHcloud's objectives.
P3.2	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.	**PCY-07.** Data subjects are informed about the choices available to them with respect to the collection, use and disclosure of personal information for which OVHcloud is controller. Moreover, OVHcloud obtains consent from data subjects before personal information is collected on its website. Documentation of explicit consent is retained in accordance with objectives related to privacy.

Ref.	Trust Criteria	OVHcloud Control
		PCY-20. Personal information is disclosed only to third parties who have agreements with OVHcloud to protect personal information in a manner consistent with OVHcloud's privacy requirements. OVHcloud has procedures in place to evaluate that the third parties meet these requirements. Moreover, personal information is disclosed only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject.
P4.1	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.	**PCY-08.** The collection, use and disclosure of personal information is limited to that necessary to meet OVHcloud's objectives.
P4.2	The entity retains personal information consistent with the entity's objectives related to privacy.	**PCY-09.** Personal information is retained for no longer than necessary to fulfill the stated purposes, unless a law or regulation specifically requires otherwise.
		PCY-10. OVHcloud has designed and implemented policies and procedures to protect personal information from erasure or destruction during the specified retention period of the information.
P4.3	The entity securely disposes of personal information to meet the entity's objectives related to privacy.	**PCY-11.** Requests for deletion of personal information are captured, and information related to the requests is identified and flagged for destruction to meet OVHcloud's objectives related to privacy.
		PCY-12. OVHcloud destroys personal information that is no longer retained. Policies and procedures are implemented to erase or otherwise destroy personal information in a manner that prevents loss, theft, misuse, or unauthorized access.
P5.1	The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	**PCY-01.** Data subjects can determine whether OVHcloud maintains personal information about them and may obtain access to and update their personal information. When data access is denied, data subjects are informed, in writing, of the reason a request was denied.
		PCY-13. The identity of data subjects who request access to their personal information is authenticated before they are given access to that information. Personal information is provided to data subjects in an understandable form, in a reasonable time frame.
P5.2	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's	**PCY-01.** Data subjects can determine whether OVHcloud maintains personal information about them and may obtain access to and update their personal information. When data access is denied, data subjects are informed, in writing, of the reason a request was denied.

Ref.	Trust Criteria	OVHcloud Control
	objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	**PCY-20.** Personal information is disclosed only to third parties who have agreements with OVHcloud to protect personal information in a manner consistent with OVHcloud's privacy requirements. OVHcloud has procedures in place to evaluate that the third parties meet these requirements. Moreover, personal information is disclosed only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject.
P6.3	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.	**PCY-14.** OVHcloud maintains a record of detected unauthorized disclosures of personal information that is complete, accurate, and timely.
P6.4	The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	**PCY-15.** OVHcloud takes remedial action in response to misuse of personal data by a third party to whom OVHcloud has transferred such information.
		PCY-20. Personal information is disclosed only to third parties who have agreements with OVHcloud to protect personal information in a manner consistent with OVHcloud's privacy requirements. OVHcloud has procedures in place to evaluate that the third parties meet these requirements. Moreover, personal information is disclosed only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject.
		CUS-15. During the process of subscribing to a Public Cloud, customers must accept the general terms of service and the specific terms of the Public Cloud offer. The general and specific terms of service describe the service, security and contractual commitments and requirements.
P6.5	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.	**PCY-15.** OVHcloud takes remedial action in response to misuse of personal data by a third party to whom OVHcloud has transferred such information.
		PCY-20. Personal information is disclosed only to third parties who have agreements with OVHcloud to protect personal information in a manner consistent with OVHcloud's privacy requirements. OVHcloud has procedures in place to evaluate that the third parties meet these requirements. Moreover, personal information is disclosed only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject.

Ref.	Trust Criteria	OVHcloud Control
P6.6	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.	**PCY-02.** Events that resulted in unauthorized use or disclosure of personal information are communicated to the data subjects, legal and regulatory authorities, and others as required.
		PCY-15. OVHcloud takes remedial action in response to misuse of personal data by a third party to whom OVHcloud has transferred such information.
P6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.	**PCY-03.** OVHcloud records customers' access requests to their personal information to maintain a complete, accurate, and timely record of such requests.
		PCY-16. The processes, systems, and third parties involved in the handling of personal information are identified.
P7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	**PCY-21.** Personal information is accurate, complete and relevant for the purposes for which it is to be used.
P8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.	**IM-03.** Employees, customers and providers have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel. OVHcloud also provides user guides, security alerts and known issues on its websites and client portals with information to improve security knowledge and awareness.
		PCY-17. OVHcloud has a process in place to address inquiries, complaints, and disputes raised by customers or legal authorities. Each complaint is addressed, and the resolution is documented and communicated to the individual.
		PCY-18. OVHcloud's top management follows-up annually on the progress of the GDPR program in order to ensure compliance with privacy objectives.
		PCY-19. OVHcloud performs ongoing procedures for monitoring the effectiveness of controls over personal information and for taking timely corrective actions when necessary.

3. Part B: Mapping between the applicable objectives set forth in C5 and OVHcloud Controls

AIS: Application & Interface Security, Application Security

Ref.	CCM Criteria	OVHcloud Control
AIS-01	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	**CUS-04.** OVHcloud has developed application programming interfaces (API) allowing its customers to interact with OVHcloud products without using the graphical customer interface. The interfaces are clearly documented for subject matter experts on how they can be used to retrieve the data. The interfaces use the RESTful standard and can be used with different programming languages.
		HR-08. OVHcloud provides security and awareness training to employees based on identified needs and security hot topics. Target group-oriented awareness and training are addressed on a regular basis providing: • best security practices including references to applicable policies and instructions such as programming good practices, training on internal practices for secure infrastructure and on advanced security including current threat situation; • regular security communications and updates on security news as needed; • secure development communications and training.
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
		CHG-07. OVHcloud has documented policies and procedures for the secure development process that include review and approval, testing, implementation and maintenance.

AAC: Audit Assurance & Compliance

Ref.	CCM Criteria	OVHcloud Control
AIS-02	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	**CUS-15.** During the process of subscribing to a Public Cloud, customers must accept the general terms of service and the specific terms of the Public Cloud offer. The general and specific terms of service describe the service, security and contractual commitments and requirements.
AAC-01	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	**GOV-07.** A procedure for planning and conducting audits is documented and communicated through the intranet. OVHcloud has established a formal audit plan that includes internal and external assessments to validate the implementation and operating effectiveness of OVHcloud control environment and to assess compliance with the relevant and applicable legal, regulatory or contractual requirements as well as compliance with the policies and procedures. The audit results are reviewed during the monthly ISMS meetings for monitoring of corrective actions.
AAC-02	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	**SEC-02.** Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		GOV-07. A procedure for planning and conducting audits is documented and communicated through the intranet. OVHcloud has established a formal audit plan that includes internal and external assessments to validate the implementation and operating effectiveness of OVHcloud control environment and to assess compliance with the relevant and applicable legal, regulatory or contractual requirements as well as compliance with the policies and procedures. The audit results are reviewed during the monthly ISMS meetings for monitoring of corrective actions.
		IAM-06. Business roles are reviewed on a bi-annual basis by the business role owners ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities.
		PHY-16. The logs of access to the data centers are reviewed monthly by management in order to detect any unauthorized access. The necessary investigations and corrective actions are performed in a timely manner.

Ref.	CCM Criteria	OVHcloud Control
		GOV-21. Information Security and Operations teams hold periodic meetings to monitor and manage respective department's progress or lack thereof as it relates to their achievement of department's responsibilities.
		GOV-03. During its ongoing and periodic business planning and budgeting process, management evaluates the need for additional tools and resources in order to achieve business objectives.
		GOV-01. A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		GOV-12. OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedures for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.

Ref.	CCM Criteria	OVHcloud Control
AAC-03	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.

BCR: Business Continuity Management & Operational Resilience

Ref.	CCM Criteria	OVHcloud Control
BCR-01	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	**GOV-02.** A business continuity plan is documented for the Public Cloud perimeter that describes: • The key architecture components and systems; • The high availability, rescue and takeover mechanisms for these components ; • Tests of the high availability, rescue and takeover mechanisms for these components when applicable. In case of major incident, the incident management process is followed and the crisis unit is triggered.
		GOV-20 Business continuity mechanisms are reviewed and tested at least annually or after significant organizational or environmental changes. The tests are documented and results are taken into account for future operational continuity measures.
BCR-02	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	**BAC-01.** Backup restoration tests are performed at least annually for internal data related to the Public Cloud solution administration. Potential errors are immediately investigated and corrected during restoration tests.
		IM-02. On an annual basis, a crisis unit simulation is performed to ensure the incident response procedures are up-to-date and accurate. When updating the incident response plan, lessons learned are used to implement changes to ensure that incident response procedures are effective.
		GOV-20 Business continuity mechanisms are reviewed and tested at least annually or after significant organizational or environmental changes. The tests are documented and results are taken into account for future operational continuity measures.
		PHY-13. Datacenter equipment receives maintenance on at least an annual basis. Generators are tested every 30 days and corrective action taken by the data center manager. *The following equipment are maintained every 3 years which are: the High Voltage Cell, TGBT, the HTA/BT transformer and the fire doors.
BCR-03	Data center utilities services and environmental conditions (e.g., water, power,	**PHY-11.** Detection measures and alerts that are communicated to personnel are implemented to identify

Ref.	CCM Criteria	OVHcloud Control
	temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	anomalies that could result from environmental threat events.
		PHY-12. Environmental protections have been installed including the following: • Cooling systems, • Air conditioning units, • Redundant communications lines, • Fire extinguishers, • Smoke detectors, • Redundant electric arrival, • UPS, • Diesel generator.
		PHY-13. Datacenter equipment receives maintenance on at least an annual basis. Generators are tested every 30 days and corrective action taken by the data center manager. *The following equipment are maintained every 3 years which are: the High Voltage Cell, TGBT, the HTA/BT transformer and the fire doors.
		PHY-18. Power and telecommunications cabling carrying data or supporting information services are protected from interception, interference or damage. Where physical protection of cabling is not feasible (e.g., in some DC Tapes), logical controls and encryption are implemented as compensating measures. The 4 DC Tapes work together and are designed to compensate for the complete or partial loss of power or communication for two of them at the same time, without interrupting the service and while maintaining the protection of customer data.
		PHY-19. The datacenters interior layout has been designed for the purpose of maximum prevention.
		PHY-20. Security guards perform a shift round to inspect the facility and document any abnormal incidents. If not, distant security guards monitor the facility H24 7/7 through CCTV and on-site technicians make the ambiguity resolution.
		PHY-21. Datacenter staff use the monitoring system to monitor datacenter equipment such as UPS, cooling and air conditioning equipment, etc. Room temperature and humidity levels are also monitored.
		PHY-22. OVHcloud has implemented structural, technical and organizational measures for protection against fire and smoke. These measures include: • Fire and smoke detection systems; • Fire extinguishers located in accessible spots and periodically checked and maintained; Regular fire protection exercises.

Ref.	CCM Criteria	OVHcloud Control
		PHY-23. Measures have been implemented by OVHcloud to prevent the failure of cooling and power supplies, including: • Appropriate redundancy of power arrivals; • Appropriate redundancy of cooling and air conditioning systems; • Use of alternative power supplies such as UPS and generators; Regular maintenance of the equipment in accordance with the manufacturer's recommendations.
		PHY-04. Access points such as delivery and loading areas where unauthorized persons could enter the premises are controlled and isolated from information processing facilities to avoid unauthorized access. For MiniDCs, physical isolation is not feasible. However, security measures such as the use of access badges are implemented to prevent unauthorized access.
		PHY-15. Security perimeters are defined and used to protect areas that contain either restricted or critical information and processing facilities. The outer doors, windows and other construction elements reach a level appropriate to the security requirements. The surrounding wall constructions as well as the locking mechanisms meet the associated requirements.
BCR-04	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	**GOV-10.** OVHcloud posts a description of its system, system boundaries, and system processes on its intranet for employees. Moreover, OVHcloud posts the documentation for the use and configuration of its services on its website for its customers.
BCR-05	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	**BAC-03.** For each Public Cloud product, the redundancy model is based on risk assessment, technical specifications and operational constraints. These elements define the choices for replication locally or at remote sites and the different possible failure scales (network, room, DC). The infrastructure of Public Cloud products is based on scalability and Software Design Storage principles, meaning that the configuration of the control plane can change at will, depending on the customers needs and the technical constraints. Moreoever, as the control planes use stateless components, they can be created or modified by simply redeploying the altered components from the code repositories. Geo-redundancy of the control plane is assured for most Public Cloud products on two locations at least (Compute, Block Storage, Kubernetes and Data). On the other side, Object Storage is a mono-datacenter offer, that does not

Ref.	CCM Criteria	OVHcloud Control
		provide yet geo-redundacy of the control plane. However, resilience is assured thanks to the OpenIO and Swift software model.
		PHY-02. A monitoring process exists to monitor entry and exit points. Measures such as surveillance cameras and trained security guards are adopted. Logs and video surveillance recordings are maintained for an agreed period of time for future reference. For DC Tape Saint-Pierre-des-Corps and DC Tape Villenave d'Ornon, there are no permanent security guards at the entrance of the datacenter. However, physical security measures are implemented, including access control systems and continuous video surveillance, as well as remote security guard who can be contacted at the entrance of the site and who is responsible of the barrier opening and remote monitoring.
		GOV-01. A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		PHY-03. A security level classification system is used to define zones for access security.
		PHY-04. Access points such as delivery and loading areas where unauthorized persons could enter the premises are controlled and isolated from information processing facilities to avoid unauthorized access. For MiniDCs, physical isolation is not feasible. However, security measures such as the use of access badges are implemented to prevent unauthorized access.
		PHY-11. Detection measures and alerts that are communicated to personnel are implemented to identify anomalies that could result from environmental threat events.
		PHY-12. Environmental protections have been installed including the following:

Ref.	CCM Criteria	OVHcloud Control
		• Cooling systems, • Air conditioning units, • Redundant communications lines, • Fire extinguishers, • Smoke detectors, • Redundant electric arrival, • UPS, • Diesel generator.
		PHY-13. Datacenter equipment receives maintenance on at least an annual basis. Generators are tested every 30days and corrective action taken by the data center manager. *The following equipment are maintained every 3 years which are the High Voltage Cell, TGBT, the HTA/BT transformer and the fire doors.
		PHY-18. Power and telecommunications cabling carrying data or supporting information services are protected from interception, interference or damage. Where physical protection of cabling is not feasible (e.g., in some DC Tapes), logical controls and encryption are implemented as compensating measures. The 4 DC Tapes work together and are designed to compensate for the complete or partial loss of power or communication for two of them at the same time, without interrupting the service and while maintaining the protection of customer data.
		PHY-19. The datacenters interior layout has been designed for the purpose of maximum prevention.
		PHY-20. Security guards perform a shift round to inspect the facility and document any abnormal incidents. If not, distant security guards monitor the facility H24 7/7 through CCTV and on-site technicians make the ambiguity resolution.
		PHY-21. Datacenter staff use the monitoring system to monitor datacenter equipment such as UPS, cooling and air conditioning equipment, etc. Rooms temperature and humidity levels are also monitored.
		PHY-22. OVHcloud has implemented structural, technical and organizational measures for protection against fire and smoke. These measures include: • Fire and smoke detection systems; • Fire extinguishers located in accessible spots and periodically checked and maintained; Regular fire protection exercises.
		PHY-23. Measures have been implemented by OVHcloud to prevent the failure of cooling and power supplies, including: • Appropriate redundancy of power arrivals;

Ref.	CCM Criteria	OVHcloud Control
		• Appropriate redundancy of cooling and air conditioning systems; • Use of alternative power supplies such as UPS and generators; Regular maintenance of the equipment in accordance with the manufacturer's recommendations.
BCR-06	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	**BAC-02.** Procedures for data backup and recovery are documented and include the frequency of data backup as well as the data retention duration. Backups are performed and monitored using an automated system and corrective actions are taken in a timely manner in case of anomaly.
		PHY-23. Measures have been implemented by OVHcloud to prevent the failure of cooling and power supplies, including: • Appropriate redundancy of power arrivals; • Appropriate redundancy of cooling and air conditioning systems; • Use of alternative power supplies such as UPS and generators; Regular maintenance of the equipment in accordance with the manufacturer's recommendations.
		PHY-12. Environmental protections have been installed including the following: • Cooling systems, • Air conditioning units, • Redundant communications lines, • Fire extinguishers, • Smoke detectors, • Redundant electric arrival, • UPS, • Diesel generator.
		PHY-13. Datacenter equipment receives maintenance on at least an annual basis. Generators are tested every 30 days and corrective action taken by the data center manager. *The following equipment are maintained every 3 years which are: the High Voltage Cell, TGBT, the HTA/BT transformer and the fire doors.
		BAC-03. For each Public Cloud product, the redundancy model is based on risk assessment, technical specifications and operational constraints. These elements define the choices for replication locally or at remote sites and the different possible failure scales (network, room, DC). The infrastructure of Public Cloud products is based on scalability and Software Design Storage principles, meaning that the configuration of the control plane can change at will, depending on the customers needs and the technical constraints. Moreoever, as the control planes use

Ref.	CCM Criteria	OVHcloud Control
		stateless components, they can be created or modified by simply redeploying the altered components from the code repositories. Geo-redundancy of the control plane is assured for most Public Cloud products on two locations at least (Compute, Block Storage, Kubernetes and Data). On the other side, Object Storage is a mono-datacenter offer, that does not provide yet geo-redundancy of the control plane. However, resilience is assured thanks to the OpenIO and Swift software model.
BCR-07	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	**PHY-13.** Datacenter equipment receives maintenance on at least an annual basis. Generators are tested every 30 days and corrective action taken by the data center manager. *The following equipment are maintained every 3 years which are: the High Voltage Cell, TGBT, the HTA/BT transformer and the fire doors.
		PHY-23. Measures have been implemented by OVHcloud to prevent the failure of cooling and power supplies, including: • Appropriate redundancy of power arrivals; • Appropriate redundancy of cooling and air conditioning systems; • Use of alternative power supplies such as UPS and generators; Regular maintenance of the equipment in accordance with the manufacturer's recommendations.
		PHY-22. OVHcloud has implemented structural, technical and organizational measures for protection against fire and smoke. These measures include: • Fire and smoke detection systems; • Fire extinguishers located in accessible spots and periodically checked and maintained; Regular fire protection exercises.
BCR-08	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically specific business impact assessment.	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer);

Ref.	CCM Criteria	OVHcloud Control
		• Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		PHY-12. Environmental protections have been installed including the following: • Cooling systems, • Air conditioning units, • Redundant communications lines, • Fire extinguishers, • Smoke detectors, • Redundant electric arrival, • UPS, • Diesel generator.
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.
		PHY-20. Security guards perform a shift round to inspect the facility and document any abnormal incidents. If not, distant security guards monitor the facility H24 7/7 through CCTV and on-site technicians make the ambiguity resolution.
		PHY-21. Datacenter staff use the monitoring system to monitor datacenter equipment such as UPS, cooling and air conditioning equipment, etc. Rooms temperature and humidity levels are also monitored.
		PHY-11. Detection measures and alerts that are communicated to personnel are implemented to identify anomalies that could result from environmental threat events.
		PHY-22. OVHcloud has implemented structural, technical and organizational measures for protection against fire and smoke. These measures include: • Fire and smoke detection systems; • Fire extinguishers located in accessible spots and periodically checked and maintained; • Regular fire protection exercises.

Ref.	CCM Criteria	OVHcloud Control
BCR-09	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
BCR-10	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery, and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	**CHG-07.** OVHcloud has documented policies and procedures for the secure development process that include review and approval, testing, implementation and maintenance.
		GOV-04. Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.
		HR-03. OVHcloud provides continued training about its security commitments and requirements for personnel to support the achievement of objectives. Security training includes: • Handling system components and information assets; • Correct behavior in the event of security incidents. Regarding third parties, service providers undertake on the contract signature to train their employees with the training materials provided by OVHcloud.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics:

Ref.	CCM Criteria	OVHcloud Control
		• information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.
		GOV-03. During its ongoing and periodic business planning and budgeting process, management evaluates the need for additional tools and resources in order to achieve business objectives.
		GOV-17. OVHcloud management has adopted a global information security policy that is communicated to employees, third parties and customers as appropriate. The information security policy describes OVHcloud's objectives, requirements and commitments to information security and refers to specific and detailed security policies that are used as a reference in the implementation of the operational security management system.
		GOV-12. OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedures for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.
		HR-03. OVHcloud provides continued training about its security commitments and requirements for personnel to support the achievement of objectives. Security training includes: • Handling system components and information assets; • Correct behavior in the event of security incidents. Regarding third parties, service providers undertake on the contract signature to train their employees with the training materials provided by OVHcloud.
BCR-11	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and	**BAC-01.** Backup restoration tests are performed at least annually for internal data related to the Public Cloud solution administration. Potential errors are immediately investigated and corrected during restoration tests.

Ref.	CCM Criteria	OVHcloud Control
	procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	**BAC-02.** Procedures for data backup and recovery are documented and include the frequency of data backup as well as the data retention duration. Backups are performed and monitored using an automated system and corrective actions are taken in a timely manner in case of anomaly.
		CUS-01. When a customer terminates his contract, a logical erasure, is performed on all the servers concerned. If this logical erasure fails, the concerned hard drives are destroyed according to a defined secure destruction process.

CCC: Change Control & Configuration Management

Ref.	CCM Criteria	OVHcloud Control
CCC-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network, and systems components, or any corporate, operations and/or data center facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	**CHG-07.** OVHcloud has documented policies and procedures for the secure development process that include review and approval, testing, implementation and maintenance.
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.
		CHG-09. OVHcloud uses dedicated tools for source code management and software deployment into production. Each developer has specific accesses to the repositories and all changes are logged.

Ref.	CCM Criteria	OVHcloud Control
CCC-03	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.	**CHG-07.** OVHcloud has documented policies and procedures for the secure development process that include review and approval, testing, implementation and maintenance.
		CHG-02. OVHcloud requires all changes, including maintenance activities, to be documented and tracked from initiation through change validation and deployment. Moreover, OVHcloud has deployed a SIEM solution that allows operation teams to monitor configuration files changes and other changes in the production environment.
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
		CHG-04. Separate environments are used for development, testing, and production. Moreover, data contained in the production environments is not used in test or development environments in order not to compromise their confidentiality. Lastly, each development must be reviewed by at least one separate reviewer before being merged to production.
		CHG-06. Planned changes to system components that affect the service availability are communicated to customers through the OVHcloud's website. This communication is made 72 hours before the change implementation.
		CHG-09. OVHcloud uses dedicated tools for source code management and software deployment into production. Each developer has specific accesses to the repositories and all changes are logged.
		CHG-05. During the development process, all pull requests must be approved by at least one peer reviewer before being pushed to production.
CCC-04		**CHG-02.** OVHcloud requires all changes, including maintenance activities, to be documented and tracked from initiation through change validation and deployment. Moreover, OVHcloud has deployed a SIEM solution that allows operation teams to monitor configuration files changes and other changes in the production environment.

Ref.	CCM Criteria	OVHcloud Control
	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	**IAM-08.** Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		SEC-07. Employees can only install trusted software available in defined stores for MAC, Windows and Linux workstations and laptops.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
CCC-05	Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations. • Infrastructure network and systems components. Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		CHG-02. OVHcloud requires all changes, including maintenance activities, to be documented and tracked from initiation through change validation and deployment. Moreover, OVHcloud has deployed a SIEM solution that allows operation teams to monitor configuration files changes and other changes in the production environment.

Ref.	CCM Criteria	OVHcloud Control
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel. Major security changes go through a risk analysis, penetration tests are then performed on n as needed basis.

DSI: Data Security & Information Lifecycle Management

Ref.	CCM Criteria	OVHcloud Control
DSI-01	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	**GOV-05.** OVHcloud has a defined information classification scheme according to information security needs. OVHcloud classifies information based on the TLP protocol: • TLP:WHITE or "Public" refers to OVHcloud official information made publicly available by communication instances; • TLP:GREEN refers to information that can freely be communicated within OVHcloud community; • TLP:AMBER or "Confidential" refers to confidential data communicated internally and to specific interested parties under NDA; • TLP:RED or "Highly confidential" refers to highly confidential data disclosed on the "need to know" basis only.Security measures for labelling, access, storage, disclosure and communication means depend on the information confidentiality level.
		GOV-06. A complete inventory of assets located at all geographical locations is maintained and updated regularly. Moreover, during its risk assessment process, OVHcloud identifies the list of assets which may be impacted by each risk scenario. A Business Impact Assessment (BIA) is performed to quantify the consequences of the confidentiality, integrity, or availability loss on the assets impacted by the risk scenario analysed. The asset's criticality depends on the result of the assessment.

Ref.	CCM Criteria	OVHcloud Control
DSI-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.	**GOV-05.** OVHcloud has a defined information classification scheme according to information security needs. OVHcloud classifies information based on the TLP protocol: • TLP:WHITE or "Public" refers to OVHcloud official information made publicly available by communication instances; • TLP:GREEN refers to information that can freely be communicated within OVHcloud community; • TLP:AMBER or "Confidential" refers to confidential data communicated internally and to specific interested parties under NDA; • TLP:RED or "Highly confidential" refers to highly confidential data disclosed on the "need to know" basis only.Security measures for labelling, access, storage, disclosure and communication means depend on the information confidentiality level.
		GOV-06. A complete inventory of assets located at all geographical locations is maintained and updated regularly. Moreover, during its risk assessment process, OVHcloud identifies the list of assets which may be impacted by each risk scenario. A Business Impact Assessment (BIA) is performed to quantify the consequences of the confidentiality, integrity, or availability loss on the assets impacted by the risk scenario analysed. The asset's criticality depends on the result of the assessment.
DSI-04	Policies and procedures shall be established for the labeling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	**GOV-05.** OVHcloud has a defined information classification scheme according to information security needs. OVHcloud classifies information based on the TLP protocol: • TLP:WHITE or "Public" refers to OVHcloud official information made publicly available by communication instances; • TLP:GREEN refers to information that can freely be communicated within OVHcloud community; • TLP:AMBER or "Confidential" refers to confidential data communicated internally and to specific interested parties under NDA; • TLP:RED or "Highly confidential" refers to highly confidential data disclosed on the "need to know" basis only.Security measures for labelling, access, storage, disclosure and communication means depend on the information confidentiality level.
		GOV-06. A complete inventory of assets located at all geographical locations is maintained and updated regularly. Moreover, during its risk assessment process, OVHcloud identifies the list of assets which may be impacted by each risk scenario. A Business Impact Assessment (BIA) is performed to quantify the consequences of the confidentiality, integrity, or availability loss on the assets impacted by the risk scenario analysed. The asset's criticality depends on the result of the assessment.

Ref.	CCM Criteria	OVHcloud Control
DSI-05	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	**CHG-04.** Separate environments are used for development, testing, and production. Moreover, data contained in the production environments is not used in test or development environments in order not to compromise their confidentiality. Lastly, each development must be reviewed by at least one separate reviewer before being merged to production.
		CHG-05. During the development process, all pull requests must be approved by at least one peer reviewer before being pushed to production.
		CHG-01. OVHcloud protects confidential and personal information during system design, development, testing, implementation and change processes to meet the OVHcloud's objectives related to confidentiality and privacy.
DSI-06	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	**GOV-06.** A complete inventory of assets located at all geographical locations is maintained and updated regularly. Moreover, during its risk assessment process, OVHcloud identifies the list of assets which may be impacted by each risk scenario. A Business Impact Assessment (BIA) is performed to quantify the consequences of the confidentiality, integrity, or availability loss on the assets impacted by the risk scenario analysed. The asset's criticality depends on the result of the assessment.
DSI-07	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	**CUS-01.** When a customer terminates his contract, a logical erasure, is performed on all the servers concerned. If this logical erasure fails, the concerned hard drives are destroyed according to a defined secure destruction process.

DCS: Datacenter Security

Ref.	CCM Criteria	OVHcloud Control
DCS-01	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.	**GOV-05.** OVHcloud has a defined information classification scheme according to information security needs. OVHcloud classifies information based on the TLP protocol: • TLP:WHITE or "Public" refers to OVHcloud official information made publicly available by communication instances; • TLP:GREEN refers to information that can freely be communicated within OVHcloud community; • TLP:AMBER or "Confidential" refers to confidential data communicated internally and to specific interested parties under NDA; • TLP:RED or "Highly confidential" refers to highly confidential data disclosed on the "need to know" basis only.Security measures for labelling, access, storage, disclosure and communication means depend on the information confidentiality level.
		GOV-06. A complete inventory of assets located at all geographical locations is maintained and updated regularly. Moreover, during its risk assessment process, OVHcloud identifies the list of assets which may be impacted by each risk scenario. A Business Impact Assessment (BIA) is performed to quantify the consequences of the confidentiality, integrity, or availability loss on the assets impacted by the risk scenario analysed. The asset's criticality depends on the result of the assessment.

Ref.	CCM Criteria	OVHcloud Control
DCS-02	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	**PHY-02.** A monitoring process exists to monitor entry and exit points. Measures such as surveillance cameras and trained security guards are adopted. Logs and video surveillance recordings are maintained for an agreed period of time for future reference. For DC Tape Saint-Pierre-des-Corps and DC Tape Villenave d'Ornon, there are no permanent security guards at the entrance of the datacenter. However, physical security measures are implemented, including access control systems and continuous video surveillance, as well as remote security guard who can be contacted at the entrance of the site and who is responsible of the barrier opening and remote monitoring.
		PHY-03. A security level classification system is used to define zones for access security.
		PHY-04. Access points such as delivery and loading areas where unauthorized persons could enter the premises are controlled and isolated from information processing facilities to avoid unauthorized access. For MiniDCs, physical isolation is not feasible. However, security measures such as the use of access badges are implemented to prevent unauthorized access.
		PHY-09. A card-based physical access control system is implemented at the entry and exit points of the datacenter and critical areas within the facilities. Two-factor authentication mechanism is used for access to Critical+ areas.
		PHY-10. Computer rooms are separated according to the level of criticality of the contents except for some DC Tapes where all the rooms are considered critical implementing all security measures associated to this level.
		PHY-14. Mantraps are used for controlling access to the datacenter. For DC Tapes, alternative access security controls are in place including the use of access badges, CCTV monitoring, security guards.
		PHY-15. Security perimeters are defined and used to protect areas that contain either restricted or critical information and processing facilities. The outer doors, windows and other construction elements reach a level appropriate to the security requirements. The surrounding wall constructions as well as the locking mechanisms meet the associated requirements.
		PHY-17. The sharing of access badges and tailgating are prohibited by policy.

Ref.	CCM Criteria	OVHcloud Control
		PHY-20. Security guards perform a shift round to inspect the facility and document any abnormal incidents. If not, distant security guards monitor the facility H24 7/7 through CCTV and on-site technicians make the ambiguity resolution.
		PHY-21. Datacenter staff use the monitoring system to monitor datacenter equipment such as UPS, cooling and air conditioning equipment, etc. Rooms temperature and humidity levels are also monitored.
		PHY-18. Power and telecommunications cabling carrying data or supporting information services are protected from interception, interference or damage. Where physical protection of cabling is not feasible (e.g., in some DC Tapes), logical controls and encryption are implemented as compensating measures. The 4 DC Tapes work together and are designed to compensate for the complete or partial loss of power or communication for two of them at the same time, without interrupting the service and while maintaining the protection of customer data.
DCS-03	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	**NET-13.** OVHcloud permits the connection to its internal network via VPN and only to authorized equipment using host-based certificates.
DCS-04	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premise.	**PHY-24.** The transfer of equipment to offsite locations is tracked on system and by the edition of transfer vouchers allowing to identify the transferred equipment. The edition of transfer vouchers is restricted to the storekeepers.
DCS-05	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premises. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full overwrite of the drive to ensure that the erased drive is released to inventory for reuse and deployment, or securely stored until it can be destroyed.	**CUS-01.** When a customer terminates his contract, a logical erasure, is performed on all the servers concerned. If this logical erasure fails, the concerned hard drives are destroyed according to a defined secure destruction process.
DCS-06		**PHY-01.** A clear desk and screen policy for information processing facilities and OVHcloud offices are adopted.

Ref.	CCM Criteria	OVHcloud Control
	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	**PHY-02.** A monitoring process exists to monitor entry and exit points. Measures such as surveillance cameras and trained security guards are adopted. Logs and video surveillance recordings are maintained for an agreed period of time for future reference. For DC Tape Saint-Pierre-des-Corps and DC Tape Villenave d'Ornon, there are no permanent security guards at the entrance of the datacenter. However, physical security measures are implemented, including access control systems and continuous video surveillance, as well as remote security guard who can be contacted at the entrance of the site and who is responsible of the barrier opening and remote monitoring.
		PHY-03. A security level classification system is used to define zones for access security.
		PHY-04. Access points such as delivery and loading areas where unauthorized persons could enter the premises are controlled and isolated from information processing facilities to avoid unauthorized access. For MiniDCs, physical isolation is not feasible. However, security measures such as the use of access badges are implemented to prevent unauthorized access.
		PHY-07. All personnel are required to wear badges at all times. Visitor badges are clearly distinguishable from employee badges.
		PHY-08. Visitors' access to OVHcloud's datacenters requires approval by the appropriate manager in the access rights management tool before access being granted. A check is performed at the entrance in order to ensure that the visitor's access is approved.
		PHY-09. A card-based physical access control system is implemented at the entry and exit points of the datacenter and critical areas within the facilities. Two-factor authentication mechanism is used for access to Critical+ areas.
		PHY-10. Computer rooms are separated according to the level of criticality of the contents except for some DC Tapes where all the rooms are considered critical implementing all security measures associated to this level.
		PHY-11. Detection measures and alerts that are communicated to personnel are implemented to identify anomalies that could result from environmental threat events.

Ref.	CCM Criteria	OVHcloud Control
		PHY-12. Environmental protections have been installed including the following: • Cooling systems, • Air conditioning units, • Redundant communications lines, • Fire extinguishers, • Smoke detectors, • Redundant electric arrival, • UPS, • Diesel generator.
		PHY-14. Mantraps are used for controlling access to the datacenter. For DC Tapes, alternative access security controls are in place including the use of access badges, CCTV monitoring, security guards.
		PHY-15. Security perimeters are defined and used to protect areas that contain either restricted or critical information and processing facilities. The outer doors, windows and other construction elements reach a level appropriate to the security requirements. The surrounding wall constructions as well as the locking mechanisms meet the associated requirements.
		PHY-17. The sharing of access badges and tailgating are prohibited by policy.
		PHY-18. Power and telecommunications cabling carrying data or supporting information services are protected from interception, interference or damage. Where physical protection of cabling is not feasible (e.g., in some DC Tapes), logical controls and encryption are implemented as compensating measures. The 4 DC Tapes work together and are designed to compensate for the complete or partial loss of power or communication for two of them at the same time, without interrupting the service and while maintaining the protection of customer data.
		PHY-19. The datacenters interior layout has been designed for the purpose of maximum prevention.
		PHY-20. Security guards perform a shift round to inspect the facility and document any abnormal incidents. If not, distant security guards monitor the facility H24 7/7 through CCTV and on-site technicians make the ambiguity resolution.
		PHY-21. Datacenter staff use the monitoring system to monitor datacenter equipment such as UPS, cooling and air conditioning equipment, etc. Rooms temperature and humidity levels are also monitored.

Ref.	CCM Criteria	OVHcloud Control
		PHY-22. OVHcloud has implemented structural, technical and organizational measures for protection against fire and smoke. These measures include: • Fire and smoke detection systems; • Fire extinguishers located in accessible spots and periodically checked and maintained; • Regular fire protection exercises.
		PHY-06. Access to the datacenter perimeter for employees and third parties requires an access request and manager approval prior to access being provisioned. Once in the perimeter, access to the physical locations according to the person's access rights is granted by authorized and approved granters and is synchronized with the person's badge.
		PHY-05. Access to the datacenter is revoked in a timely manner as part of the termination process.
DCS-07	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	**PHY-02.** A monitoring process exists to monitor entry and exit points. Measures such as surveillance cameras and trained security guards are adopted. Logs and video surveillance recordings are maintained for an agreed period of time for future reference. For DC Tape Saint-Pierre-des-Corps and DC Tape Villenave d'Ornon, there are no permanent security guards at the entrance of the datacenter. However, physical security measures are implemented, including access control systems and continuous video surveillance, as well as remote security guard who can be contacted at the entrance of the site and who is responsible of the barrier opening and remote monitoring.
		PHY-04. Access points such as delivery and loading areas where unauthorized persons could enter the premises are controlled and isolated from information processing facilities to avoid unauthorized access. For MiniDCs, physical isolation is not feasible. However, security measures such as the use of access badges are implemented to prevent unauthorized access.
		PHY-05. Access to the datacenter is revoked in a timely manner as part of the termination process.
		PHY-06. Access to the datacenter perimeter for employees and third parties requires an access request and manager approval prior to access being provisioned. Once in the perimeter, access to the physical locations according to the person's access rights is granted by authorized and approved granters and is synchronized with the person's badge.

Ref.	CCM Criteria	OVHcloud Control
		PHY-08. Visitors' access to OVHcloud's datacenters requires approval by the appropriate manager in the access rights management tool before access being granted. A check is performed at the entrance in order to ensure that the visitor's access is approved.
		PHY-09. A card-based physical access control system is implemented at the entry and exit points of the datacenter and critical areas within the facilities. Two-factor authentication mechanism is used for access to Critical+ areas.
		PHY-14. Mantraps are used for controlling access to the datacenter. For DC Tapes, alternative access security controls are in place including the use of access badges, CCTV monitoring, security guards.
		PHY-15. Security perimeters are defined and used to protect areas that contain either restricted or critical information and processing facilities. The outer doors, windows and other construction elements reach a level appropriate to the security requirements. The surrounding wall constructions as well as the locking mechanisms meet the associated requirements.
		PHY-16. The logs of access to the data centers are reviewed monthly by management in order to detect any unauthorized access. The necessary investigations and corrective actions are performed in a timely manner.
		PHY-17. The sharing of access badges and tailgating are prohibited by policy.
		PHY-20. Security guards perform a shift round to inspect the facility and document any abnormal incidents. If not, distant security guards monitor the facility H24 7/7 through CCTV and on-site technicians make the ambiguity resolution.
DCS-08	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	**PHY-02.** A monitoring process exists to monitor entry and exit points. Measures such as surveillance cameras and trained security guards are adopted. Logs and video surveillance recordings are maintained for an agreed period of time for future reference. For DC Tape Saint-Pierre-des-Corps and DC Tape Villenave d'Ornon, there are no permanent security guards at the entrance of the datacenter. However, physical security measures are implemented, including access control systems and continuous video surveillance, as well as remote security guard who can be contacted at the entrance of the site and who is responsible of the barrier opening and remote monitoring.

Ref.	CCM Criteria	OVHcloud Control
		PHY-04. Access points such as delivery and loading areas where unauthorized persons could enter the premises are controlled and isolated from information processing facilities to avoid unauthorized access. For MiniDCs, physical isolation is not feasible. However, security measures such as the use of access badges are implemented to prevent unauthorized access.
DCS-09	Physical access to information assets and functions by users and support personnel shall be restricted.	**PHY-03.** A security level classification system is used to define zones for access security.
		PHY-05. Access to the datacenter is revoked in a timely manner as part of the termination process.
		PHY-06. Access to the datacenter perimeter for employees and third parties requires an access request and manager approval prior to access being provisioned. Once in the perimeter, access to the physical locations according to the person's access rights is granted by authorized and approved granters and is synchronized with the person's badge.
		PHY-07. All personnel are required to wear badges at all times. Visitor badges are clearly distinguishable from employee badges.
		PHY-08. Visitors' access to OVHcloud's datacenters requires approval by the appropriate manager in the access rights management tool before access being granted. A check is performed at the entrance in order to ensure that the visitor's access is approved.
		PHY-09. A card-based physical access control system is implemented at the entry and exit points of the datacenter and critical areas within the facilities. Two-factor authentication mechanism is used for access to Critical+ areas.
		PHY-10. Computer rooms are separated according to the level of criticality of the contents except for some DC Tapes where all the rooms are considered critical implementing all security measures associated to this level.
		PHY-14. Mantraps are used for controlling access to the datacenter. For DC Tapes, alternative access security controls are in place including the use of access badges, CCTV monitoring, security guards.
		PHY-16. The logs of access to the data centers are reviewed monthly by management in order to detect any unauthorized access. The necessary investigations and corrective actions are performed in a timely manner.

Ref.	CCM Criteria	OVHcloud Control
		PHY-17. The sharing of access badges and tailgating are prohibited by policy.

EKM: Encryption & Key Management

Ref.	CCM Criteria	OVHcloud Control
EKM-01	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	**SEC-09.** Policies and procedures for data encryption are documented and include: • Usage of strong and trusted encryption procedures and secure network protocols that correspond to the state-of-the-art, such as trusted symmetric encryption algorithms, trusted hashing algorithms, trusted one-way password encryption algorithms, trusted key exchange algorithms, trusted SSL/TLS Protocols and certificates... etc. • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys.
		SEC-10. OVHcloud has documented a key management policy that describes the process of secure key management that include: • Keys generation in a secure Locker / Vault using trusted and secure algorithms; • Key storage and communication over secure channels; • Key lifecycle and disposal.
EKM-02	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	**SEC-09.** Policies and procedures for data encryption are documented and include: • Usage of strong and trusted encryption procedures and secure network protocols that correspond to the state-of-the-art, such as trusted symmetric encryption algorithms, trusted hashing algorithms, trusted one-way password encryption algorithms, trusted key exchange algorithms, trusted SSL/TLS Protocols and certificates... etc. • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys.
		SEC-10. OVHcloud has documented a key management policy that describes the process of secure key management that include: • Keys generation in a secure Locker / Vault using trusted and secure algorithms; • Key storage and communication over secure channels; • Key lifecycle and disposal.

Ref.	CCM Criteria	OVHcloud Control
EKM-03	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	**IAM-07.** OVHcloud permits remote access to production systems by authorized employees, using authorized devices, with multi-factor authentication (MFA) and over encrypted virtual private network (VPN) connection.
		NET-06. OVHcloud has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information.
		SEC-03. Storage for laptops and workstations having access to the production environment is encrypted.
		NET-12. OVHcloud has established policies, procedures and technical measures to protect wireless network environments, including the following: • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) User access to wireless network devices restricted to authorized personnel.
		SEC-09. Policies and procedures for data encryption are documented and include: • Usage of strong and trusted encryption procedures and secure network protocols that correspond to the state-of-the-art, such as trusted symmetric encryption algorithms, trusted hashing algorithms, trusted one-way password encryption algorithms, trusted key exchange algorithms, trusted SSL/TLS Protocols and certificates... etc. Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys.
		SEC-10. OVHcloud has documented a key management policy that describes the process of secure key management that include: • Keys generation in a secure Locker / Vault using trusted and secure algorithms; • Key storage and communication over secure channels; Key lifecycle and disposal.
		NET-13. OVHcloud permits the connection to its internal network via VPN and only to authorized equipment using host-based certificates.

GRM: Governance and Risk Management

Ref.	CCM Criteria	OVHcloud Control
GRM-01	Baseline security requirements shall be established for developed or acquired, organizationally owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs.	**SEC-05.** System components used to provide the services on the Public Cloud perimeter are hardened according to generally accepted industry standards. The use of a hardened operating system known as the Hardened Debian distribution provided by Digit Core (based on CIS configuration) is encouraged. Moreover, for CI/CD, the use of collaborative tools like Puppet or Bitbucket is mandatory to ensure versioning or integrity monitoring..
		GOV-01. A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management;

Ref.	CCM Criteria	OVHcloud Control
		• security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
		GOV-12. OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedures for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.
		GOV-16. Exceptions to the policies and procedures for information security as well as respective controls go through the risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners.
GRM-02	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).

Ref.	CCM Criteria	OVHcloud Control
		GOV-05. OVHcloud has a defined information classification scheme according to information security needs. OVHcloud classifies information based on the TLP protocol: • TLP:WHITE or "Public" refers to OVHcloud official information made publicly available by communication instances; • TLP:GREEN refers to information that can freely be communicated within OVHcloud community; • TLP:AMBER or "Confidential" refers to confidential data communicated internally and to specific interested parties under NDA; • TLP:RED or "Highly confidential" refers to highly confidential data disclosed on the "need to know" basis only.Security measures for labelling, access, storage, disclosure and communication means depend on the information confidentiality level.
		GOV-06. A complete inventory of assets located at all geographical locations is maintained and updated regularly. Moreover, during its risk assessment process, OVHcloud identifies the list of assets which may be impacted by each risk scenario. A Business Impact Assessment (BIA) is performed to quantify the consequences of the confidentiality, integrity, or availability loss on the assets impacted by the risk scenario analysed. The asset's criticality depends on the result of the assessment.
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
GRM-03	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	**HR-03.** OVHcloud provides continued training about its security commitments and requirements for personnel to support the achievement of objectives. Security training includes: • Handling system components and information assets; • Correct behavior in the event of security incidents. Regarding third parties, service providers undertake on the contract signature to train their employees with the training materials provided by OVHcloud.
		GOV-04. Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.
		HR-02. OVHcloud management performs annual performance evaluations of employees where past

Ref.	CCM Criteria	OVHcloud Control
		performance and future developments are assessed and discussed. Annual performance evaluations also include review of skills to be further developed and actions to perform such as trainings to follow, specific projects to participate in or roles to take up. The performance evaluation is validated by the employee's manager.
GRM-04	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		GOV-12. OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedures for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.

Ref.	CCM Criteria	OVHcloud Control
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.
		GOV-17. OVHcloud management has adopted a global information security policy that is communicated to employees, third parties and customers as appropriate. The information security policy describes OVHcloud's objectives, requirements and commitments to information security and refers to specific and detailed security policies that are used as a reference in the implementation of the operational security management system.

Ref.	CCM Criteria	OVHcloud Control
GRM-05	Executive and line management shall take formal action to support information security through clearly documented direction and commitment and shall ensure the action has been assigned.	**GOV-04.** Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.
		GOV-17. OVHcloud management has adopted a global information security policy that is communicated to employees, third parties and customers as appropriate. The information security policy describes OVHcloud's objectives, requirements and commitments to information security and refers to specific and detailed security policies that are used as a reference in the implementation of the operational security management system.
		GOV-12. OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedures for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.
		GOV-15. Reporting relationships and organizational structures are defined and reviewed periodically by senior management and adjusted as needed based on changing entity commitments and requirements relevant to security, availability, confidentiality and privacy.

Ref.	CCM Criteria	OVHcloud Control
GRM-06	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-03. During its ongoing and periodic business planning and budgeting process, management evaluates the need for additional tools and resources in order to achieve business objectives.
		GOV-17. OVHcloud management has adopted a global information security policy that is communicated to employees, third parties and customers as appropriate. The information security policy describes OVHcloud's objectives, requirements and commitments to information security and refers to specific and detailed security policies that are used as a reference in the implementation of the operational security management system.
		GOV-04. Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.

Ref.	CCM Criteria	OVHcloud Control
		GOV-12. OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedures for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.
		GOV-15. Reporting relationships and organizational structures are defined and reviewed periodically by senior management and adjusted as needed based on changing entity commitments and requirements relevant to security, availability, confidentiality and privacy.
GRM-07	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	**HR-01.** OVHcloud has documented a code of ethics which is reviewed, updated when necessary, and approved by management. Moreover, personnel are required to read and accept the IT charter and the internal regulations upon their recruitment. Acceptance of information security policy is formally reaffirmed annually. Disciplinary measures and sanctions are established for employees who have violated security policies and procedures, internal regulations or the IT charter.
GRM-08	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.);

Ref.	CCM Criteria	OVHcloud Control
		• Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-12. OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedures for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.
GRM-09	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	**GOV-12.** OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedures for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.
GRM-10	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.

Ref.	CCM Criteria	OVHcloud Control
GRM-11	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		GOV-16. Exceptions to the policies and procedures for information security as well as respective controls go through the risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners.

HRS: Human Resources

Ref.	CCM Criteria	OVHcloud Control
HRS-01	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally owned assets shall be returned within an established period.	**IAM-01.** Logical access is revoked in a timely manner as part of the termination process and any assets handed over are provably returned upon termination of employment.
		HR-07. OVHcloud's employees are provably committed to the IT Charter that defines the guidelines on the acceptable use and safe handling of information assets. Any assets handed over are provably returned upon termination of employment.
HRS-02	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	**HR-04.** Prior to recruitment, a background screening of personnel is performed. Personnel are verified against regulatory screening databases and their experience as well as training are evaluated (if applicable, depending on the country). For third parties, OVHcloud performs a background check of the enterprise during the third parties audit. Moreover, the third party undertakes on the contract signature to perform a background check of its employees.
HRS-03	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	**HR-01.** OVHcloud has documented an Information and Communiation Charter, a Code of Ethics and depending on geographic locations, an Employee Handbook which are reviewed, updated when necessary, and approved by management. Personnel are required to read and accept these documents upon their recruitment. Acceptance of information security policy is formally reaffirmed annually through perimeter membership renewal. Disciplinary measures and sanctions are established for employees who have violated security policies and procedures, internal regulations or the IT charter.

Ref.	CCM Criteria	OVHcloud Control
HRS-04	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	**HR-09.** Roles and responsibilities for performing employment termination or change in employment are described in the perimeter exit procedure.
		GOV-04. Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.
HRS-05	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	**GOV-09.** OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.
HRS-06	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	**GOV-11.** OVHcloud's confidentiality commitments and the associated system requirements, are documented and reviewed when necessary. These commitments and system requirements as well as their changes are communicated to employees, customers and providers, as appropriate which must accept them.
		GOV-14. OVHcloud's security and privacy commitments and changes to these commitments, are communicated to customers and are available on OVHcloud's website.

Ref.	CCM Criteria	OVHcloud Control
HRS-07	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	**GOV-04.** Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.
		THP-05. A security policy with third parties has been implemented by OVHcloud that includes: • Signature of agreements with third parties that define business activities and security requirements; • Background check of third parties; • Audit and monitoring of third parties; • Security training and awareness of third parties.
		THP-04. Third-party relationships are formalized with agreements that identify the critical business activities performed by the third party and the security requirements. Moreover, OVHcloud keeps a file for the monitoring of third parties that includes: • Company name; • Address; • Date of contract signature and contract end; • Description of the service; • Responsible contact person at OVHcloud and at the service provider.
		THP-02. OVHcloud has clauses in its agreements with providers to terminate relationships when necessary.

Ref.	CCM Criteria	OVHcloud Control
HRS-08	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.	**HR-01.** OVHcloud has documented an Information and Communiation Charter, a Code of Ethics and depending on geographic locations, an Employee Handbook which are reviewed, updated when necessary, and approved by management. Personnel are required to read and accept these documents upon their recruitment. Acceptance of information security policy is formally reaffirmed annually through perimeter membership renewal. Disciplinary measures and sanctions are established for employees who have violated security policies and procedures, internal regulations or the IT charter.
		GOV-09. OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.
		HR-07. OVHcloud's employees are provably committed to the IT Charter that defines the guidelines on the acceptable use and safe handling of information assets. Any assets handed over are provably returned upon termination of employment.
HRS-09	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	**IM-03.** Employees, customers and providers have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel. OVHcloud also provides user guides, security alerts and known issues on its websites and client portal with information to improve security knowledge and awareness.
		HR-03. OVHcloud provides continued training about its security commitments and requirements for personnel to support the achievement of objectives. Security training includes: • Handling system components and information assets; • Correct behavior in the event of security incidents. Regarding third parties, service providers undertake on the contract signature to train their employees with the training materials provided by OVHcloud.

Ref.	CCM Criteria	OVHcloud Control
		HR-08. OVHcloud provides security and awareness training to employees based on identified needs and security hot topics. Target group-oriented awareness and training are addressed on a regular basis providing: - best security practices including references to applicable policies and instructions such as programming good practices, training on internal practices for secure infrastructure and on advanced security including current threat situation; - regular security communications and updates on security news as needed; - secure development communications and training.
HRS-10	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	**GOV-04.** Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.
		HR-03. OVHcloud provides continued training about its security commitments and requirements for personnel to support the achievement of objectives. Security training includes: • Handling system components and information assets; • Correct behavior in the event of security incidents. Regarding third parties, service providers undertake on the contract signature to train their employees with the training materials provided by OVHcloud.
HRS-11	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions are disabled after an established period of inactivity.	**PHY-01.** A clear desk and screen policy for information processing facilities and OVHcloud offices are adopted.

IAM: Identity & Access Management

Ref.	CCM Criteria	OVHcloud Controls
IAM-01	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segregated and access restricted to prevent inappropriate disclosure and tampering of log data.	**MON-06.** OVHcloud has documented policies and procedures regarding protection requirements, lifecycle and retention of logs on its systems, that include: • Access only to authorized users and systems; • Backup and retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.
		IAM-05. OVHcloud has designed a set of business roles corresponding to users' job functions to provide with the strict authorizations to access relevant systems and components they need to complete their functions.
IAM-02	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information	**IAM-04.** In-scope system components require unique username, passwords or authorized SSH keys prior to user authentication.
		IAM-07. OVHcloud permits remote access to production systems by authorized employees, using authorized devices, with multi-factor authentication (MFA) and over encrypted virtual private network (VPN) connection.
		IAM-01. Logical access is revoked in a timely manner as part of the termination process and any assets handed over are provably returned upon termination of employment.
		IAM-02. Perimeter entrance requires a documented access request and manager approval prior to access being provisioned. Logical access rights within a perimeter are granted by authorized and approved granters based on rules of need to know and least privilege.
		PHY-05. Access to the datacenter is revoked in a timely manner as part of the termination process.
		PHY-06. Access to the datacenter perimeter for employees and third parties requires an access request and manager approval prior to access being provisioned. Once in the perimeter, access to the physical locations according to the person's access rights is granted by authorized and approved granters and is synchronized with the person's badge.
		PHY-09. A card-based physical access control system is implemented at the entry and exit points of the datacenter and critical areas within the facilities. Two-factor authentication mechanism is used for access to Critical+ areas.

Ref.	CCM Criteria	OVHcloud Controls
	processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements	**GOV-13.** OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.
		IAM-06. Business roles are reviewed on a bi-annual basis by the business role owners ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities.
		CUS-02. OVHcloud provides the Public Cloud customers with access rights mechanisms to manage customer users' access rights on the Public Cloud.
		IAM-08. Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
		IAM-10. Passwords for in-scope system components are configured according to OVHcloud's password policy.
		IAM-03. Generic accounts are used on OVHcloud servers used to manage the cloud service. Access to and use of the generic accounts is traced in the bastions and users are clearly identifiable. Logs of the usage of generic accounts contain the following information: source IP address, username of the accessor, type of access, request made. In addition, a capture of the

Ref.	CCM Criteria	OVHcloud Controls
		session is made and can be replayed. Bastion logs are saved for at least one year.
		IAM-12. OVHcloud has established a secure password configuration policy for in-scope system components that includes: • Restriction on password length and complexity (use of alphanumeric, upper- and lower-case characters); • Password age must not exceed 90 days; • The server-side storage takes place using cryptographically strong hash functions; • Guidelines and instructions on the secure handling and protection of passwords.
		IAM-13. Access to customer data and infrastructure by OVHcloud employees is traced through bastions.
IAM-03	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	**MON-07.** Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
		IAM-08. Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
IAM-04	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	**IAM-02.** Perimeter entrance requires a documented access request and manager approval prior to access being provisioned. Logical access rights within a perimeter are granted by authorized and approved granters based on rules of need to know and least privilege.
		IAM-06. Business roles are reviewed on a bi-annual basis by the business role owners ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities.
		IAM-08. Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.

Ref.	CCM Criteria	OVHcloud Controls
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
		IAM-04. In-scope system components require unique username, passwords or authorized SSH keys prior to user authentication.
		IAM-02. Perimeter entrance requires a documented access request and manager approval prior to access being provisioned. Logical access rights within a perimeter are granted by authorized and approved granters based on rules of need to know and least privilege.
IAM-05	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	**IAM-08.** Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		IAM-06. Business roles are reviewed on a bi-annual basis by the business role owners ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities.
IAM-06	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	**MON-07.** Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
		CHG-09. OVHcloud uses dedicated tools for source code management and software deployment into production. Each developer has specific accesses to the repositories and all changes are logged.
		IAM-06. Business roles are reviewed on a bi-annual basis by the business role owners ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities.
		IAM-02. Perimeter entrance requires a documented access request and manager approval prior to access being provisioned.

Ref.	CCM Criteria	OVHcloud Controls
		Logical access rights within a perimeter are granted by authorized and approved granters based on rules of need to know and least privilege.
		IAM-08. Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
IAM-07	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		IAM-02. Perimeter entrance requires a documented access request and manager approval prior to access being provisioned. Logical access rights within a perimeter are granted by authorized and approved granters based on rules of need to know and least privilege.
		PHY-06. Access to the datacenter perimeter for employees and third parties requires an access request and manager approval prior to access being provisioned. Once in the perimeter, access to the physical locations according to the person's access rights is granted by authorized and approved granters and is synchronized with the person's badge.
		THP-05. A security policy with third parties has been implemented by OVHcloud that includes: • Signature of agreements with third parties that define business activities and security requirements; • Background check of third parties; • Audit and monitoring of third parties; Security training and awareness of third parties.
		THP-03. OVHcloud limits the risk related to the intervention of service providers in the perimeter of its provided

Ref.	CCM Criteria	OVHcloud Controls
		services and products. Service providers do not contribute to the processes of development, change and incident management of the services provided by OVHcloud and thus, do not have access to confidential information. If a third party develops software for a perimeter, a development guideline based on OWASP is provided to them and its employees must be trained accordingly.
		THP-01. OVHcloud annually monitors the compliance of service providers with its security requirements and internal policies through annual audits. These audits include: • The review and renewal of service agreements; • Background check on the company providing the service; • Review of provided services and activities; • Review of certificates of the management systems' compliance with international standards (when applicable); Identified violations and deviations are subjected to analysis, evaluation and treatment.
IAM-08	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	**IAM-02.** Perimeter entrance requires a documented access request and manager approval prior to access being provisioned. Logical access rights within a perimeter are granted by authorized and approved granters based on rules of need to know and least privilege.
		IAM-08. Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		IAM-06. Business roles are reviewed on a bi-annual basis by the business role owners ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
IAM-09	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners, and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network	**IAM-02.** Perimeter entrance requires a documented access request and manager approval prior to access being provisioned. Logical access rights within a perimeter are granted by authorized and approved granters based on rules of need to know and least privilege.

Ref.	CCM Criteria	OVHcloud Controls
	components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	**IAM-08.** Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
		PHY-06. Access to the datacenter perimeter for employees and third parties requires an access request and manager approval prior to access being provisioned. Once in the perimeter, access to the physical locations according to the person's access rights is granted by authorized and approved granters and is synchronized with the person's badge.
IAM-10	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	**IAM-08.** Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		IAM-06. Business roles are reviewed on a bi-annual basis by the business role owners ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities.
		PHY-16. The logs of access to the data centers are reviewed monthly by management in order to detect any unauthorized access. The necessary investigations and corrective actions are performed in a timely manner.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
IAM-11	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure	**IAM-01.** Logical access is revoked in a timely manner as part of the termination process and any assets handed over are provably returned upon termination of employment.

Ref.	CCM Criteria	OVHcloud Controls
	systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	**PHY-05.** Access to the datacenter is revoked in a timely manner as part of the termination process.
IAM-12	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential and/or identity store minimization or re-use when feasible	**IAM-04.** In-scope system components require unique username, passwords or authorized SSH keys prior to user authentication.
		IAM-07. OVHcloud permits remote access to production systems by authorized employees, using authorized devices and over encrypted virtual private network (VPN) connection.
		IAM-10. Passwords for in-scope system components are configured according to OVHcloud's password policy.
		IAM-12. OVHcloud has established a secure password configuration policy for in-scope system components that includes: • Restriction on password length and complexity (use of alphanumeric, upper- and lower-case characters); • Password age must not exceed 90 days; • The server-side storage takes place using cryptographically strong hash functions; • Guidelines and instructions on the secure handling and protection of passwords.
IAM-13	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	**MON-03.** Activity logs on the administration infrastructure are centralized on dedicated syslog servers and are automatically monitored according to defined scenarios in order to detect potential security events. Detected events are raised through alerts to the appropriate departments for investigation and corrective action. Access logs on the bastions are monitored automatically and alerts are raised when suspicious events occur according to predefined patterns. Investigations and corrective actions are performed in a timely manner.
		SEC-05. System components used to provide the services on the Public Cloud perimeter are hardened according to generally accepted industry standards. The use of a hardened operating system known as the Hardened Debian distribution provided by Digit Core (based on CIS configuration) is encouraged. Moreover, for CI/CD, the use of collaborative tools like Puppet or Bitbucket is mandatory to ensure versioning or integrity monitoring..

IVS: Infrastructure & Virtualization Security

Ref.	CCM Criteria	OVHcloud Control
IVS-01	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	**MON-04.** As part of its monitoring processes, OVHcloud monitors the logging and monitoring components in order to detect any failure that could cause the logging to stop or that could alter the logs. Failures are automatically reported, and corrective actions are taken in a timely manner.
		MON-06. OVHcloud has documented policies and procedures regarding protection requirements, lifecycle and retention of logs on its systems, that include: • Access only to authorized users and systems; • Backup and retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.
		MON-01. External access by OVHcloud personnel is logged by the VPN with the following information: accessor IP address, date and event type. Logs are retained for at least 1 year.
		IAM-08. Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.

Ref.	CCM Criteria	OVHcloud Control
IVS-02	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).	**CHG-02.** OVHcloud requires all changes, including maintenance activities, to be documented and tracked from initiation through change validation and deployment. Moreover, OVHcloud has deployed a SIEM solution that allows operation teams to monitor configuration files changes and other changes in the production environment.
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel. Major security changes go through a risk analysis, penetration tests are then performed on n as needed basis.
		CHG-06. Planned changes to system components that affect the service availability are communicated to customers through the OVHcloud's website. This communication is made 72 hours before the change implementation.
		SEC-05. System components used to provide the services on the Public Cloud perimeter are hardened according to generally accepted industry standards. The use of a hardened operating system known as the Hardened Debian distribution provided by Digit Core (based on CIS configuration) is encouraged. Moreover, for CI/CD, the use of collaborative tools like Puppet or Bitbucket is mandatory to ensure versioning or integrity monitoring..
		CUS-12. OVHcloud provides its customers with the ability to restrict the access to a virtual machine via the administration console.
IVS-03	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	**NET-11.** OVHcloud uses NTP servers in order to synchronize the system clocks of all relevant components.
IVS-04	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	**MON-02.** Use of system components is monitored against acceptable tolerance levels using dedicated tools. Moreover, provisioning and de-provisioning of cloud services are monitored continuously in order to adapt hardware orders and equipment availability. Actual capacity and service provision levels are monitored according to specifities of teams and products.
		GOV-03. During its ongoing and periodic business planning and budgeting process, management evaluates the need for additional tools and resources in order to achieve business objectives.

Ref.	CCM Criteria	OVHcloud Control
IVS-05	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware).	**SEC-02.** Vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		SEC-06. OVHcloud uses CVSS (Common Vulnerability Scoring System) for the scoring of vulnerabilities and relies on the online NIST database as well as other sources for the discovery of vulnerabilities. Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities are based on a list of assets ordered by criticality that relies on product-specific criteria for each Public Cloud product. Security patches are then deployed within a time-frame based on asset criticality.
IVS-06	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually and supported by a documented justification for use for all allowed services, protocols, ports, and by compensating controls.	**NET-01.** End user and server workload network traffic is segmented to support isolation. Moreover, there are dedicated networks for the administrative management of the infrastructure. These networks are separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication.
		NET-03. Intrusion detection systems and other technical measures are implemented in order to detect and response to network-based attacks, including network monitoring and traffic filtering.
		NET-07. Incoming and outgoing traffic is formally identified and limited to what is strictly necessary according to the firewall rules. System firewalls are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined and validated by the Information Security Operational Referent (ROSI) or appropriate validator.
		NET-09. Virtual hosts are behind software firewalls which are configured to prevent TCP/IP spoofing, packet sniffing, and restrict incoming connections to customer-specified ports.
		SEC-05. System components used to provide the services on the Public Cloud perimeter are hardened according to generally accepted industry standards. The use of a hardened operating system known as the Hardened Debian distribution provided by Digit Core (based on CIS configuration) is encouraged. Moreover, for CI/CD, the use of collaborative tools like Puppet or Bitbucket is mandatory to ensure versioning or integrity monitoring..

Ref.	CCM Criteria	OVHcloud Control
		NET-02. Firewall configuration files are automatically promoted to production firewall devices. Thus, firewall rules are regularly reviewed by peers before approving any change in the corresponding configuration files in production, thanks to CI/CD processes and tools.
IVS-07	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	**SEC-01.** OVHcloud's procedures on antivirus and anti-malware protection are documented and communicated through its intranet. Antivirus and anti-malware program is implemented and kept updated on workstations and laptops to provide for the interception or detection and remediation of malware.
		NET-07. Incoming and outgoing traffic is formally identified and limited to what is strictly necessary according to the firewall rules. System firewalls are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined and validated by the Information Security Operational Referent (ROSI) or appropriate validator.
		NET-09. Virtual hosts are behind software firewalls which are configured to prevent TCP/IP spoofing, packet sniffing, and restrict incoming connections to customer-specified ports.
		SEC-05. System components used to provide the services on the Public Cloud perimeter are hardened according to generally accepted industry standards. The use of a hardened operating system known as the Hardened Debian distribution provided by Digit Core (based on CIS configuration) is encouraged. Moreover, for CI/CD, the use of collaborative tools like Puppet or Bitbucket is mandatory to ensure versioning or integrity monitoring..
IVS-08	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	**CHG-04.** Separate environments are used for development and production. Moreover, data contained in the production environments is not used in development environment in order not to compromise their confidentiality.
		CHG-05. During the development process, all pull requests must be approved by at least one peer reviewer before being pushed to production.

Ref.	CCM Criteria	OVHcloud Control
IVS-09	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory, and regulatory compliance obligations	**NET-01.** End user and server workload network traffic is segmented to support isolation. Moreover, there are dedicated networks for the administrative management of the infrastructure. These networks are separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication.
		NET-07. Incoming and outgoing traffic is formally identified and limited to what is strictly necessary according to the firewall rules. System firewalls are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined and validated by the Information Security Operational Referent (ROSI) or appropriate validator.
IVS-10	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	**NET-01.** End user and server workload network traffic is segmented to support isolation. Moreover, there are dedicated networks for the administrative management of the infrastructure. These networks are separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication.
		NET-06. OVHcloud has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information.
		SEC-09. Policies and procedures for data encryption are documented and include: • Usage of strong and trusted encryption procedures and secure network protocols that correspond to the state-of-the-art, such as trusted symmetric encryption algorithms, trusted hashing algorithms, trusted one-way password encryption algorithms, trusted key exchange algorithms, trusted SSL/TLS Protocols and certificates... etc. • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys.
		IAM-07. OVHcloud permits remote access to production systems by authorized employees, using authorized devices, with multi-factor authentication (MFA) and over encrypted virtual private network (VPN) connection.
IVS-11		**IAM-04.** In-scope system components require unique username, passwords or authorized SSH keys prior to user authentication.
		IAM-07. OVHcloud permits remote access to production systems by authorized employees, using authorized devices and over encrypted virtual private network (VPN) connection.

Ref.	CCM Criteria	OVHcloud Control
	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	**NET-06.** OVHcloud has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information.
		IAM-08. Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
IVS-12	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	**NET-12.** OVHcloud has established policies, procedures and technical measures to protect wireless network environments, including the following: • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel.
IVS-13	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	**IAM-07.** OVHcloud permits remote access to production systems by authorized employees, using authorized devices, with multi-factor authentication (MFA) and over encrypted virtual private network (VPN) connection.
		NET-09. Virtual hosts are behind software firewalls which are configured to prevent TCP/IP spoofing, packet sniffing, and restrict incoming connections to customer-specified ports.
		NET-03. Intrusion detection systems and other technical measures are implemented in order to detect and response to network-based attacks, including network monitoring and traffic filtering.

Ref.	CCM Criteria	OVHcloud Control
		NET-06. OVHcloud has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information.
		NET-07. Incoming and outgoing traffic is formally identified and limited to what is strictly necessary according to the firewall rules. System firewalls are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined and validated by the Information Security Operational Referent (ROSI) or appropriate validator.
		NET-01. End user and server workload network traffic is segmented to support isolation. Moreover, there are dedicated networks for the administrative management of the infrastructure. These networks are separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication.
		NET-10. The documentation of the logical structure of the network used to provision and operate the service is traceable and up-to-date and made available to the employees on the internal documentation system. The documentation shows how the subnets are allocated and how the network is zoned and segmented.

IPY: Interoperability & Portability

Ref.	CCM Criteria	OVHcloud Control
IPY-01	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	**CUS-04.** OVHcloud has developed application programming interfaces (API) allowing its customers to interact with OVHcloud products without using the graphical customer interface. The interfaces are clearly documented for subject matter experts on how they can be used to retrieve the data. The interfaces use the RESTful standard and can be used with different programming languages.
IPY-02	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).	**CUS-04.** OVHcloud has developed application programming interfaces (API) allowing its customers to interact with OVHcloud products without using the graphical customer interface. The interfaces are clearly documented for subject matter experts on how they can be used to retrieve the data. The interfaces use the RESTful standard and can be used with different programming languages.
IPY-03	Policies, procedures, and mutually agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.	**CUS-04.** OVHcloud has developed application programming interfaces (API) allowing its customers to interact with OVHcloud products without using the graphical customer interface. The interfaces are clearly documented for subject matter experts on how they can be used to retrieve the data. The interfaces use the RESTful standard and can be used with different programming languages.
IPY-04	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	**CUS-04.** OVHcloud has developed application programming interfaces (API) allowing its customers to interact with OVHcloud products without using the graphical customer interface. The interfaces are clearly documented for subject matter experts on how they can be used to retrieve the data. The interfaces use the RESTful standard and can be used with different programming languages.

Ref.	CCM Criteria	OVHcloud Control
IPY-05	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use and all solution-specific virtualization hooks available for customer review.	**SEC-12.** The Public Cloud solution is based on OpenStack technologies. It is a market-recognized open-source tool offering standardized virtualization tools and features that are compatible with other solutions.
		CUS-09. OVHcloud provides the Public Cloud customers with guidelines and recommendations for the configuration and use of the cloud service provided. The information is publicly available on OVHcloud's website and includes: • Instructions for secure configuration; • Authentication mechanisms; • Access and access rights management; and • Services and functions for administration of the cloud service.

MOS: Mobile Security

Ref.	CCM Criteria	OVHcloud Control
MOS-01	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	**HR-03.** OVHcloud provides continued training about its security commitments and requirements for personnel to support the achievement of objectives. Security training includes: • Handling system components and information assets; • Correct behavior in the event of security incidents. Regarding third parties, service providers undertake on the contract signature to train their employees with the training materials provided by OVHcloud.
MOS-02	A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing provider managed data.	**GOV-09.** OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.
MOS-03	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	**GOV-09.** OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.
MOS-04	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	**GOV-09.** OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...);

Ref.	CCM Criteria	OVHcloud Control
		• Use and protection of password / PIN and other authentication mechanisms.
MOS-05	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	**GOV-09.** OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.
		HR-03. OVHcloud provides continued training about its security commitments and requirements for personnel to support the achievement of objectives. Security training includes: • Handling system components and information assets; • Correct behavior in the event of security incidents. Regarding third parties, service providers undertake on the contract signature to train their employees with the training materials provided by OVHcloud.
MOS-06	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	**GOV-09.** OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.
MOS-07	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	**CHG-03.** OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel

Ref.	CCM Criteria	OVHcloud Control
		Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
MOS-08	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	**GOV-09.** OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.
MOS-09	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)) will be included for each device in the inventory.	**GOV-09.** OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.
MOS-10	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	**GOV-09.** OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.

Ref.	CCM Criteria	OVHcloud Control
MOS-11	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.	**GOV-09.** OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.
MOS-12	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and shall enforce the prohibition through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).	**GOV-09.** OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.
MOS-13	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations regarding the loss of non-company data in the case that a wipe of the device is required.	**GOV-09.** OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.

Ref.	CCM Criteria	OVHcloud Control
MOS-14	BYOD and/or company-owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	**GOV-09.** OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.
MOS-15	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	**GOV-09.** OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.
		CHG-02. OVHcloud requires all changes, including maintenance activities, to be documented and tracked from initiation through deployment and validation. OVHcloud utilizes configuration monitoring tool that notifies management of unauthorized changes to production systems.
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
MOS-16		**IAM-04.** In-scope system components require unique username, passwords or authorized SSH keys prior to user authentication.

Ref.	CCM Criteria	OVHcloud Control
	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	**IAM-10.** Passwords for in-scope system components are configured according to OVHcloud's password policy.
		GOV-09. OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.
MOS-17	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	**GOV-09.** OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.
		SEC-01. OVHcloud's procedures on antivirus and anti-malware protection are documented and communicated through its intranet. An antivirus and anti-malware program is implemented and kept updated on workstations, laptops, and servers, to provide for the interception or detection and remediation of malware.
MOS-18	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	**GOV-09.** OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.

Ref.	CCM Criteria	OVHcloud Control
MOS-19	Mobile devices connecting to corporate networks, or storing and accessing company information, shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	**GOV-09.** OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.
MOS-20	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	**GOV-09.** OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.

SEF: Security Incident Management, E-Discovery, & Cloud Forensics

Ref.	CCM Criteria	OVHcloud Control
SEF-01	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	**HR-05.** OVHcloud IT Security team members are members of special interest groups specialized in information security, as appropriate for their functions.
		CUS-06. Investigation requests from government agencies are checked by the Legal Team in order to assess their authenticity and their compliance with the applicable legal framework. Access to or disclosure of customer data to the government agency is performed only after the Legal Team has confirmed the request's authenticity and legal basis.
		PCY-02. Events that resulted in unauthorized use or disclosure of personal information are communicated to the data subjects, legal and regulatory authorities, and others as required.
		GOV-04. Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.
SEF-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	**IM-05.** When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.

Ref.	CCM Criteria	OVHcloud Control
		IM-01. After a security incident has been identified and analyzed for root cause analysis and impact, the action plan is carried out and documented. In the case, the security incident has an impact on the cloud services, a communication is sent to the affected customers. The security incident is formalized within a post-mortem detailing all security incident processing steps.
SEF-03	Workforce personnel and external business relationships shall be informed of their responsibilities and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	**IM-03.** Employees, customers and providers have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel. OVHcloud also provides user guides, security alerts and known issues on its websites and client portal with information to improve security knowledge and awareness.
		IM-04. OVHcloud has a whistle blowing platform available to employees and customers. Management monitors customers and employees' complaints reported via the platform.
SEF-04	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	**CUS-07.** OVHcloud informs the concerned customer during an investigation or request for evidence by a government agency, unless it is prohibited by the applicable law.
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.
		MON-03. Activity logs on the administration infrastructure are centralized on dedicated syslog servers and are automatically monitored according to defined scenarios in order to detect potential security events. Detected events are raised through alerts to the appropriate departments for investigation and corrective action. Access logs on the bastions are monitored automatically and alerts are raised when suspicious events occur according to predefined patterns. Investigations and corrective actions are performed in a timely manner.
		MON-05. OVHcloud has documented policies and procedures regarding the logging and monitoring of events on system components, that include: • Operational aspects of logging and monitoring (logs generation, lifecycle, retention, review and alerting); • Time synchronization of system components; and

Ref.	CCM Criteria	OVHcloud Control
		Compliance with legal and regulatory frameworks.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
SEF-05	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	**IM-01.** After a security incident has been identified and analyzed for root cause analysis and impact, the action plan is carried out and documented. In the case, the security incident has an impact on the cloud services, a communication is sent to the affected customers. The security incident is formalized within a post-mortem detailing all security incident processing steps.
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.
		IM-02. On an annual basis, a crisis unit simulation is performed to ensure the incident response procedures are up-to-date and accurate. When updating the incident response plan, lessons learned are used to implement changes to ensure that incident response procedures are effective.

STA: Supply Chain Management, Transparency, and Accountability

Ref.	CCM Criteria	OVHcloud Control
STA-01	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	**IAM-08.** Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
		THP-01. OVHcloud annually monitors the compliance of service providers with its security requirements and internal policies through annual audits. These audits include: • The review and renewal of service agreements; • Background check on the company providing the service; • Review of provided services and activities; • Review of certificates of the management systems' compliance with international standards (when applicable); Identified violations and deviations are subjected to analysis, evaluation and treatment.
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning;

Ref.	CCM Criteria	OVHcloud Control
		• security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.
		THP-03. OVHcloud limits the risk related to the intervention of service providers in the perimeter of its provided services and products. Service providers do not contribute to the processes of development, change and incident management of the services provided by OVHcloud and thus, do not have access to confidential information. If a third party develops software for a perimeter, a development guideline based on OWASP is provided to them and their employees must be trained accordingly.
		IAM-06. Business roles are reviewed on a bi-annual basis by the business role owners ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities
		CHG-04. Separate environments are used for development, testing, and production. Moreover, data contained in the production environments is not used in test or development environments in order not to compromise their confidentiality. Lastly, each development must be reviewed by at least one separate reviewer before being merged to production.
		CHG-05. During the development process, all pull requests must be approved by at least one peer reviewer before being pushed to production.
STA-02	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	**IM-03.** Employees, customers and providers have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel. OVHcloud also provides user guides, security alerts and known issues on its websites and client portal with information to improve security knowledge and awareness.

Ref.	CCM Criteria	OVHcloud Control
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.
STA-03	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	**CHG-03.** OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
		CHG-06. Planned changes to system components that affect the service availability are communicated to customers through the OVHcloud's website. This communication is made 72 hours before the change implementation.
		MON-02. Use of system components is monitored against acceptable tolerance levels using dedicated tools. Moreover, provisioning and de-provisioning of cloud services are monitored continuously in order to adapt hardware orders and equipment availability. Actual capacity and service provision levels are monitored according to specifities of teams and products.
STA-04	The provider shall perform annual internal assessments of conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics.	**GOV-07.** A procedure for planning and conducting audits is documented and communicated through the intranet. OVHcloud has established a formal audit plan that includes internal and external assessments to validate the implementation and operating effectiveness of the OVHcloud control environment and to assess compliance with the relevant and applicable legal, regulatory or contractual requirements as well as compliance with the policies and procedures. The audit results are reviewed during the monthly ISMS meetings for monitoring of corrective actions.

Ref.	CCM Criteria	OVHcloud Control
		GOV-12. OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedures for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.
STA-05	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and data interoperability and	**GOV-11.** OVHcloud's confidentiality commitments and the associated system requirements, are documented and reviewed when necessary. These commitments and system requirements as well as their changes are communicated to employees, customers and providers, as appropriate which must accept them.
		THP-02. OVHcloud has clauses in its agreements with providers to terminate relationships when necessary.
		THP-01. OVHcloud annually monitors the compliance of service providers with its security requirements and internal policies through annual audits. These audits include: • The review and renewal of service agreements; • Background check on the company providing the service; • Review of provided services and activities; • Review of certificates of the management systems' compliance with international standards (when applicable); Identified violations and deviations are subjected to analysis, evaluation and treatment.
		THP-05. A security policy with third parties has been implemented by OVHcloud that includes: • Signature of agreements with third parties that define business activities and security requirements; • Background check of third parties; • Audit and monitoring of third parties; • Security training and awareness of third parties.
		CUS-05. OVHcloud has defined in customer contractual agreements, the aspects related to the termination of the contractual relationship. The customer is responsible of taking all the necessary measures in order to ensure the conservation of their data before the cancellation of the service. All content and data stored by the customer as part of the service are deleted within an agreed duration from the expiration date of the service or end of payment.
		CUS-15. During the process of subscribing to a Public Cloud, customers must accept the general terms of service and the specific terms of the Public Cloud offer. The general and specific terms of service describe the service, security and contractual commitments and requirements.

Ref.	CCM Criteria	OVHcloud Control
	portability requirements for application development and information exchange, usage, and integrity persistence	**THP-04.** Third-party relationships are formalized with agreements that identify the critical business activities performed by the third party and the security requirements. Moreover, OVHcloud keeps a file for the monitoring of third parties that includes: • Company name; • Address; • Date of contract signature and contract end; • Description of the service; • Responsible contact person at OVHcloud and at the service provider.
		GOV-14. OVHcloud's security and privacy commitments and changes to these commitments, are communicated to customers and are available on OVHcloud's website.

Ref.	CCM Criteria	OVHcloud Control
STA-06	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	**THP-03.** OVHcloud limits the risk related to the intervention of service providers in the perimeter of its provided services and products. Service providers do not contribute to the processes of development, change and incident management of the services provided by OVHcloud and thus, do not have access to confidential information. If a third party develops software for a perimeter, a development guideline based on OWASP is provided to them and their employees must be trained accordingly.
		GOV-01. A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
STA-07	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify any non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	**THP-01.** OVHcloud annually monitors the compliance of service providers with its security requirements and internal policies through annual audits. These audits include: • The review and renewal of service agreements; • Background check on the company providing the service; • Review of provided services and activities; • Review of certificates of the management systems' compliance with international standards (when applicable); Identified violations and deviations are subjected to analysis, evaluation and treatment.
		THP-05. A security policy with third parties has been implemented by OVHcloud that includes: • Signature of agreements with third parties that define business activities and security requirements; • Background check of third parties; • Audit and monitoring of third parties; • Security training and awareness of third parties.

Ref.	CCM Criteria	OVHcloud Control
STA-08	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party-providers upon which their information supply chain depends on.	**THP-03.** OVHcloud limits the risk related to the intervention of service providers in the perimeter of its provided services and products. Service providers do not contribute to the processes of development, change and incident management of the services provided by OVHcloud and thus, do not have access to confidential information. If a third party develops software for a perimeter, a development guideline based on OWASP is provided to them and their employees must be trained accordingly.
		GOV-01. A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		THP-01. OVHcloud annually monitors the compliance of service providers with its security requirements and internal policies through annual audits. These audits include: • The review and renewal of service agreements; • Background check on the company providing the service; • Review of provided services and activities; • Review of certificates of the management systems' compliance with international standards (when applicable); Identified violations and deviations are subjected to analysis, evaluation and treatment.
STA-09	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	**THP-01.** OVHcloud annually monitors the compliance of service providers with its security requirements and internal policies through annual audits. These audits include: • The review and renewal of service agreements; • Background check on the company providing the service; • Review of provided services and activities; • Review of certificates of the management systems' compliance with international standards (when applicable); Identified violations and deviations are subjected to analysis, evaluation and treatment.

Ref.	CCM Criteria	OVHcloud Control
		THP-04. Third-party relationships are formalized with agreements that identify the critical business activities performed by the third party and the security requirements. Moreover, OVHcloud keeps a file for the monitoring of third parties that includes: • Company name; • Address; • Date of contract signature and contract end; • Description of the service; • Responsible contact person at OVHcloud and at the service provider.
		THP-05. A security policy with third parties has been implemented by OVHcloud that includes: • Signature of agreements with third parties that define business activities and security requirements; • Background check of third parties; • Audit and monitoring of third parties; • Security training and awareness of third parties.
		GOV-11. OVHcloud's confidentiality commitments and the associated system requirements, are documented and reviewed when necessary. These commitments and system requirements as well as their changes are communicated to employees, customers and providers, as appropriate which must accept them.

TVM: Threat and Vulnerability Management

Ref.	CCM Criteria	OVHcloud Control
TVM-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	**SEC-01.** OVHcloud's procedures on antivirus and anti-malware protection are documented and communicated through its intranet. Antivirus and anti-malware program is implemented and kept updated on workstations and laptops to provide for the interception or detection and remediation of malware.

Ref.	CCM Criteria	OVHcloud Control
TVM-02	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	**SEC-02.** Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		SEC-06. OVHcloud uses CVSS (Common Vulnerability Scoring System) for the scoring of vulnerabilities and relies on the online NIST database as well as other sources for the discovery of vulnerabilities. Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities are based on a list of assets ordered by criticality that relies on product-specific criteria for each Public Cloud product. Security patches are then deployed within a time-frame based on asset criticality.
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.
		CHG-02. OVHcloud requires all changes, including maintenance activities, to be documented and tracked from initiation through change validation and deployment. Moreover, OVHcloud have a troubleshooting procedure through which operations teams monitor configuration files changes and other changes in the production environment.

Ref.	CCM Criteria	OVHcloud Control
TVM-03	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	**SEC-01.** OVHcloud's procedures on antivirus and anti-malware protection are documented and communicated through its intranet. Antivirus and anti-malware program is implemented and kept updated on workstations and laptops to provide for the interception or detection and remediation of malware.
		CHG-02. OVHcloud requires all changes, including maintenance activities, to be documented and tracked from initiation through change validation and deployment. Moreover, OVHcloud have a troubleshooting procedure through which operations teams monitor configuration files changes and other changes in the production environment.

4. Part C: Mapping between the applicable objectives set forth in C5 and OVHcloud Controls

OIS: Organization of Information Security
Control Objective: Planning, implementation, maintenance and continuous improvement of a framework regarding information security within the organization.

Ref.	C5 Requirement	OVHcloud Control
OIS-01	The Cloud Service Provider operates an information security management system (ISMS) in accordance with ISO/IEC 27001. The scope of the ISMS covers the Cloud Service Provider's organizational units, locations and procedures for providing the cloud service. The measures for setting up, implementing, maintaining and continuously improving the ISMS are documented. The documentation includes: • Scope of the ISMS (Section 4.3 of ISO/IEC 27001); • Declaration of applicability (Section 6.1.3), and • Results of the last management review (Section 9.3).	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-17. OVHcloud management has adopted a global information security policy that is communicated to employees, third parties and customers as appropriate. The information security policy describes OVHcloud's objectives, requirements and commitments to information security and refers to specific and detailed security policies that are used as a reference in the implementation of the operational security management system.
		GOV-04. Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.

Ref.	C5 Requirement	OVHcloud Control
		GOV-12. OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedures for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.

Ref.	C5 Requirement	OVHcloud Control
OIS-02	The top management of the Cloud Service Provider has adopted an information security policy and communicated it to internal and external employees as well as cloud customers. The policy describes: • the importance of information security, based on the requirements of cloud customers in relation to information security; • the security objectives and the desired security level, based on the business goals and tasks of the Cloud Service Provider; • the most important aspects of the security strategy to achieve the security objectives set; and • the organizational structure for information security in the ISMS application area.	**GOV-17.** OVHcloud management has adopted a global information security policy that is communicated to employees, third parties and customers as appropriate. The information security policy describes OVHcloud's objectives, requirements and commitments to information security and refers to specific and detailed security policies that are used as a reference in the implementation of the operational security management system.
		GOV-04. Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.
		GOV-12. OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedures for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.
OIS-03		**GOV-11.** OVHcloud's confidentiality commitments and the associated system requirements, are documented and reviewed when necessary. These commitments and system requirements as well as their changes are communicated to employees, customers and providers, as appropriate which must accept them.

Ref.	C5 Requirement	OVHcloud Control
	Interfaces and dependencies between cloud service delivery activities performed by the Cloud Service Provider and activities performed by third parties are documented and communicated. This includes dealing with the following events: • Vulnerabilities; • Security incidents; and • Malfunctions. The type and scope of the documentation is geared towards the information requirements of the subject matter experts of the affected organizations in order to carry out the activities appropriately (e.g. definition of roles and responsibilities in guidelines, description of cooperation obligations in service descriptions and contracts). The communication of changes to the interfaces and dependencies takes place in a timely manner so that the affected organizations and third parties can react appropriately with organizational and technical measures before the changes take effect.	**GOV-14.** OVHcloud's security and privacy commitments and changes to these commitments, are communicated to customers and are available on OVHcloud's website.
		THP-04. Third-party relationships are formalized with agreements that identify the critical business activities performed by the third party and the security requirements. Moreover, OVHcloud keeps a file for the monitoring of third parties that includes: • Company name; • Address; • Date of contract signature and contract end; • Description of the service; • Responsible contact person at OVHcloud and at the service provider.
		THP-05. A security policy with third parties has been implemented by OVHcloud that includes: • Signature of agreements with third parties that define business activities and security requirements; • Background check of third parties; • Audit and monitoring of third parties; • Security training and awareness of third parties.
		CUS-15. During the process of subscribing to a Public cloud, customers must accept the general terms of service and the specific terms of the Public cloud offer. The general and specific terms of service describe the service, security and contractual commitments and requirements.
		THP-01. OVHcloud annually monitors the compliance of service providers with its security requirements and internal policies through annual audits. These audits include: • The review and renewal of service agreements; • Background check on the company providing the service; • Review of provided services and activities; • Review of certificates of the management systems' compliance with international standards (when applicable); Identified violations and deviations are subjected to analysis, evaluation and treatment.
OIS-04	Conflicting tasks and responsibilities are separated based on an OIS-06 risk assessment to reduce the risk of unauthorized or unintended changes or misuse of cloud customer data processed,	**IAM-08.** Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.

Ref.	C5 Requirement	OVHcloud Control
	stored or transmitted in the cloud service. The risk assessment covers the following areas, insofar as these are applicable to the provision of the Cloud Service and are in the area of responsibility of the Cloud Service Provider: • Administration of rights profiles, approval and assignment of access and access authorizations (cf. IDM-01); • Development, testing and release of changes (cf. DEV-01); and • Operation of the system components. If separation cannot be established for organizational or technical reasons, measures are in place to monitor the activities in order to detect unauthorized or unintended changes as well as misuse and to take appropriate actions.	**MON-07.** Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
		IAM-06. Business roles are reviewed on a bi-annual basis by the business role owners ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities
		CHG-04. Separate environments are used for development and production. Moreover, data contained in the production environments is not used in development environment in order not to compromise their confidentiality.
		GOV-01. A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		CHG-05. During the development process, all pull requests must be approved by at least one peer reviewer before being pushed to production.
OIS-05	The Cloud Service Provider leverages relevant authorities and interest groups in order to stay informed about current threats and vulnerabilities. The information flows into the procedures for handling risks (cf. OIS-06) and vulnerabilities (cf. OPS-19).	**HR-05.** OVHcloud IT Security team members are members of special interest groups specialized in information security, as appropriate for their functions.

Ref.	C5 Requirement	OVHcloud Control
OIS-06	Policies and instructions for risk management procedures are documented, communicated and provided in accordance with SP-01 for the following aspects: • Identification of risks associated with the loss of confidentiality, integrity, availability and authenticity of information within the scope of the ISMS and assigning risk owners; • Analysis of the probability and impact of occurrence and determination of the level of risk; • Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritization of handling; • Handling of risks through measures, including approval of authorization and acceptance of residual risks by risk owners; and • Documentation of the activities implemented to enable consistent, valid and comparable results.	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.

Ref.	C5 Requirement	OVHcloud Control
OIS-07	The Cloud Service Provider executes the process for handling risks as needed or at least once a year. The following aspects are taken into account when identifying risks, insofar as they are applicable to the cloud service provided and are within the area of responsibility of the Cloud Service Provider: • Processing, storage or transmission of data of cloud customers with different protection needs; • Occurrence of weak points and malfunctions in technical protective measures for separating shared resources; • Attacks via access points, including interfaces accessible from public networks; • Conflicting tasks and areas of responsibility that cannot be separated for organizational or technical reasons; and • Dependencies on subservice organizations. The analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, is reviewed for adequacy at least annually by the risk owners.	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.

SP: Security Policies and Instructions
Control Objective: Provide policies and instructions regarding security requirements and to support business requirements.

Ref.	C5 Requirement	OVHcloud Control
SP-01	Policies and instructions (incl. concepts and guidelines) are derived from the information security policy and are documented according to a uniform structure. They are communicated and made available to all internal and external employees of the Cloud Service Provider in an appropriate manner. The policies and instructions are version controlled and approved by the top management of the Cloud Service Provider or an authorized body. The policies and instructions describe at least the following aspects: • Objectives; • Scope; • Roles and responsibilities, including staff qualification requirements and the establishment of substitution rules; • Roles and dependencies on other organizations (especially cloud customers and subservice organizations); • Steps for the execution of the security strategy; and • Applicable legal and regulatory requirements.	**GOV-04.** Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.
		GOV-12. OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedures for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.
		GOV-17. OVHcloud management has adopted a global information security policy that is communicated to employees, third parties and customers as appropriate. The information security policy describes OVHcloud's objectives, requirements and commitments to information security and refers to specific and detailed security policies that are used as a reference in the implementation of the operational security management system.

Ref.	C5 Requirement	OVHcloud Control
SP-02	Information security policies and instructions are reviewed at least annually for adequacy by the Cloud Service Provider's subject matter experts. The review shall consider at least the following aspects: • Organizational and technical changes in the procedures for providing the cloud service; and • Legal and regulatory changes in the Cloud Service Provider's environment. Revised policies and instructions are approved before they become effective.	**GOV-12.** OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedures for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.
SP-03	Exceptions to the policies and instructions for information security as well as respective controls go through the OIS-06 risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners. The approvals of exceptions are documented, limited in time and are reviewed for appropriateness at least annually by the risk owners.	**GOV-16.** Exceptions to the policies and procedures for information security as well as respective controls go through the risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners.

HR: Personnel
Control Objective: Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organization's assets are protected in the event of changes in responsibilities or termination.

Ref.	C5 Requirement	OVHcloud Control
HR-01	The competency and integrity of all internal and external employees of the Cloud Service Provider with access to cloud customer data or system components under the Cloud Service Provider's responsibility who are responsible to provide the cloud service in the production environment shall be verified prior to commencement of employment in accordance with local legislation and regulation by the Cloud Service Provider. To the extent permitted by law, the review will cover the following areas: • Verification of the person through identity card; • Verification of the CV; • Verification of academic titles and degrees; • Request of a police clearance certificate for applicants; • Certificate of good conduct or national equivalent; and • Evaluation of the risk to be blackmailed.	**HR-04.** Prior to recruitment, a background screening of personnel is performed. Personnel are verified against regulatory screening databases and their experience as well as training are evaluated (if applicable, depending on the country). For third parties, OVHcloud performs a background check of the enterprise during the third parties audit. Moreover, the third party undertakes on the contract signature to perform a background check of its employees.
		THP-01. OVHcloud annually monitors the compliance of service providers with its security requirements and internal policies through annual audits. These audits include: • The review and renewal of service agreements; • Background check on the company providing the service; • Review of provided services and activities; • Review of certificates of the management systems' compliance with international standards (when applicable); Identified violations and deviations are subjected to analysis, evaluation and treatment.

Ref.	C5 Requirement	OVHcloud Control
HR-02	The Cloud Service Provider's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security. The information security policy, and the policies and instructions based on it, are to be acknowledged by the internal and external personnel in a documented form before access is granted to any cloud customer data or system components under the responsibility of the Cloud Service Provider used to provide the cloud service in the production environment.	**GOV-11.** OVHcloud's confidentiality commitments and the associated system requirements, are documented and reviewed when necessary. These commitments and system requirements as well as their changes are communicated to employees, customers and providers, as appropriate which must accept them.
		HR-01. OVHcloud has documented an Information and Communiation Charter, a Code of Ethics and depending on geographic locations, an Employee Handbook which are reviewed, updated when necessary, and approved by management. Personnel are required to read and accept these documents upon their recruitment. Acceptance of information security policy is formally reaffirmed annually through perimeter membership renewal. Disciplinary measures and sanctions are established for employees who have violated security policies and procedures, internal regulations or the IT charter.
		GOV-14. OVHcloud's security and privacy commitments and changes to these commitments, are communicated to customers and are available on OVHcloud's website.
		GOV-04. Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.
HR-03	The Cloud Service Provider operates a target group-oriented security awareness and training program, which is completed by all internal and external employees of the Cloud Service Provider on a regular basis. The program is regularly updated based on changes to policies and instructions and the current threat situation and includes the following aspects: • Handling system components used to provide the cloud service in the production environment in accordance with applicable policies and procedures; • Handling cloud customer data in accordance with applicable policies and instructions and applicable legal and regulatory requirements; • Information about the current threat situation; and • Correct behavior in the event of security incidents.	**HR-03.** OVHcloud provides continued training about its security commitments and requirements for personnel to support the achievement of objectives. Security training includes: • Handling system components and information assets; • Correct behavior in the event of security incidents. Regarding third parties, service providers undertake on the contract signature to train their employees with the training materials provided by OVHcloud.
		HR-08. OVHcloud provides security and awareness training to employees based on identified needs and security hot topics. Target group-oriented awareness and training are addressed on a regular basis providing: - best security practices including references to applicable policies and instructions such as programming good practices, training on internal practices for secure infrastructure and on advanced security including current threat situation; - regular security communications and updates on security news as needed; - secure development communications and training.

Ref.	C5 Requirement	OVHcloud Control
HR-04	In the event of violations of policies and instructions or applicable legal and regulatory requirements, actions are taken in accordance with a defined policy that includes the following aspects: • Verifying whether a violation has occurred; and • Consideration of the nature and severity of the violation and its impact. The internal and external employees of the Cloud Service Provider are informed about possible disciplinary measures. The use of disciplinary measures is appropriately documented.	**HR-01.** OVHcloud has documented an Information and Communiation Charter, a Code of Ethics and depending on geographic locations, an Employee Handbook which are reviewed, updated when necessary, and approved by management. Personnel are required to read and accept these documents upon their recruitment. Acceptance of information security policy is formally reaffirmed annually through perimeter membership renewal. Disciplinary measures and sanctions are established for employees who have violated security policies and procedures, internal regulations or the IT charter.
		IM-04. OVHcloud has a whistle blowing platform available to employees and customers. Management monitors customers and employees' complaints reported via the platform.
HR-05	Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long.	**HR-06.** Employees and service providers have been informed about which responsibilities related to confidentiality, will remain in place when their employment is terminated or changed and for how long.
HR-06	The non-disclosure or confidentiality agreements to be agreed with internal employees, external service providers and suppliers of the Cloud Service Provider are based on the requirements identified by the Cloud Service Provider for the protection of confidential information and operational details. The agreements are to be accepted by external service providers and suppliers when the contract is agreed. The agreements must be accepted by internal employees of the Cloud Service Provider before authorization to access data of cloud customers is granted. The requirements must be documented and reviewed at regular intervals (at least annually). If the review shows that the requirements need to be adapted, the non-disclosure or confidentiality agreements are updated. The Cloud Service Provider must inform the internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement.	**GOV-11.** OVHcloud's confidentiality commitments and the associated system requirements, are documented and reviewed when necessary. These commitments and system requirements as well as their changes are communicated to employees, customers and providers, as appropriate which must accept them.
		GOV-14. OVHcloud's security and privacy commitments and changes to these commitments, are communicated to customers and are available on OVHcloud's website.

AM: Asset Management
Control Objective: Identify the organization's own assets and ensure an appropriate level of protection throughout their lifecycle.

Ref.	C5 Requirement	OVHcloud Control
AM-01	The Cloud Service Provider has established procedures for inventorying assets. The inventory is performed automatically and/or by the people or teams responsible for the assets to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle. Assets are recorded with the information needed to apply the Risk Management Procedure (Cf. OIS-07), including the measures taken to manage these risks throughout the asset lifecycle. Changes to this information are logged.	**GOV-06.** A complete inventory of assets located at all geographical locations is maintained and updated regularly. Moreover, during its risk assessment process, OVHcloud identifies the list of assets which may be impacted by each risk scenario. A Business Impact Assessment (BIA) is performed to quantify the consequences of the confidentiality, integrity, or availability loss on the assets impacted by the risk scenario analysed. The asset's criticality depends on the result of the assessment.
AM-02	Policies and instructions for acceptable use and safe handling of assets are documented, communicated and provided in accordance with SP-01 and address the following aspects of the asset lifecycle as applicable to the asset: • Approval procedures for acquisition, commissioning, maintenance, decommissioning, and disposal by authorized personnel or system components; • Inventory; • Classification and labelling based on the need for protection of the information and measures for the level of protection identified; • Secure configuration of mechanisms for error handling, logging, encryption, authentication and authorization; • Requirements for versions of software and images as well as application of patches; • Handling of software for which support and security patches are not available anymore; • Restriction of software installations or use of services; • Protection against malware; • Remote deactivation, deletion or blocking; • Physical delivery and transport; • dealing with incidents and vulnerabilities; and • Complete and irrevocable deletion of the data upon decommissioning.	**GOV-18.** Policies and procedures for acceptable use and safe handling of assets are documented, communicated and address the following aspects: • Inventory; • Risk assessment and classification based on the criticality of the asset and the need for protection of the related information; • Restriction of software installations or use of services; • Protection against malware; • Remote deactivation, deletion or blocking; • Dealing with incidents and vulnerabilities; and • Complete and irrevocable deletion of the data upon decommissioning.

Ref.	C5 Requirement	OVHcloud Control
AM-03	The Cloud Service Provider has an approval process for the use of hardware to be commissioned, which is used to provide the cloud service in the production environment, in which the risks arising from the commissioning are identified, analyzed and mitigated. Approval is granted after verification of the secure configuration of the mechanisms for error handling, logging, encryption, authentication and authorization according to the intended use and based on the applicable policies.	**SEC-08.** OVHcloud has a hardware conformity check process to test the servers when they are assembled and before being used by a customer. The performed tests include tests on CPU, RAM, Motherboard, Network, disks, etc. in order to ensure that the server is fully operational before being put in production.
AM-04	The decommissioning of hardware used to operate system components supporting the cloud service production environment under the responsibility of the Cloud Service Provider requires approval based on the applicable policies. The decommissioning includes the complete and permanent deletion of the data or proper destruction of the media.	**GOV-18.** Policies and procedures for acceptable use and safe handling of assets are documented, communicated and address the following aspects: • Inventory; • Risk assessment and classification based on the criticality of the asset and the need for protection of the related information; • Restriction of software installations or use of services; • Protection against malware; • Remote deactivation, deletion or blocking; • Dealing with incidents and vulnerabilities; and • Complete and irrevocable deletion of the data upon decommissioning.
		CUS-01. When a customer terminates his contract, a logical erasure, is performed on all the servers concerned. If this logical erasure fails, the concerned hard drives are destroyed according to a defined secure destruction process.
AM-05	The Cloud Service Provider's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the Cloud Service Provider has determined in a risk assessment that loss or unauthorized access could compromise the information security of the Cloud Service. Any assets handed over are provably returned upon termination of employment.	**HR-07.** OVHcloud's employees are provably committed to the IT Charter that defines the guidelines on the acceptable use and safe handling of information assets. Any assets handed over are provably returned upon termination of employment.

Ref.	C5 Requirement	OVHcloud Control
AM-06	Assets are classified and, if possible, labelled. Classification and labelling of an asset reflects the protection needs of the information it processes, stores, or transmits. The need for protection is determined by the individuals or groups responsible for the assets of the Cloud Service Provider according to a uniform schema. The schema provides levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives.	**GOV-06.** A complete inventory of assets located at all geographical locations is maintained and updated regularly. Moreover, during its risk assessment process, OVHcloud identifies the list of assets which may be impacted by each risk scenario. A Business Impact Assessment (BIA) is performed to quantify the consequences of the confidentiality, integrity, or availability loss on the assets impacted by the risk scenario analysed. The asset's criticality depends on the result of the assessment.

PS: Physical Security
Control Objective: Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.

Ref.	C5 Requirement	OVHcloud Control
PS-01	Security requirements for premises and buildings related to the cloud service provided, are based on the security objectives of the information security policy, identified protection requirements for the cloud service and the assessment of risks to physical and environmental security. The security requirements are documented, communicated and provided in a policy or concept according to SP-01. The security requirements for data centers are based on criteria which comply with established rules of technology. They are suitable for addressing the following risks in accordance with the applicable legal and contractual requirements: • Faults in planning; • Unauthorized access; • Insufficient surveillance; • Insufficient air-conditioning; • Fire and smoke; • Water; • Power failure; and • Air ventilation and filtration. If the Cloud Service Provider uses premises or buildings operated by third parties to provide the Cloud Service, the document describes which security requirements the Cloud Service Provider places on these third parties. The appropriate and effective verification of implementation is carried out in accordance with the criteria for controlling and monitoring subcontractors (cf. SSO-01, SSO-02).	**BAC-03.** For each Public Cloud product, the redundancy model is based on risk assessment, technical specifications and operational constraints. These elements define the choices for replication locally or at remote sites and the different possible failure scales (network, room, DC). The infrastructure of Public Cloud products is based on scalability and Software Design Storage principles, meaning that the configuration of the control plane can change at will, depending on the customers needs and the technical constraints. Moreoever, as the control planes use stateless components, they can be created or modified by simply redeploying the altered components from the code repositories. Geo-redundancy of the control plane is assured for most Public Cloud products on two locations at least (Compute, Block Storage, Kubernetes and Data). On the other side, Object Storage is a mono-datacenter offer, that does not provide yet geo-redundancy of the control plane. However, resilience is assured thanks to the OpenIO and Swift software model.
		GOV-01. A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		PHY-04. Access points such as delivery and loading areas where unauthorized persons could enter the premises are controlled and isolated from information processing facilities to avoid unauthorized access. For MiniDCs, physical isolation is not feasible. However, security measures such as the use of access badges are implemented to prevent unauthorized access.

Ref.	C5 Requirement	OVHcloud Control
		PHY-05. Access to the datacenter is revoked in a timely manner as part of the termination process.
		PHY-06. Access to the datacenter perimeter for employees and third parties requires an access request and manager approval prior to access being provisioned. Once in the perimeter, access to the physical locations according to the person's access rights is granted by authorized and approved granters and is synchronized with the person's badge.
		PHY-08. Visitors' access to OVHcloud's datacenters requires approval by the appropriate manager in the access rights management tool before access being granted. A check is performed at the entrance in order to ensure that the visitor's access is approved.
		PHY-09. A card-based physical access control system is implemented at the entry and exit points of the datacenter and critical areas within the facilities. Two-factor authentication mechanism is used for access to Critical+ areas.
		PHY-10. Computer rooms are separated according to the level of criticality of the contents except for some DC Tapes where all the rooms are considered critical implementing all security measures associated to this level.
		PHY-11. Detection measures and alerts that are communicated to personnel are implemented to identify anomalies that could result from environmental threat events.
		PHY-12. Environmental protections have been installed including the following: • Cooling systems, • Air conditioning units, • Redundant communications lines, • Fire extinguishers, • Smoke detectors, • Redundant electric arrival, • UPS, • Diesel generator.
		PHY-13. Datacenter equipment receives maintenance on at least an annual basis. Generators are tested every 30 days and corrective action taken by the data center manager. *The following equipment are maintained every 3 years which are: the High Voltage Cell, TGBT, the HTA/BT transformer and the fire doors.
		PHY-14. Mantraps are used for controlling access to the datacenter.

Ref.	C5 Requirement	OVHcloud Control
		For DC Tapes, alternative access security controls are in place including the use of access badges, CCTV monitoring, security guards.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.
		PHY-22. OVHcloud has implemented structural, technical and organizational measures for protection against fire and smoke. These measures include: • Fire and smoke detection systems; • Fire extinguishers located in accessible spots and periodically checked and maintained; Regular fire protection exercises.
		PHY-23. Measures have been implemented by OVHcloud to prevent the failure of cooling and power supplies, including: • Appropriate redundancy of power arrivals; • Appropriate redundancy of cooling and air conditioning systems; • Use of alternative power supplies such as UPS and generators; Regular maintenance of the equipment in accordance with the manufacturer's recommendations.
		PHY-15. Security perimeters are defined and used to protect areas that contain either restricted or critical information and processing facilities. The outer doors, windows and other construction elements reach a level appropriate to the security requirements. The surrounding wall constructions as well as the locking mechanisms meet the associated requirements.

Ref.	C5 Requirement	OVHcloud Control
		PHY-16. The logs of access to the data centers are reviewed monthly by management in order to detect any unauthorized access. The necessary investigations and corrective actions are performed in a timely manner.
		PHY-18. Power and telecommunications cabling carrying data or supporting information services are protected from interception, interference or damage. Where physical protection of cabling is not feasible (e.g., in some DC Tapes), logical controls and encryption are implemented as compensating measures. The 4 DC Tapes work together and are designed to compensate for the complete or partial loss of power or communication for two of them at the same time, without interrupting the service and while maintaining the protection of customer data.
		PHY-19. The datacenters interior layout has been designed for the purpose of maximum prevention.
		PHY-20. Security guards perform a shift round to inspect the facility and document any abnormal incidents. If not, distant security guards monitor the facility H24 7/7 through CCTV and on-site technicians make the ambiguity resolution.
		PHY-21. Datacenter staff use the monitoring system to monitor datacenter equipment such as UPS, cooling and air conditioning equipment, etc. Rooms temperature and humidity levels are also monitored.
PS-02	The cloud service is provided from two locations that are redundant to each other. The locations meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept) and are located in an adequate distance to each other to achieve operational redundancy. Operational redundancy is designed in a way that ensures that the availability requirements specified in the service level agreement are met. The functionality of the redundancy is checked at least annually by suitable tests and exercises (cf. BCM-04 - Verification, updating and testing of business continuity).	**BAC-03.** For each Public Cloud product, the redundancy model is based on risk assessment, technical specifications and operational constraints. These elements define the choices for replication locally or at remote sites and the different possible failure scales (network, room, DC). The infrastructure of Public Cloud products is based on scalability and Software Design Storage principles, meaning that the configuration of the control plane can change at will, depending on the customers needs and the technical constraints. Moreoever, as the control planes use stateless components, they can be created or modified by simply redeploying the altered components from the code repositories. Geo-redundancy of the control plane is assured for most Public Cloud products on two locations at least (Compute, Block Storage, Kubernetes and Data). On the other side, Object Storage is a mono-datacenter offer, that does not provide yet geo-redundacy of the control plane. However, resilience is assured thanks to the OpenIO and Swift software model.

Ref.	C5 Requirement	OVHcloud Control
		GOV-20 Business continuity mechanisms are reviewed and tested at least annually or after significant organizational or environmental changes. The tests are documented and results are taken into account for future operational continuity measures.
PS-03	The structural shell of premises and buildings related to the cloud service provided are physically solid and protected by adequate security measures that meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept). The security measures are designed to detect and prevent unauthorized access in a timely manner so that it does not compromise the information security of the cloud service. The outer doors, windows and other construction elements reach a level appropriate to the security requirements and withstand a burglary attempt for at least 10 minutes. The surrounding wall constructions as well as the locking mechanisms meet the associated requirements.	**PHY-02.** A monitoring process exists to monitor entry and exit points. Measures such as surveillance cameras and trained security guards are adopted. Logs and video surveillance recordings are maintained for an agreed period of time for future reference. For DC Tape Saint-Pierre-des-Corps and DC Tape Villenave d'Ornon, there are no permanent security guards at the entrance of the datacenter. However, physical security measures are implemented, including access control systems and continuous video surveillance, as well as remote security guard who can be contacted at the entrance of the site and who is responsible of the barrier opening and remote monitoring.
		PHY-04. Access points such as delivery and loading areas where unauthorized persons could enter the premises are controlled and isolated from information processing facilities to avoid unauthorized access. For MiniDCs, physical isolation is not feasible. However, security measures such as the use of access badges are implemented to prevent unauthorized access.
		PHY-05. Access to the datacenter is revoked in a timely manner as part of the termination process.
		PHY-06. Access to the datacenter perimeter for employees and third parties requires an access request and manager approval prior to access being provisioned. Once in the perimeter, access to the physical locations according to the person's access rights is granted by authorized and approved granters and is synchronized with the person's badge.
		PHY-08. Visitors' access to OVHcloud's datacenters requires approval by the appropriate manager in the access rights management tool before access being granted. A check is performed at the entrance in order to ensure that the visitor's access is approved.
		PHY-09. A card-based physical access control system is implemented at the entry and exit points of the datacenter and critical areas within the facilities. Two-factor authentication mechanism is used for access to Critical+ areas.
		PHY-14. Mantraps are used for controlling access to the datacenter.

Ref.	C5 Requirement	OVHcloud Control
		For DC Tapes, alternative access security controls are in place including the use of access badges, CCTV monitoring, security guards.
		PHY-15. Security perimeters are defined and used to protect areas that contain either restricted or critical information and processing facilities. The outer doors, windows and other construction elements reach a level appropriate to the security requirements. The surrounding wall constructions as well as the locking mechanisms meet the associated requirements.
PS-04	At access points to premises and buildings related to the cloud service provided, physical access controls are set up in accordance with the Cloud Service Provider's security requirements (cf. PS-01 Security Concept) to prevent unauthorized access. Access controls are supported by an access control system. The requirements for the access control system are documented, communicated and provided in a policy or concept in accordance with SP-01 and include the following aspects: • Specified procedure for the granting and revoking of access authorizations (cf. IDM-02) based on the principle of least authorization ("least-privilege-principle") and as necessary for the performance of tasks ("need-to-know-principle"); • Automatic revocation of access authorizations if they have not been used for a period of 2 month; • Automatic withdrawal of access authorizations if they have not been used for a period of 6 months; • Two-factor authentication for access to areas hosting system components that process cloud customer information; • Visitors and external personnel are tracked individually by the access control during their work in the premises and buildings, identified as such (e.g. by visible wearing of a visitor pass) and supervised during their stay; and • Existence and nature of access logging that enables the Cloud Service Provider, in the sense of an effectiveness audit, to check whether only defined personnel have entered the premises and buildings related to the cloud service provided.	**PHY-05.** Access to the datacenter is revoked in a timely manner as part of the termination process.
		PHY-06. Access to the datacenter perimeter for employees and third parties requires an access request and manager approval prior to access being provisioned. Once in the perimeter, access to the physical locations according to the person's access rights is granted by authorized and approved granters and is synchronized with the person's badge.
		PHY-08. Visitors' access to OVHcloud's datacenters requires approval by the appropriate manager in the access rights management tool before access being granted. A check is performed at the entrance in order to ensure that the visitor's access is approved.
		PHY-09. A card-based physical access control system is implemented at the entry and exit points of the datacenter and critical areas within the facilities. Two-factor authentication mechanism is used for access to Critical+ areas.
		PHY-16. The logs of access to the data centers are reviewed monthly by management in order to detect any unauthorized access. The necessary investigations and corrective actions are performed in a timely manner.

Ref.	C5 Requirement	OVHcloud Control
PS-05	Premises and buildings related to the cloud service provided are protected from fire and smoke by structural, technical and organizational measures that meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept) and include the following aspects: a) Structural Measures: Establishment of fire sections with a fire resistance duration of at least 90 minutes for all structural parts. b) Technical Measures: • Early fire detection with automatic voltage release. The monitored areas are sufficiently fragmented to ensure that the prevention of the spread of incipient fires is proportionate to the maintenance of the availability of the cloud service provided; • Extinguishing system or oxygen reduction; and • Fire alarm system with reporting to the local fire department. c) Organizational Measures • Regular fire protection inspections to check compliance with fire protection requirements; and • Regular fire protection exercises.	**PHY-12.** Inquired with the control owner to gain an understanding of environmental protections and were informed that environmental protections have been installed including the following: • Cooling systems, • Air conditioning units, • Redundant communications lines, • Fire extinguishers, • Smoke detectors, • Redundant electric arrival, • UPS, Diesel generator.
		PHY-22. OVHcloud has implemented structural, technical and organizational measures for protection against fire and smoke. These measures include: • Fire and smoke detection systems; • Fire extinguishers located in accessible spots and periodically checked and maintained; Regular fire protection exercises.

Ref.	C5 Requirement	OVHcloud Control
PS-06	Measures to prevent the failure of the technical supply facilities required for the operation of system components with which information from cloud customers is processed, are documented and set up in accordance with the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept) with respect to the following aspects: a) Operational redundancy (N+1) in power and cooling supply b) Use of appropriately sized uninterruptible power supplies (UPS) and emergency power systems (NEA), designed to ensure that all data remains undamaged in the event of a power failure. The functionality of UPS and NEA is checked at least annually by suitable tests and exercises (cf. BCM-04 - Verification, updating and testing of business continuity). c) Maintenance (servicing, inspection, repair) of the utilities in accordance with the manufacturer's recommendations. d) Protection of power supply and telecommunications lines against interruption, interference, damage and eavesdropping. The protection is checked regularly, but at least every two years, as well as in case of suspected manipulation by qualified personnel regarding the following aspects: • Traces of violent attempts to open closed distributors; • Up-to-datedness of the documentation in the distribution list; • Conformity of the actual wiring and patching with the documentation; • The short-circuits and earthing of unneeded cables are intact; and • Impermissible installations and modifications.	**BAC-03.** For each Public Cloud product, the redundancy model is based on risk assessment, technical specifications and operational constraints. These elements define the choices for replication locally or at remote sites and the different possible failure scales (network, room, DC). The infrastructure of Public Cloud products is based on scalability and Software Design Storage principles, meaning that the configuration of the control plane can change at will, depending on the customers needs and the technical constraints. Moreoever, as the control planes use stateless components, they can be created or modified by simply redeploying the altered components from the code repositories. Geo-redundancy of the control plane is assured for most Public Cloud products on two locations at least (Compute, Block Storage, Kubernetes and Data). On the other side, Object Storage is a mono-datacenter offer, that does not provide yet geo-redundacy of the control plane. However, resilience is assured thanks to the OpenIO and Swift software model.
		PHY-23. Measures have been implemented by OVHcloud to prevent the failure of cooling and power supplies, including: • Appropriate redundancy of power arrivals; • Appropriate redundancy of cooling and air conditioning systems; • Use of alternative power supplies such as UPS and generators; Regular maintenance of the equipment in accordance with the manufacturer's recommendations.
		PHY-22. OVHcloud has implemented structural, technical and organizational measures for protection against fire and smoke. These measures include: • Fire and smoke detection systems; • Fire extinguishers located in accessible spots and periodically checked and maintained; Regular fire protection exercises.
		PHY-13. Datacenter equipment receives maintenance on at least an annual basis. Generators are tested every 30 days and corrective action taken by the data center manager. *The following equipment are maintained every 3 years which are: the High Voltage Cell, TGBT, the HTA/BT transformer and the fire doors.

Ref.	C5 Requirement	OVHcloud Control
		PHY-18. Power and telecommunications cabling carrying data or supporting information services are protected from interception, interference or damage. Where physical protection of cabling is not feasible (e.g., in some DC Tapes), logical controls and encryption are implemented as compensating measures. The 4 DC Tapes work together and are designed to compensate for the complete or partial loss of power or communication for two of them at the same time, without interrupting the service and while maintaining the protection of customer data.
		PHY-12. Environmental protections have been installed including the following: • Cooling systems, • Air conditioning units, • Redundant communications lines, • Fire extinguishers, • Smoke detectors, • Redundant electric arrival, • UPS, • Diesel generator.
PS-07	The operating parameters of the technical utilities (cf. PS-06) and the environmental parameters of the premises and buildings related to the cloud service provided are monitored and controlled in accordance with the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept). When the permitted control range is exceeded, the responsible departments of the Cloud-Provider are automatically informed in order to promptly initiate the necessary measures for return to the control range.	**PHY-11.** Detection measures and alerts that are communicated to personnel are implemented to identify anomalies that could result from environmental threat events.
		PHY-21. Datacenter staff use the monitoring system to monitor datacenter equipment such as UPS, cooling and air conditioning equipment, etc. Rooms temperature and humidity levels are also monitored.
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.

OPS: Operations
Control Objective: Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.

Ref.	C5 Requirement	OVHcloud Control
OPS-01	The planning of capacities and resources (personnel and IT resources) follows an established procedure in order to avoid possible capacity bottlenecks. The procedures include forecasting future capacity requirements in order to identify usage trends and manage system overload. Cloud Service Providers take appropriate measures to ensure that they continue to meet the requirements agreed with cloud customers for the provision of the cloud service in the event of capacity bottlenecks or outages regarding personnel and IT resources, in particular those relating to the dedicated use of system components, in accordance with the respective agreements.	**GOV-03.** During its ongoing and periodic business planning and budgeting process, management evaluates the need for additional tools and resources in order to achieve business objectives. **MON-02.** Use of system components is monitored against acceptable tolerance levels using dedicated tools. Moreover, provisioning and de-provisioning of cloud services are monitored continuously in order to adapt hardware orders and equipment availability. Actual capacity and service provision levels are monitored according to specifities of teams and products.
OPS-02	Technical and organizational safeguards for the monitoring and provisioning and de-provisioning of cloud services are defined. Thus, the Cloud Service Provider ensures that resources are provided and/or services are rendered according to the contractual agreements and that compliance with the service level agreements is ensured.	**MON-02.** Use of system components is monitored against acceptable tolerance levels using dedicated tools. Moreover, provisioning and de-provisioning of cloud services are monitored continuously in order to adapt hardware orders and equipment availability. Actual capacity and service provision levels are monitored according to specifities of teams and products.
OPS-03	Depending on the capabilities of the respective service model, the cloud customer can control and monitor the allocation of the system resources assigned to the customer for administration/use in order to avoid overcrowding of resources and to achieve sufficient performance.	**CUS-14.** OVHcloud provides Public Cloud customers with mechanisms to control and monitor the capacity and allocation of resources using dedicated tools in order to ensure sufficient performance and efficient use of resources.

Ref.	C5 Requirement	OVHcloud Control
OPS-04	Policies and instructions that provide protection against malware are documented, communicated, and provided in accordance with SP-01 with respect to the following aspects: • Use of system-specific protection mechanisms; • Operating protection programs on system components under the responsibility of the Cloud Service Provider that are used to provide the cloud service in the production environment; and • Operation of protection programs for employees' terminal equipment.	**SEC-01.** OVHcloud's procedures on antivirus and anti-malware protection are documented and communicated through its intranet. Antivirus and anti-malware program is implemented and kept updated on workstations and laptops to provide for the interception or detection and remediation of malware.
OPS-05	System components under the Cloud Service Provider's responsibility that are used to deploy the cloud service in the production environment are configured with malware protection according to the policies and instructions. If protection programs are set up with signature and behavior-based malware detection and removal, these protection programs are updated at least daily.	**SEC-01.** OVHcloud's procedures on antivirus and anti-malware protection are documented and communicated through its intranet. Antivirus and anti-malware program is implemented and kept updated on workstations and laptops to provide for the interception or detection and remediation of malware.
OPS-06	Policies and instructions for data backup and recovery are documented, communicated and provided in accordance with SP-01 regarding the following aspects. • The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the cloud customers and the Cloud Service Provider's operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); • Data is backed up in encrypted, state-of-the-art form; • Access to the backed-up data and the execution of restores is performed only by authorized persons; and • Tests of recovery procedures (cf. OPS-08).	**BAC-01.** Backup restoration tests are performed at least annually for internal data related to the Public Cloud solution administration. Potential errors are immediately investigated and corrected during restoration tests. **BAC-02.** Procedures for data backup and recovery are documented and include the frequency of data backup as well as the data retention duration. Backups are performed and monitored using an automated system and corrective actions are taken in a timely manner in case of anomaly. **BAC-04.** The ability to modify backup schedules is restricted to the authorized personnel.
OPS-07	The execution of data backups is monitored by technical and organizational measures. Malfunctions are investigated by qualified staff and rectified promptly to ensure compliance with contractual obligations to cloud customers or the Cloud Service	**BAC-02.** Procedures for data backup and recovery are documented and include the frequency of data backup as well as the data retention duration. Backups are performed and monitored using an automated system and corrective actions are taken in a timely manner in case of anomaly.

Ref.	C5 Requirement	OVHcloud Control
	Provider's business requirements regarding the scope and frequency of data backup and the duration of storage.	**BAC-04.** The ability to modify backup schedules is restricted to the authorized personnel.
OPS-08	Restore procedures are tested regularly, at least annually. The tests allow an assessment to be made as to whether the contractual agreements as well as the specifications for the maximum tolerable downtime (Recovery Time Objective, RTO) and the maximum permissible data loss (Recovery Point Objective, RPO) are adhered to (cf. BCM-02). Deviations from the specifications are reported to the responsible personnel or system components so that these can promptly assess the deviations and initiate the necessary actions.	**BAC-01.** Backup restoration tests are performed at least annually for internal data related to the Public Cloud solution administration. Potential errors are immediately investigated and corrected during restoration tests.
OPS-09	The Cloud Service Provider transfers data to be backed up to a remote location or transports these on backup media to a remote location. If the data backup is transmitted to the remote location via a network, the data backup or the transmission of the data takes place in an encrypted form that corresponds to the state-of-the-art. The distance to the main site is chosen after sufficient consideration of the factors recovery times and impact of disasters on both sites. The physical and environmental security measures at the remote site are at the same level as at the main site.	**BAC-02.** Procedures for data backup and recovery are documented and include the frequency of data backup as well as the data retention duration. Backups are performed and monitored using an automated system and corrective actions are taken in a timely manner in case of anomaly.
		NET-06. OVHcloud has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information.
		BAC-03. For each Public Cloud product, the redundancy model is based on risk assessment, technical specifications and operational constraints. These elements define the choices for replication locally or at remote sites and the different possible failure scales (network, room, DC). The infrastructure of Public Cloud products is based on scalability and Software Design Storage principles, meaning that the configuration of the control plane can change at will, depending on the customers needs and the technical constraints. Moreoever, as the control planes use stateless components, they can be created or modified by simply redeploying the altered components from the code repositories.

Ref.	C5 Requirement	OVHcloud Control
		Geo-redundancy of the control plane is assured for most Public Cloud products on two locations at least (Compute, Block Storage, Kubernetes and Data). On the other side, Object Storage is a mono-datacenter offer, that does not provide yet geo-redundacy of the control plane. However, resilience is assured thanks to the OpenIO and Swift software model.
OPS-10	The Cloud Service Provider has established policies and instructions that govern the logging and monitoring of events on system components within its area of responsibility. These policies and instructions are documented, communicated and provided according to SP-01 with respect to the following aspects: • Definition of events that could lead to a violation of the protection goals; • Specifications for activating, stopping and pausing the various logs; • Information regarding the purpose and retention period of the logs. • Define roles and responsibilities for setting up and monitoring logging; • Time synchronization of system components; and • Compliance with legal and regulatory frameworks.	**MON-05.** OVHcloud has documented policies and procedures regarding the logging and monitoring of events : • Operational aspects of logging and monitoring (logs generation, lifecycle, retention, review and alerting); • Time synchronization of system components; and • Compliance with legal and regulatory frameworks.
OPS-11	Policies and instructions for the secure handling of metadata (usage data) are documented, communicated and provided according to SP-01 with regard to the following aspects: • Metadata is collected and used solely for billing, incident management and security incident management purposes; • Exclusively anonymous metadata to deploy and enhance the cloud service so that no conclusions can be drawn about the cloud customer or user; • No commercial use; • Storage for a fixed period reasonably related to the purposes of the collection; • Immediate deletion if the purposes of the collection are fulfilled and further storage is no longer necessary. • Provision to cloud customers according to contractual agreements.	**GOV-19.** As part of contract execution, the metadata collected by OVHcloud is used for the purposes of business management, information and support, claims management, invoicing and accounting, payment management, process improvement and customer relationship management. The collected data, its usage and its retention period are documented.

Ref.	C5 Requirement	OVHcloud Control
OPS-12	The requirements for the logging and monitoring of events and for the secure handling of metadata are implemented by technically supported procedures with regard to the following restrictions: • Access only to authorized users and systems; • Retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.	**MON-06.** OVHcloud has documented policies and procedures regarding protection requirements, lifecycle and retention of logs on its systems, that include: • Access only to authorized users and systems; • Backup and retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.
OPS-13	The logging data is automatically monitored for events that may violate the protection goals in accordance with the logging and monitoring requirements. This also includes the detection of relationships between events (event correlation). Identified events are automatically reported to the appropriate departments for prompt evaluation and action.	**MON-03.** Activity logs on the administration infrastructure are centralized on dedicated syslog servers and are automatically monitored according to defined scenarios in order to detect potential security events. Detected events are raised through alerts to the appropriate departments for investigation and corrective action. Access logs on the bastions are monitored automatically and alerts are raised when suspicious events occur according to predefined patterns. Investigations and corrective actions are performed in a timely manner.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
OPS-14	The Cloud Service Provider retains the generated log data and keeps these in an appropriate, unchangeable and aggregated form, regardless of the source of such data, so that a central, authorized evaluation of the data is possible. Log data is deleted if it is no longer required for the purpose for which they were collected. Between logging servers and the assets to be logged, authentication takes place to protect the integrity and authenticity of the information transmitted and stored. The transfer takes place using state-of-the-art encryption or a dedicated administration network (out-of-band management).	**MON-06.** OVHcloud has documented policies and procedures regarding protection requirements, lifecycle and retention of logs on its systems, that include: • Access only to authorized users and systems; • Backup and retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
OPS-15	The log data generated allows an unambiguous identification of user accesses at tenant level to support (forensic) analysis in the event of a security incident. Interfaces are available to conduct forensic analyses and perform backups of	**MON-03.** Activity logs on the administration infrastructure are centralized on dedicated syslog servers and are automatically monitored according to defined scenarios in order to detect potential security events. Detected events are raised through alerts to the appropriate departments for investigation and corrective action.

Ref.	C5 Requirement	OVHcloud Control
	infrastructure components and their network communication.	Access logs on the bastions are monitored automatically and alerts are raised when suspicious events occur according to predefined patterns. Investigations and corrective actions are performed in a timely manner.
		MON-04. As part of its monitoring processes, OVHcloud monitors the logging and monitoring components in order to detect any failure that could cause the logging to stop or that could alter the logs. Failures are automatically reported, and corrective actions are taken in a timely manner.
		CUS-10. OVHcloud provides its customers with dedicated tools for monitoring and supervision of their Public Cloud. These tools provide information regarding system performance and availability and include alerts and error handling mechanisms.
		MON-05. OVHcloud has documented policies and procedures regarding the logging and monitoring of events on system components, that include: • Operational aspects of logging and monitoring (logs generation, lifecycle, retention, review and alerting); • Time synchronization of system components; and • Compliance with legal and regulatory frameworks.
		MON-06. OVHcloud has documented policies and procedures regarding protection requirements, lifecycle and retention of logs on its systems, that include: • Access only to authorized users and systems; • Backup and retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.
		MON-01. External access by OVHcloud personnel is logged by the VPN with the following information: accessor IP address, date and event type. Logs are retained for at least 1 year.
		IAM-08. Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.

Ref.	C5 Requirement	OVHcloud Control
OPS-16	Access to system components for logging and monitoring in the Cloud Service Provider's area of responsibility is restricted to authorized users. Changes to the configuration are made in accordance with the applicable policies (cf. DEV-03).	**IAM-05.** OVHcloud has designed a set of business roles corresponding to users' job functions to provide with the strict authorizations to access relevant systems and components they need to complete their functions.
		IAM-08. Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
OPS-17	The Cloud Service Provider monitors the system components for logging and monitoring in its area of responsibility. Failures are automatically and promptly reported to the Cloud Service Provider's responsible departments so that these can assess the failures and take required action.	**MON-04.** As part of its monitoring processes, OVHcloud monitors the logging and monitoring components in order to detect any failure that could cause the logging to stop or that could alter the logs. Failures are automatically reported, and corrective actions are taken in a timely manner.
OPS-18	Guidelines and instructions with technical and organizational measures are documented, communicated and provided in accordance with SP-01 to ensure the timely identification and addressing of vulnerabilities in the system components used to provide the cloud service. These guidelines and instructions contain specifications regarding the following aspects: • Regular identification of vulnerabilities; • Assessment of the severity of identified vulnerabilities; • Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and • Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.	**SEC-02.** Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		SEC-06. OVHcloud uses CVSS (Common Vulnerability Scoring System) for the scoring of vulnerabilities and relies on the online NIST database as well as other sources for the discovery of vulnerabilities. Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities are based on a list of assets ordered by criticality that relies on product-specific criteria for each Public Cloud product. Security patches are then deployed within a time-frame based on asset criticality.
		CHG-02. OVHcloud requires all changes, including maintenance activities, to be documented and tracked from initiation through change validation and deployment. Moreover, OVHcloud have a troubleshooting

Ref.	C5 Requirement	OVHcloud Control
		procedure through which operations teams monitor configuration files changes and other changes in the production environment.
		GOV-01. A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security

Ref.	C5 Requirement	OVHcloud Control
		incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.
OPS-19	The Cloud Service Provider has penetration tests carried out by qualified internal personnel or external service providers at least once a year. The penetration tests are carried out according to a documented test methodology and include the system components relevant to the provision of the cloud service in the area of responsibility of the Cloud Service Provider, which have been identified as such in a risk analysis. The Cloud Service Provider assess the severity of the findings made in penetration tests according to defined criteria. For findings with medium or high criticality regarding the confidentiality, integrity or availability of the cloud service, actions must be taken within defined time windows for prompt remediation or mitigation.	**SEC-02.** Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		SEC-06. OVHcloud uses CVSS (Common Vulnerability Scoring System) for the scoring of vulnerabilities and relies on the online NIST database as well as other sources for the discovery of vulnerabilities. Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities are based on a list of assets ordered by criticality that relies on product-specific criteria for each Public Cloud product. Security patches are then deployed within a time-frame based on asset criticality.
OPS-20	The Cloud Service Provider regularly measures, analyses and assesses the procedures with which vulnerabilities and incidents are handled to verify their continued suitability, appropriateness and effectiveness. Results are evaluated at least quarterly by accountable departments at the Cloud Service Provider to initiate continuous improvement actions and to verify their effectiveness.	**IM-02.** On an annual basis, a crisis unit simulation is performed to ensure the incident response procedures are up-to-date and accurate. When updating the incident response plan, lessons learned are used to implement changes to ensure that incident response procedures are effective.
OPS-21	The Cloud Service Provider periodically informs the cloud customer on the status of incidents affecting the cloud customer, or, where appropriate and necessary, involve the customer in the resolution, in a manner consistent with the contractual agreements. As soon as an incident has been resolved from the Cloud Service Provider's perspective, the cloud customer is informed according to the contractual agreements, about the actions taken.	**IM-05.** When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.
		CHG-06. Planned changes to system components that affect the service availability are communicated to clients through the OVHcloud's website. This communication is made 72 hours before the change implementation.
OPS-22	System components in the area of responsibility of the Cloud Service Provider for the provision of the cloud service are automatically checked for known	**SEC-02.** Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible

Ref.	C5 Requirement	OVHcloud Control
	vulnerabilities at least once a month in accordance with the policies for handling vulnerabilities (cf. OPS-18), the severity is assessed in accordance with defined criteria and measures for timely remediation or mitigation are initiated within defined time windows.	with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		SEC-06. OVHcloud uses CVSS (Common Vulnerability Scoring System) for the scoring of vulnerabilities and relies on the online NIST database as well as other sources for the discovery of vulnerabilities. Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities are based on a list of assets ordered by criticality that relies on product-specific criteria for each Public Cloud product. Security patches are then deployed within a time-frame based on asset criticality.
OPS-23	System components in the production environment used to provide the cloud service under the Cloud Service Provider's responsibility are hardened according to generally accepted industry standards. The hardening requirements for each system component are documented. If non-modifiable ("immutable") images are used, compliance with the hardening specifications as defined in the hardening requirements is checked upon creation of the images. Configuration and log files regarding the continuous availability of the images are retained.	**SEC-05.** System components used to provide the services on the Public Cloud perimeter are hardened according to generally accepted industry standards. The use of a hardened operating system known as the Hardened Debian distribution provided by Digit Core (based on CIS configuration) is encouraged. Moreover, for CI/CD, the use of collaborative tools like Puppet or Bitbucket is mandatory to ensure versioning or integrity monitoring.
OPS-24	Cloud customer data stored and processed on shared virtual and physical resources is securely and strictly separated according to a documented approach based on OIS-07 risk analysis to ensure the confidentiality and integrity of this data.	**NET-01.** End user and server workload network traffic is segmented to support isolation. Moreover, there are dedicated networks for the administrative management of the infrastructure. These networks are separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication.
		NET-07. Incoming and outgoing traffic is formally identified and limited to what is strictly necessary according to the firewall rules. System firewalls are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined and validated by the Information Security Operational Referent (ROSI) or appropriate validator.
		NET-10. The documentation of the logical structure of the network used to provision and operate the service is traceable and up-to-date and made available to the employees on the internal documentation system. The documentation shows how the subnets are allocated and how the network is zoned and segmented.

Ref.	C5 Requirement	OVHcloud Control
OPS-01	The planning of capacities and resources (personnel and IT resources) follows an established procedure in order to avoid possible capacity bottlenecks. The procedures include forecasting future capacity requirements in order to identify usage trends and manage system overload. Cloud Service Providers take appropriate measures to ensure that they continue to meet the requirements agreed with cloud customers for the provision of the cloud service in the event of capacity bottlenecks or outages regarding personnel and IT resources, in particular those relating to the dedicated use of system components, in accordance with the respective agreements.	**GOV-03.** During its ongoing and periodic business planning and budgeting process, management evaluates the need for additional tools and resources in order to achieve business objectives.
		MON-02. Use of system components is monitored against acceptable tolerance levels using dedicated tools. Moreover, provisioning and de-provisioning of cloud services are monitored continuously in order to adapt hardware orders and equipment availability. Actual capacity and service provision levels are monitored according to specifities of teams and products.
OPS-02	Technical and organizational safeguards for the monitoring and provisioning and de-provisioning of cloud services are defined. Thus, the Cloud Service Provider ensures that resources are provided and/or services are rendered according to the contractual agreements and that compliance with the service level agreements is ensured.	**MON-02.** Use of system components is monitored against acceptable tolerance levels using dedicated tools. Moreover, provisioning and de-provisioning of cloud services are monitored continuously in order to adapt hardware orders and equipment availability. Actual capacity and service provision levels are monitored according to specifities of teams and products.
OPS-03	Depending on the capabilities of the respective service model, the cloud customer can control and monitor the allocation of the system resources assigned to the customer for administration/use in order to avoid overcrowding of resources and to achieve sufficient performance.	**CUS-14.** OVHcloud provides Public Cloud customers with mechanisms to control and monitor the capacity and allocation of resources using dedicated tools in order to ensure sufficient performance and efficient use of resources.

Ref.	C5 Requirement	OVHcloud Control
OPS-04	Policies and instructions that provide protection against malware are documented, communicated, and provided in accordance with SP-01 with respect to the following aspects: • Use of system-specific protection mechanisms; • Operating protection programs on system components under the responsibility of the Cloud Service Provider that are used to provide the cloud service in the production environment; and • Operation of protection programs for employees' terminal equipment.	**SEC-01.** OVHcloud's procedures on antivirus and anti-malware protection are documented and communicated through its intranet. Antivirus and anti-malware program is implemented and kept updated on workstations and laptops to provide for the interception or detection and remediation of malware.
OPS-05	System components under the Cloud Service Provider's responsibility that are used to deploy the cloud service in the production environment are configured with malware protection according to the policies and instructions. If protection programs are set up with signature and behavior-based malware detection and removal, these protection programs are updated at least daily.	**SEC-01.** OVHcloud's procedures on antivirus and anti-malware protection are documented and communicated through its intranet. Antivirus and anti-malware program is implemented and kept updated on workstations and laptops to provide for the interception or detection and remediation of malware.
OPS-06	Policies and instructions for data backup and recovery are documented, communicated and provided in accordance with SP-01 regarding the following aspects. • The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the cloud customers and the Cloud Service Provider's operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); • Data is backed up in encrypted, state-of-the-art form; • Access to the backed-up data and the execution of restores is performed only by authorized persons; and • Tests of recovery procedures (cf. OPS-08).	**BAC-01.** Backup restoration tests are performed at least annually for internal data related to the Public Cloud solution administration. Potential errors are immediately investigated and corrected during restoration tests. **BAC-02.** Procedures for data backup and recovery are documented and include the frequency of data backup as well as the data retention duration. Backups are performed and monitored using an automated system and corrective actions are taken in a timely manner in case of anomaly. **BAC-04.** The ability to modify backup schedules is restricted to the authorized personnel.
OPS-07	The execution of data backups is monitored by technical and organizational measures. Malfunctions are investigated by qualified staff and rectified promptly to ensure compliance with contractual obligations to cloud customers or the Cloud Service	**BAC-02.** Procedures for data backup and recovery are documented and include the frequency of data backup as well as the data retention duration. Backups are performed and monitored using an automated system and corrective actions are taken in a timely manner in case of anomaly.

Ref.	C5 Requirement	OVHcloud Control
	Provider's business requirements regarding the scope and frequency of data backup and the duration of storage.	**BAC-04.** The ability to modify backup schedules is restricted to the authorized personnel.
OPS-08	Restore procedures are tested regularly, at least annually. The tests allow an assessment to be made as to whether the contractual agreements as well as the specifications for the maximum tolerable downtime (Recovery Time Objective, RTO) and the maximum permissible data loss (Recovery Point Objective, RPO) are adhered to (cf. BCM-02). Deviations from the specifications are reported to the responsible personnel or system components so that these can promptly assess the deviations and initiate the necessary actions.	**BAC-01.** Backup restoration tests are performed at least annually for internal data related to the Public Cloud solution administration. Potential errors are immediately investigated and corrected during restoration tests.
OPS-09	The Cloud Service Provider transfers data to be backed up to a remote location or transports these on backup media to a remote location. If the data backup is transmitted to the remote location via a network, the data backup or the transmission of the data takes place in an encrypted form that corresponds to the state-of-the-art. The distance to the main site is chosen after sufficient consideration of the factors recovery times and impact of disasters on both sites. The physical and environmental security measures at the remote site are at the same level as at the main site.	**BAC-02.** Procedures for data backup and recovery are documented and include the frequency of data backup as well as the data retention duration. Backups are performed and monitored using an automated system and corrective actions are taken in a timely manner in case of anomaly.
		NET-06. OVHcloud has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information.
		BAC-03. For each Public Cloud product, the redundancy model is based on risk assessment, technical specifications and operational constraints. These elements define the choices for replication locally or at remote sites and the different possible failure scales (network, room, DC). The infrastructure of Public Cloud products is based on scalability and Software Design Storage principles, meaning that the configuration of the control plane can change at will, depending on the customers needs and the technical constraints. Moreoever, as the control planes use stateless components, they can be created or modified by simply redeploying the altered components from the code repositories.

Ref.	C5 Requirement	OVHcloud Control
		Geo-redundancy of the control plane is assured for most Public Cloud products on two locations at least (Compute, Block Storage, Kubernetes and Data). On the other side, Object Storage is a mono-datacenter offer, that does not provide yet geo-redundacy of the control plane. However, resilience is assured thanks to the OpenIO and Swift software model.
OPS-10	The Cloud Service Provider has established policies and instructions that govern the logging and monitoring of events on system components within its area of responsibility. These policies and instructions are documented, communicated and provided according to SP-01 with respect to the following aspects: • Definition of events that could lead to a violation of the protection goals; • Specifications for activating, stopping and pausing the various logs; • Information regarding the purpose and retention period of the logs. • Define roles and responsibilities for setting up and monitoring logging; • Time synchronization of system components; and • Compliance with legal and regulatory frameworks.	**MON-05.** OVHcloud has documented policies and procedures regarding the logging and monitoring of events : • Operational aspects of logging and monitoring (logs generation, lifecycle, retention, review and alerting); • Time synchronization of system components; and • Compliance with legal and regulatory frameworks.
OPS-11	Policies and instructions for the secure handling of metadata (usage data) are documented, communicated and provided according to SP-01 with regard to the following aspects: • Metadata is collected and used solely for billing, incident management and security incident management purposes; • Exclusively anonymous metadata to deploy and enhance the cloud service so that no conclusions can be drawn about the cloud customer or user; • No commercial use; • Storage for a fixed period reasonably related to the purposes of the collection; • Immediate deletion if the purposes of the collection are fulfilled and further storage is no longer necessary. • Provision to cloud customers according to contractual agreements.	**GOV-19.** As part of contract execution, the metadata collected by OVHcloud is used for the purposes of business management, information and support, claims management, invoicing and accounting, payment management, process improvement and customer relationship management. The collected data, its usage and its retention period are documented.

Ref.	C5 Requirement	OVHcloud Control
OPS-12	The requirements for the logging and monitoring of events and for the secure handling of metadata are implemented by technically supported procedures with regard to the following restrictions: • Access only to authorized users and systems; • Retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.	**MON-06.** OVHcloud has documented policies and procedures regarding protection requirements, lifecycle and retention of logs on its systems, that include: • Access only to authorized users and systems; • Backup and retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.
OPS-13	The logging data is automatically monitored for events that may violate the protection goals in accordance with the logging and monitoring requirements. This also includes the detection of relationships between events (event correlation). Identified events are automatically reported to the appropriate departments for prompt evaluation and action.	**MON-03.** Activity logs on the administration infrastructure are centralized on dedicated syslog servers and are automatically monitored according to defined scenarios in order to detect potential security events. Detected events are raised through alerts to the appropriate departments for investigation and corrective action. Access logs on the bastions are monitored automatically and alerts are raised when suspicious events occur according to predefined patterns. Investigations and corrective actions are performed in a timely manner.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
OPS-14	The Cloud Service Provider retains the generated log data and keeps these in an appropriate, unchangeable and aggregated form, regardless of the source of such data, so that a central, authorized evaluation of the data is possible. Log data is deleted if it is no longer required for the purpose for which they were collected. Between logging servers and the assets to be logged, authentication takes place to protect the integrity and authenticity of the information transmitted and stored. The transfer takes place using state-of-the-art encryption or a dedicated administration network (out-of-band management).	**MON-06.** OVHcloud has documented policies and procedures regarding protection requirements, lifecycle and retention of logs on its systems, that include: • Access only to authorized users and systems; • Backup and retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
OPS-15	The log data generated allows an unambiguous identification of user accesses at tenant level to support (forensic) analysis in the event of a security incident. Interfaces are available to conduct forensic analyses and perform backups of	**MON-03.** Activity logs on the administration infrastructure are centralized on dedicated syslog servers and are automatically monitored according to defined scenarios in order to detect potential security events. Detected events are raised through alerts to the appropriate departments for investigation and corrective action.

Ref.	C5 Requirement	OVHcloud Control
	infrastructure components and their network communication.	Access logs on the bastions are monitored automatically and alerts are raised when suspicious events occur according to predefined patterns. Investigations and corrective actions are performed in a timely manner.
		MON-04. As part of its monitoring processes, OVHcloud monitors the logging and monitoring components in order to detect any failure that could cause the logging to stop or that could alter the logs. Failures are automatically reported, and corrective actions are taken in a timely manner.
		CUS-10. OVHcloud provides its customers with dedicated tools for monitoring and supervision of their Public Cloud. These tools provide information regarding system performance and availability and include alerts and error handling mechanisms.
		MON-05. OVHcloud has documented policies and procedures regarding the logging and monitoring of events on system components, that include: • Operational aspects of logging and monitoring (logs generation, lifecycle, retention, review and alerting); • Time synchronization of system components; and • Compliance with legal and regulatory frameworks.
		MON-06. OVHcloud has documented policies and procedures regarding protection requirements, lifecycle and retention of logs on its systems, that include: • Access only to authorized users and systems; • Backup and retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.
		MON-01. External access by OVHcloud personnel is logged by the VPN with the following information: accessor IP address, date and event type. Logs are retained for at least 1 year.
		IAM-08. Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.

Ref.	C5 Requirement	OVHcloud Control
OPS-16	Access to system components for logging and monitoring in the Cloud Service Provider's area of responsibility is restricted to authorized users. Changes to the configuration are made in accordance with the applicable policies (cf. DEV-03).	**IAM-05.** OVHcloud has designed a set of business roles corresponding to users' job functions to provide with the strict authorizations to access relevant systems and components they need to complete their functions.
		IAM-08. Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
OPS-17	The Cloud Service Provider monitors the system components for logging and monitoring in its area of responsibility. Failures are automatically and promptly reported to the Cloud Service Provider's responsible departments so that these can assess the failures and take required action.	**MON-04.** As part of its monitoring processes, OVHcloud monitors the logging and monitoring components in order to detect any failure that could cause the logging to stop or that could alter the logs. Failures are automatically reported, and corrective actions are taken in a timely manner.
OPS-18	Guidelines and instructions with technical and organizational measures are documented, communicated and provided in accordance with SP-01 to ensure the timely identification and addressing of vulnerabilities in the system components used to provide the cloud service. These guidelines and instructions contain specifications regarding the following aspects: • Regular identification of vulnerabilities; • Assessment of the severity of identified vulnerabilities; • Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and • Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.	**SEC-02.** Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		SEC-06. OVHcloud uses CVSS (Common Vulnerability Scoring System) for the scoring of vulnerabilities and relies on the online NIST database as well as other sources for the discovery of vulnerabilities. Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities are based on a list of assets ordered by criticality that relies on product-specific criteria for each Public Cloud product. Security patches are then deployed within a time-frame based on asset criticality.
		CHG-02. OVHcloud requires all changes, including maintenance activities, to be documented and tracked from initiation through change validation and deployment. Moreover, OVHcloud have a troubleshooting

Ref.	C5 Requirement	OVHcloud Control
		procedure through which operations teams monitor configuration files changes and other changes in the production environment.
		GOV-01. A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security

Ref.	C5 Requirement	OVHcloud Control
		incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.
OPS-19	The Cloud Service Provider has penetration tests carried out by qualified internal personnel or external service providers at least once a year. The penetration tests are carried out according to a documented test methodology and include the system components relevant to the provision of the cloud service in the area of responsibility of the Cloud Service Provider, which have been identified as such in a risk analysis. The Cloud Service Provider assess the severity of the findings made in penetration tests according to defined criteria. For findings with medium or high criticality regarding the confidentiality, integrity or availability of the cloud service, actions must be taken within defined time windows for prompt remediation or mitigation.	**SEC-02.** Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		SEC-06. OVHcloud uses CVSS (Common Vulnerability Scoring System) for the scoring of vulnerabilities and relies on the online NIST database as well as other sources for the discovery of vulnerabilities. Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities are based on a list of assets ordered by criticality that relies on product-specific criteria for each Public Cloud product. Security patches are then deployed within a time-frame based on asset criticality.
OPS-20	The Cloud Service Provider regularly measures, analyses and assesses the procedures with which vulnerabilities and incidents are handled to verify their continued suitability, appropriateness and effectiveness. Results are evaluated at least quarterly by accountable departments at the Cloud Service Provider to initiate continuous improvement actions and to verify their effectiveness.	**IM-02.** On an annual basis, a crisis unit simulation is performed to ensure the incident response procedures are up-to-date and accurate. When updating the incident response plan, lessons learned are used to implement changes to ensure that incident response procedures are effective.
OPS-21	The Cloud Service Provider periodically informs the cloud customer on the status of incidents affecting the cloud customer, or, where appropriate and necessary, involve the customer in the resolution, in a manner consistent with the contractual agreements. As soon as an incident has been resolved from the Cloud Service Provider's perspective, the cloud customer is informed according to the contractual agreements, about the actions taken.	**IM-05.** When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.
		CHG-06. Planned changes to system components that affect the service availability are communicated to clients through the OVHcloud's website. This communication is made 72 hours before the change implementation.
OPS-22	System components in the area of responsibility of the Cloud Service Provider for the provision of the cloud service are automatically checked for known	**SEC-02.** Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible

Ref.	C5 Requirement	OVHcloud Control
	vulnerabilities at least once a month in accordance with the policies for handling vulnerabilities (cf. OPS-18), the severity is assessed in accordance with defined criteria and measures for timely remediation or mitigation are initiated within defined time windows.	with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		SEC-06. OVHcloud uses CVSS (Common Vulnerability Scoring System) for the scoring of vulnerabilities and relies on the online NIST database as well as other sources for the discovery of vulnerabilities. Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities are based on a list of assets ordered by criticality that relies on product-specific criteria for each Public Cloud product. Security patches are then deployed within a time-frame based on asset criticality.
OPS-23	System components in the production environment used to provide the cloud service under the Cloud Service Provider's responsibility are hardened according to generally accepted industry standards. The hardening requirements for each system component are documented. If non-modifiable ("immutable") images are used, compliance with the hardening specifications as defined in the hardening requirements is checked upon creation of the images. Configuration and log files regarding the continuous availability of the images are retained.	**SEC-05.** System components used to provide the services on the Public Cloud perimeter are hardened according to generally accepted industry standards. The use of a hardened operating system known as the Hardened Debian distribution provided by Digit Core (based on CIS configuration) is encouraged. Moreover, for CI/CD, the use of collaborative tools like Puppet or Bitbucket is mandatory to ensure versioning or integrity monitoring.
OPS-24	Cloud customer data stored and processed on shared virtual and physical resources is securely and strictly separated according to a documented approach based on OIS-07 risk analysis to ensure the confidentiality and integrity of this data.	**NET-01.** End user and server workload network traffic is segmented to support isolation. Moreover, there are dedicated networks for the administrative management of the infrastructure. These networks are separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication.
		NET-07. Incoming and outgoing traffic is formally identified and limited to what is strictly necessary according to the firewall rules. System firewalls are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined and validated by the Information Security Operational Referent (ROSI) or appropriate validator.
		NET-10. The documentation of the logical structure of the network used to provision and operate the service is traceable and up-to-date and made available to the employees on the internal documentation system. The documentation shows how the subnets are allocated and how the network is zoned and segmented.

Ref.	C5 Requirement	OVHcloud Control
OPS-01	The planning of capacities and resources (personnel and IT resources) follows an established procedure in order to avoid possible capacity bottlenecks. The procedures include forecasting future capacity requirements in order to identify usage trends and manage system overload. Cloud Service Providers take appropriate measures to ensure that they continue to meet the requirements agreed with cloud customers for the provision of the cloud service in the event of capacity bottlenecks or outages regarding personnel and IT resources, in particular those relating to the dedicated use of system components, in accordance with the respective agreements.	**GOV-03.** During its ongoing and periodic business planning and budgeting process, management evaluates the need for additional tools and resources in order to achieve business objectives.
		MON-02. Use of system components is monitored against acceptable tolerance levels using dedicated tools. Moreover, provisioning and de-provisioning of cloud services are monitored continuously in order to adapt hardware orders and equipment availability. Actual capacity and service provision levels are monitored according to specifities of teams and products.
OPS-02	Technical and organizational safeguards for the monitoring and provisioning and de-provisioning of cloud services are defined. Thus, the Cloud Service Provider ensures that resources are provided and/or services are rendered according to the contractual agreements and that compliance with the service level agreements is ensured.	**MON-02.** Use of system components is monitored against acceptable tolerance levels using dedicated tools. Moreover, provisioning and de-provisioning of cloud services are monitored continuously in order to adapt hardware orders and equipment availability. Actual capacity and service provision levels are monitored according to specifities of teams and products.
OPS-03	Depending on the capabilities of the respective service model, the cloud customer can control and monitor the allocation of the system resources assigned to the customer for administration/use in order to avoid overcrowding of resources and to achieve sufficient performance.	**CUS-14.** OVHcloud provides Public Cloud customers with mechanisms to control and monitor the capacity and allocation of resources using dedicated tools in order to ensure sufficient performance and efficient use of resources.

Ref.	C5 Requirement	OVHcloud Control
OPS-04	Policies and instructions that provide protection against malware are documented, communicated, and provided in accordance with SP-01 with respect to the following aspects: • Use of system-specific protection mechanisms; • Operating protection programs on system components under the responsibility of the Cloud Service Provider that are used to provide the cloud service in the production environment; and • Operation of protection programs for employees' terminal equipment.	**SEC-01.** OVHcloud's procedures on antivirus and anti-malware protection are documented and communicated through its intranet. Antivirus and anti-malware program is implemented and kept updated on workstations and laptops to provide for the interception or detection and remediation of malware.
OPS-05	System components under the Cloud Service Provider's responsibility that are used to deploy the cloud service in the production environment are configured with malware protection according to the policies and instructions. If protection programs are set up with signature and behavior-based malware detection and removal, these protection programs are updated at least daily.	**SEC-01.** OVHcloud's procedures on antivirus and anti-malware protection are documented and communicated through its intranet. Antivirus and anti-malware program is implemented and kept updated on workstations and laptops to provide for the interception or detection and remediation of malware.
OPS-06	Policies and instructions for data backup and recovery are documented, communicated and provided in accordance with SP-01 regarding the following aspects. • The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the cloud customers and the Cloud Service Provider's operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); • Data is backed up in encrypted, state-of-the-art form; • Access to the backed-up data and the execution of restores is performed only by authorized persons; and • Tests of recovery procedures (cf. OPS-08).	**BAC-01.** Backup restoration tests are performed at least annually for internal data related to the Public Cloud solution administration. Potential errors are immediately investigated and corrected during restoration tests. **BAC-02.** Procedures for data backup and recovery are documented and include the frequency of data backup as well as the data retention duration. Backups are performed and monitored using an automated system and corrective actions are taken in a timely manner in case of anomaly. **BAC-04.** The ability to modify backup schedules is restricted to the authorized personnel.
OPS-07	The execution of data backups is monitored by technical and organizational measures. Malfunctions are investigated by qualified staff and rectified promptly to ensure compliance with contractual obligations to cloud customers or the Cloud Service	**BAC-02.** Procedures for data backup and recovery are documented and include the frequency of data backup as well as the data retention duration. Backups are performed and monitored using an automated system and corrective actions are taken in a timely manner in case of anomaly.

Ref.	C5 Requirement	OVHcloud Control
	Provider's business requirements regarding the scope and frequency of data backup and the duration of storage.	**BAC-04.** The ability to modify backup schedules is restricted to the authorized personnel.
OPS-08	Restore procedures are tested regularly, at least annually. The tests allow an assessment to be made as to whether the contractual agreements as well as the specifications for the maximum tolerable downtime (Recovery Time Objective, RTO) and the maximum permissible data loss (Recovery Point Objective, RPO) are adhered to (cf. BCM-02). Deviations from the specifications are reported to the responsible personnel or system components so that these can promptly assess the deviations and initiate the necessary actions.	**BAC-01.** Backup restoration tests are performed at least annually for internal data related to the Public Cloud solution administration. Potential errors are immediately investigated and corrected during restoration tests.
OPS-09	The Cloud Service Provider transfers data to be backed up to a remote location or transports these on backup media to a remote location. If the data backup is transmitted to the remote location via a network, the data backup or the transmission of the data takes place in an encrypted form that corresponds to the state-of-the-art. The distance to the main site is chosen after sufficient consideration of the factors recovery times and impact of disasters on both sites. The physical and environmental security measures at the remote site are at the same level as at the main site.	**BAC-02.** Procedures for data backup and recovery are documented and include the frequency of data backup as well as the data retention duration. Backups are performed and monitored using an automated system and corrective actions are taken in a timely manner in case of anomaly.
		NET-06. OVHcloud has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information.
		BAC-03. For each Public Cloud product, the redundancy model is based on risk assessment, technical specifications and operational constraints. These elements define the choices for replication locally or at remote sites and the different possible failure scales (network, room, DC). The infrastructure of Public Cloud products is based on scalability and Software Design Storage principles, meaning that the configuration of the control plane can change at will, depending on the customers needs and the technical constraints. Moreoever, as the control planes use stateless components, they can be created or modified by simply redeploying the altered components from the code repositories.

Ref.	C5 Requirement	OVHcloud Control
		Geo-redundancy of the control plane is assured for most Public Cloud products on two locations at least (Compute, Block Storage, Kubernetes and Data). On the other side, Object Storage is a mono-datacenter offer, that does not provide yet geo-redundacy of the control plane. However, resilience is assured thanks to the OpenIO and Swift software model.
OPS-10	The Cloud Service Provider has established policies and instructions that govern the logging and monitoring of events on system components within its area of responsibility. These policies and instructions are documented, communicated and provided according to SP-01 with respect to the following aspects: • Definition of events that could lead to a violation of the protection goals; • Specifications for activating, stopping and pausing the various logs; • Information regarding the purpose and retention period of the logs. • Define roles and responsibilities for setting up and monitoring logging; • Time synchronization of system components; and • Compliance with legal and regulatory frameworks.	**MON-05.** OVHcloud has documented policies and procedures regarding the logging and monitoring of events : • Operational aspects of logging and monitoring (logs generation, lifecycle, retention, review and alerting); • Time synchronization of system components; and • Compliance with legal and regulatory frameworks.
OPS-11	Policies and instructions for the secure handling of metadata (usage data) are documented, communicated and provided according to SP-01 with regard to the following aspects: • Metadata is collected and used solely for billing, incident management and security incident management purposes; • Exclusively anonymous metadata to deploy and enhance the cloud service so that no conclusions can be drawn about the cloud customer or user; • No commercial use; • Storage for a fixed period reasonably related to the purposes of the collection; • Immediate deletion if the purposes of the collection are fulfilled and further storage is no longer necessary. • Provision to cloud customers according to contractual agreements.	**GOV-19.** As part of contract execution, the metadata collected by OVHcloud is used for the purposes of business management, information and support, claims management, invoicing and accounting, payment management, process improvement and customer relationship management. The collected data, its usage and its retention period are documented.

Ref.	C5 Requirement	OVHcloud Control
OPS-12	The requirements for the logging and monitoring of events and for the secure handling of metadata are implemented by technically supported procedures with regard to the following restrictions: • Access only to authorized users and systems; • Retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.	**MON-06.** OVHcloud has documented policies and procedures regarding protection requirements, lifecycle and retention of logs on its systems, that include: • Access only to authorized users and systems; • Backup and retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.
OPS-13	The logging data is automatically monitored for events that may violate the protection goals in accordance with the logging and monitoring requirements. This also includes the detection of relationships between events (event correlation). Identified events are automatically reported to the appropriate departments for prompt evaluation and action.	**MON-03.** Activity logs on the administration infrastructure are centralized on dedicated syslog servers and are automatically monitored according to defined scenarios in order to detect potential security events. Detected events are raised through alerts to the appropriate departments for investigation and corrective action. Access logs on the bastions are monitored automatically and alerts are raised when suspicious events occur according to predefined patterns. Investigations and corrective actions are performed in a timely manner.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
OPS-14	The Cloud Service Provider retains the generated log data and keeps these in an appropriate, unchangeable and aggregated form, regardless of the source of such data, so that a central, authorized evaluation of the data is possible. Log data is deleted if it is no longer required for the purpose for which they were collected. Between logging servers and the assets to be logged, authentication takes place to protect the integrity and authenticity of the information transmitted and stored. The transfer takes place using state-of-the-art encryption or a dedicated administration network (out-of-band management).	**MON-06.** OVHcloud has documented policies and procedures regarding protection requirements, lifecycle and retention of logs on its systems, that include: • Access only to authorized users and systems; • Backup and retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
OPS-15	The log data generated allows an unambiguous identification of user accesses at tenant level to support (forensic) analysis in the event of a security incident. Interfaces are available to conduct forensic analyses and perform backups of	**MON-03.** Activity logs on the administration infrastructure are centralized on dedicated syslog servers and are automatically monitored according to defined scenarios in order to detect potential security events. Detected events are raised through alerts to the appropriate departments for investigation and corrective action.

Ref.	C5 Requirement	OVHcloud Control
	infrastructure components and their network communication.	Access logs on the bastions are monitored automatically and alerts are raised when suspicious events occur according to predefined patterns. Investigations and corrective actions are performed in a timely manner.
		MON-04. As part of its monitoring processes, OVHcloud monitors the logging and monitoring components in order to detect any failure that could cause the logging to stop or that could alter the logs. Failures are automatically reported, and corrective actions are taken in a timely manner.
		CUS-10. OVHcloud provides its customers with dedicated tools for monitoring and supervision of their Public Cloud. These tools provide information regarding system performance and availability and include alerts and error handling mechanisms.
		MON-05. OVHcloud has documented policies and procedures regarding the logging and monitoring of events on system components, that include: • Operational aspects of logging and monitoring (logs generation, lifecycle, retention, review and alerting); • Time synchronization of system components; and • Compliance with legal and regulatory frameworks.
		MON-06. OVHcloud has documented policies and procedures regarding protection requirements, lifecycle and retention of logs on its systems, that include: • Access only to authorized users and systems; • Backup and retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.
		MON-01. External access by OVHcloud personnel is logged by the VPN with the following information: accessor IP address, date and event type. Logs are retained for at least 1 year.
		IAM-08. Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.

Ref.	C5 Requirement	OVHcloud Control
OPS-16	Access to system components for logging and monitoring in the Cloud Service Provider's area of responsibility is restricted to authorized users. Changes to the configuration are made in accordance with the applicable policies (cf. DEV-03).	**IAM-05.** OVHcloud has designed a set of business roles corresponding to users' job functions to provide with the strict authorizations to access relevant systems and components they need to complete their functions.
		IAM-08. Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
OPS-17	The Cloud Service Provider monitors the system components for logging and monitoring in its area of responsibility. Failures are automatically and promptly reported to the Cloud Service Provider's responsible departments so that these can assess the failures and take required action.	**MON-04.** As part of its monitoring processes, OVHcloud monitors the logging and monitoring components in order to detect any failure that could cause the logging to stop or that could alter the logs. Failures are automatically reported, and corrective actions are taken in a timely manner.
OPS-18	Guidelines and instructions with technical and organizational measures are documented, communicated and provided in accordance with SP-01 to ensure the timely identification and addressing of vulnerabilities in the system components used to provide the cloud service. These guidelines and instructions contain specifications regarding the following aspects: • Regular identification of vulnerabilities; • Assessment of the severity of identified vulnerabilities; • Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and • Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.	**SEC-02.** Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		SEC-06. OVHcloud uses CVSS (Common Vulnerability Scoring System) for the scoring of vulnerabilities and relies on the online NIST database as well as other sources for the discovery of vulnerabilities. Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities are based on a list of assets ordered by criticality that relies on product-specific criteria for each Public Cloud product. Security patches are then deployed within a time-frame based on asset criticality.
		CHG-02. OVHcloud requires all changes, including maintenance activities, to be documented and tracked from initiation through change validation and deployment. Moreover, OVHcloud have a troubleshooting

Ref.	C5 Requirement	OVHcloud Control
		procedure through which operations teams monitor configuration files changes and other changes in the production environment.
		GOV-01. A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security

Ref.	C5 Requirement	OVHcloud Control
		incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.
OPS-19	The Cloud Service Provider has penetration tests carried out by qualified internal personnel or external service providers at least once a year. The penetration tests are carried out according to a documented test methodology and include the system components relevant to the provision of the cloud service in the area of responsibility of the Cloud Service Provider, which have been identified as such in a risk analysis. The Cloud Service Provider assess the severity of the findings made in penetration tests according to defined criteria. For findings with medium or high criticality regarding the confidentiality, integrity or availability of the cloud service, actions must be taken within defined time windows for prompt remediation or mitigation.	**SEC-02.** Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		SEC-06. OVHcloud uses CVSS (Common Vulnerability Scoring System) for the scoring of vulnerabilities and relies on the online NIST database as well as other sources for the discovery of vulnerabilities. Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities are based on a list of assets ordered by criticality that relies on product-specific criteria for each Public Cloud product. Security patches are then deployed within a time-frame based on asset criticality.
OPS-20	The Cloud Service Provider regularly measures, analyses and assesses the procedures with which vulnerabilities and incidents are handled to verify their continued suitability, appropriateness and effectiveness. Results are evaluated at least quarterly by accountable departments at the Cloud Service Provider to initiate continuous improvement actions and to verify their effectiveness.	**IM-02.** On an annual basis, a crisis unit simulation is performed to ensure the incident response procedures are up-to-date and accurate. When updating the incident response plan, lessons learned are used to implement changes to ensure that incident response procedures are effective.
OPS-21	The Cloud Service Provider periodically informs the cloud customer on the status of incidents affecting the cloud customer, or, where appropriate and necessary, involve the customer in the resolution, in a manner consistent with the contractual agreements. As soon as an incident has been resolved from the Cloud Service Provider's perspective, the cloud customer is informed according to the contractual agreements, about the actions taken.	**IM-05.** When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.
		CHG-06. Planned changes to system components that affect the service availability are communicated to clients through the OVHcloud's website. This communication is made 72 hours before the change implementation.
OPS-22	System components in the area of responsibility of the Cloud Service Provider for the provision of the cloud service are automatically checked for known	**SEC-02.** Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible

Ref.	C5 Requirement	OVHcloud Control
	vulnerabilities at least once a month in accordance with the policies for handling vulnerabilities (cf. OPS-18), the severity is assessed in accordance with defined criteria and measures for timely remediation or mitigation are initiated within defined time windows.	with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		SEC-06. OVHcloud uses CVSS (Common Vulnerability Scoring System) for the scoring of vulnerabilities and relies on the online NIST database as well as other sources for the discovery of vulnerabilities. Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities are based on a list of assets ordered by criticality that relies on product-specific criteria for each Public Cloud product. Security patches are then deployed within a time-frame based on asset criticality.
OPS-23	System components in the production environment used to provide the cloud service under the Cloud Service Provider's responsibility are hardened according to generally accepted industry standards. The hardening requirements for each system component are documented. If non-modifiable ("immutable") images are used, compliance with the hardening specifications as defined in the hardening requirements is checked upon creation of the images. Configuration and log files regarding the continuous availability of the images are retained.	**SEC-05.** System components used to provide the services on the Public Cloud perimeter are hardened according to generally accepted industry standards. The use of a hardened operating system known as the Hardened Debian distribution provided by Digit Core (based on CIS configuration) is encouraged. Moreover, for CI/CD, the use of collaborative tools like Puppet or Bitbucket is mandatory to ensure versioning or integrity monitoring.
OPS-24	Cloud customer data stored and processed on shared virtual and physical resources is securely and strictly separated according to a documented approach based on OIS-07 risk analysis to ensure the confidentiality and integrity of this data.	**NET-01.** End user and server workload network traffic is segmented to support isolation. Moreover, there are dedicated networks for the administrative management of the infrastructure. These networks are separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication.
		NET-07. Incoming and outgoing traffic is formally identified and limited to what is strictly necessary according to the firewall rules. System firewalls are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined and validated by the Information Security Operational Referent (ROSI) or appropriate validator.
		NET-10. The documentation of the logical structure of the network used to provision and operate the service is traceable and up-to-date and made available to the employees on the internal documentation system. The documentation shows how the subnets are allocated and how the network is zoned and segmented.

IDM: Identity and Access Management
Control Objective: Secure the authorization and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorized access.

Ref.	C5 Requirement	OVHcloud Control
IDM-01	A role and rights concept based on the business and security requirements of the Cloud Service Provider as well as a policy for managing user accounts and access rights for internal and external employees of the Cloud Service Provider and system components that have a role in automated authorization processes of the Cloud Service Provider are documented, communicated and made available according to SP-01: • Assignment of unique usernames; • Granting and modifying user accounts and access rights based on the “least-privilege-principle” and the “need-to-know” principle; • Segregation of duties between operational and monitoring functions (“Segregation of Duties”); • Segregation of duties between managing, approving and assigning user accounts and access rights; • Approval by authorized individual(s) or system(s) for granting or modifying user accounts and access rights before data of the cloud customer or system components used to provision the cloud service can be accessed; • Regular review of assigned user accounts and access rights; • Blocking and removing access accounts in the event of inactivity; • Time-based or event-driven removal or adjustment of access rights in the event of changes to job responsibility; • Two-factor or multi-factor authentication for users with privileged access; • Requirements for the approval and documentation of the management of user accounts and access rights.	**IAM-03.** Generic accounts are used on OVHcloud servers used to manage the cloud service. Access to and use of the generic accounts is traced in the bastions and users are clearly identifiable. Logs of the usage of generic accounts contain the following information: source IP address, username of the accessor, type of access, request made. In addition, a capture of the session is made and can be replayed. Bastion logs are saved for at least one year.
		IAM-04. In-scope system components require unique username, passwords or authorized SSH keys prior to user authentication.
		IAM-01. Logical access is revoked in a timely manner as part of the termination process and any assets handed over are provably returned upon termination of employment.
		IAM-02. Perimeter entrance requires a documented access request and manager approval prior to access being provisioned. Logical access rights within a perimeter are granted by authorized and approved granters based on rules of need to know and least privilege.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.

Ref.	C5 Requirement	OVHcloud Control
		IAM-10. Passwords for in-scope system components are configured according to OVHcloud's password policy.
		IAM-08. Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		IAM-06. Business roles are reviewed on a bi-annual basis by the business role owners ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.

Ref.	C5 Requirement	OVHcloud Control
IDM-02	Specified procedures for granting and modifying user accounts and access rights for internal and external employees of the Cloud Service Provider as well as for system components involved in automated authorization processes of the Cloud Service Provider ensure compliance with the role and rights concept as well as the policy for managing user accounts and access rights.	**IAM-08.** Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
		IAM-02. Perimeter entrance requires a documented access request and manager approval prior to access being provisioned. Logical access rights within a perimeter are granted by authorized and approved granters based on rules of need to know and least privilege.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.
IDM-03	User accounts of internal and external employees of the Cloud Service Provider as well as for system components involved in automated authorization processes of the Cloud Service Provider are automatically locked if they have not been used for a period of two months. Approval from authorized personnel or system components are	**IAM-11.** OVHcloud employees' accounts on the bastions are automatically deactivated if they have not been used for a period of 90 days. Locked accounts are reactivated by authorized users.
		IAM-06. Business roles are reviewed on a bi-annual basis by the business role owners ensuring roles remain relevant

Ref.	C5 Requirement	OVHcloud Control
	required to unlock these accounts. Locked user accounts are automatically revoked after six months. After revocation, the procedure for granting user accounts and access rights (cf. IDM-02) must be repeated.	over time, based on the principle of least privilege and exempt of conflicting responsibilities.

Ref.	C5 Requirement	OVHcloud Control
IDM-04	Access rights are promptly revoked if the job responsibilities of the Cloud Service Provider's internal or external staff or the tasks of system components involved in the Cloud Service Provider's automated authorization processes change. Privileged access rights are adjusted or revoked within 48 hours after the change taking effect. All other access rights are adjusted or revoked within 14 days. After revocation, the procedure for granting user accounts and access rights (cf. IDM-02) must be repeated.	**IAM-11.** OVHcloud employees' accounts on the bastions are automatically deactivated if they have not been used for a period of 90 days. Locked accounts are reactivated by authorized users.
		IAM-01. Logical access is revoked in a timely manner as part of the termination process and any assets handed over are provably returned upon termination of employment.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.
		PHY-05. Access to the datacenter is revoked in a timely manner as part of the termination process.
IDM-05	Access rights of internal and external employees of the Cloud Service Provider as well as of system components that play a role in automated authorization processes of the Cloud Service Provider are reviewed at least once a year to ensure that they still correspond to the actual area of use. The review is carried out by authorized persons from the Cloud Service Provider's organizational units, who can assess the appropriateness of the assigned access rights based on their knowledge of the task areas of the employees or system components. Identified deviations will be dealt with promptly, but no later than 7 days after their detection, by appropriate modification or withdrawal of the access rights.	**IAM-06.** Business roles are reviewed on a bi-annual basis by the business role owners ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities.

Ref.	C5 Requirement	OVHcloud Control
IDM-06	Privileged access rights for internal and external employees as well as technical users of the Cloud Service Provider are assigned and changed in accordance to the policy for managing user accounts and access rights (cf. IDM-01) or a separate specific policy. Privileged access rights are personalized, limited in time according to a risk assessment and assigned as necessary for the execution of tasks ("need-to-know principle"). Technical users are assigned to internal or external employees of the Cloud Service Provider. Activities of users with privileged access rights are logged in order to detect any misuse of privileged access in suspicious cases. The logged information is automatically monitored for defined events that may indicate misuse. When such an event is identified, the responsible personnel are automatically informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken in accordance with HR-04.	**IAM-08.** Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.
		MON-07. Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.
IDM-07	The cloud customer is informed by the Cloud Service Provider whenever internal or external employees of the Cloud Service Provider read or write to the cloud customer's data processed, stored or transmitted in the cloud service or have accessed it without the prior consent of the cloud customer. The Information is provided whenever data of the cloud customer is/was not encrypted, the encryption is/was disabled for access or the contractual agreements do not explicitly exclude such information. The information contains the cause, time, duration, type and scope of the access. The information is sufficiently detailed to enable subject matter experts of the cloud customer to assess the risks of the access. The information is provided in accordance with the contractual agreements, or within 72 hours after the access.	**IAM-13.** Access to customer data and infrastructure by OVHcloud employees is traced through bastions.

Ref.	C5 Requirement	OVHcloud Control
IDM-08	The allocation of authentication information to access system components used to provide the cloud service to internal and external users of the cloud provider and system components that are involved in automated authorization processes of the cloud provider is done in an orderly manner that ensures the confidentiality of the information. If passwords are used as authentication information, their confidentiality is ensured by the following procedures, as far as technically possible: • Users can initially create the password themselves or must change an initial password when logging on to the system component for the first time. An initial password loses its validity after a maximum of 14 days. • When creating passwords, compliance with the password specifications (cf. IDM-12) is enforced as far as technically possible. • The user is informed about changing or resetting the password. • The server-side storage takes place using cryptographically strong hash functions. Deviations are evaluated by means of a risk analysis and mitigating measures derived from this are implemented.	**IAM-12.** OVHcloud has established a secure password configuration policy for in-scope system components that includes: • Restriction on password length and complexity (use of alphanumeric, upper- and lower-case characters); • Password age must not exceed 90 days; • The server-side storage takes place using cryptographically strong hash functions; • Guidelines and instructions on the secure handling and protection of passwords.
IDM-09	System components in the Cloud Service Provider's area of responsibility that are used to provide the cloud service, authenticate users of the Cloud Service Provider's internal and external employees as well as system components that are involved in the Cloud Service Provider's automated authorization processes. Access to the production environment requires two-factor or multi-factor authentication. Within the production environment, user authentication takes place through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security. If digitally signed certificates are used, administration is carried out in accordance with the Guideline for Key Management (cf. CRY-01). The password requirements are derived from a risk assessment and documented, communicated and provided in a password policy according to SP-01. Compliance with the requirements is enforced by the configuration of the system components, as far as technically possible.	**IAM-04.** In-scope system components require unique username, passwords or authorized SSH keys prior to user authentication. **IAM-07.** OVHcloud permits remote access to production systems by authorized employees, using authorized devices and over encrypted virtual private network (VPN) connection. **IAM-10.** Passwords for in-scope system components are configured according to OVHcloud's password policy.

CRY: Cryptography and Key Management
Control Objective: Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.

Ref.	C5 Requirement	OVHcloud Control
CRY-01	Policies and instructions with technical and organizational safeguards for encryption procedures and key management are documented, communicated and provided according to SP-01, in which the following aspects are described: • Usage of strong encryption procedures and secure network protocols that correspond to the state-of-the-art; • Risk-based provisions for the use of encryption which are aligned with the data classification schemes and consider the communication channel, type, strength and quality of the encryption; • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys; and • Consideration of relevant legal and regulatory obligations and requirements.	**SEC-09.** Policies and procedures for data encryption are documented and include: • Usage of strong and trusted encryption procedures and secure network protocols that correspond to the state-of-the-art, such as trusted symmetric encryption algorithms, trusted hashing algorithms, trusted one-way password encryption algorithms, trusted key exchange algorithms, trusted SSL/TLS Protocols and certificates... etc. • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys.
CRY-02	The Cloud Service Provider has established procedures and technical measures for strong encryption and authentication for the transmission of data of cloud customers over public networks.	**IAM-04.** In-scope system components require unique username, passwords or authorized SSH keys prior to user authentication.
		NET-06. OVHcloud has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information.
		IAM-07. OVHcloud permits remote access to production systems by authorized employees, using authorized devices and over encrypted virtual private network (VPN) connection.
CRY-04	Procedures and technical safeguards for secure key management in the area of responsibility of the Cloud Service Provider include at least the following aspects: • Generation of keys for different cryptographic systems and applications; • Issuing and obtaining public-key certificates; • Provisioning and activation of the keys; • Secure storage of keys (separation of key management system from application and middleware level) including description of how authorized users get access; • Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes	**SEC-10.** OVHcloud has documented a key management policy that describes the process of secure key management that include: • Keys generation in a secure Locker / Vault using trusted and secure algorithms; • Key storage and communication over secure channels; Key lifecycle and disposal.

Ref.	C5 Requirement	OVHcloud Control
	and/or updates are to be realized; • Handling of compromised keys; • Withdrawal and deletion of keys; and • If pre-shared keys are used, the specific provisions relating to the safe use of this procedure are specified separately.	

COS: Communication Security
Control Objective: Ensure the protection of information in networks and the corresponding information processing systems

Ref.	C5 Requirement	OVHcloud Control
COS-01	Based on the results of a risk analysis carried out according to OIS-06, the Cloud Service Provider has implemented technical safeguards which are suitable to promptly detect and respond to network-based attacks on the basis of irregular incoming or outgoing traffic patterns and/or Distributed Denial- of-Service (DDoS) attacks. Data from corresponding technical protection measures implemented is fed into a comprehensive SIEM (Security Information and Event Management) system, so that (counter) measures regarding correlating events can be initiated. The safeguards are documented, communicated and provided in accordance with SP-01.	**NET-06.** OVHcloud has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information.
		NET-03. Intrusion detection systems and other technical measures are implemented in order to detect and response to network-based attacks, including network monitoring and traffic filtering.
		IAM-07. OVHcloud permits remote access to production systems by authorized employees, using authorized devices, with multi-factor authentication (MFA) and over encrypted virtual private network (VPN) connection.
		NET-10. The documentation of the logical structure of the network used to provision and operate the service is traceable and up-to-date and made available to the employees on the internal documentation system. The documentation shows how the subnets are allocated and how the network is zoned and segmented.
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.
		NET-09. Virtual hosts are behind software firewalls which are configured to prevent TCP/IP spoofing, packet sniffing, and restrict incoming connections to customer-specified ports.
COS-02	Specific security requirements are designed, published and provided for establishing connections within the Cloud Service Provider's network. The security requirements define for the Cloud Service Provider's area of responsibility:	**NET-01.** End user and server workload network traffic is segmented to support isolation. Moreover, there are dedicated networks for the administrative management of the infrastructure. These networks are separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication.

Ref.	C5 Requirement	OVHcloud Control
	• in which cases the security zones are to be separated and in which cases cloud customers are to be logically or physically segregated; • which communication relationships and which network and application protocols are permitted in each case; • how the data traffic for administration and monitoring is segregated from each on network level; • which internal, cross-location communication is permitted and; • which cross-network communication is allowed	**NET-03.** Intrusion detection systems and other technical measures are implemented in order to detect and response to network-based attacks, including network monitoring and traffic filtering.
		NET-07. Incoming and outgoing traffic is formally identified and limited to what is strictly necessary according to the firewall rules. System firewalls are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined and validated by the Information Security Operational Referent (ROSI) or appropriate validator.
		NET-09. Virtual hosts are behind software firewalls which are configured to prevent TCP/IP spoofing, packet sniffing, and restrict incoming connections to customer-specified ports.
		NET-10. The documentation of the logical structure of the network used to provision and operate the service is traceable and up-to-date and made available to the employees on the internal documentation system. The documentation shows how the subnets are allocated and how the network is zoned and segmented.

Ref.	C5 Requirement	OVHcloud Control
COS-03	A distinction is made between trusted and untrusted networks. Based on a risk assessment, these are separated into different security zones for internal and external network areas (and DMZ, if applicable). Physical and virtualized network environments are designed and configured to restrict and monitor the established connection to trusted or untrusted networks according to the defined security requirements. The entirety of the conception and configuration undertaken to monitor the connections mentioned is assessed in a risk-oriented manner, at least annually, with regard to the resulting security requirements. Identified vulnerabilities and deviations are subject to risk assessment in accordance with the risk management procedure (cf. OIS-06) and follow-up measures are defined and tracked (cf. OPS-18). At specified intervals, the business justification for using all services, protocols, and ports is reviewed. The review also includes the justifications for compensatory measures for the use of protocols that are considered insecure.	**NET-07.** Incoming and outgoing traffic is formally identified and limited to what is strictly necessary according to the firewall rules. System firewalls are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined and validated by the Information Security Operational Referent (ROSI) or appropriate validator.
		NET-09. Virtual hosts are behind software firewalls which are configured to prevent TCP/IP spoofing, packet sniffing, and restrict incoming connections to customer-specified ports.
		NET-01. End user and server workload network traffic is segmented to support isolation. Moreover, there are dedicated networks for the administrative management of the infrastructure. These networks are separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication.
COS-04	Each network perimeter is controlled by security gateways. The system access authorization for cross-network access is based on a security assessment based on the requirements of the cloud customers.	**NET-01.** End user and server workload network traffic is segmented to support isolation. Moreover, there are dedicated networks for the administrative management of the infrastructure. These networks are separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication.
		NET-03. Intrusion detection systems and other technical measures are implemented in order to detect and response to network-based attacks, including network monitoring and traffic filtering.
		NET-07. Incoming and outgoing traffic is formally identified and limited to what is strictly necessary according to the firewall rules. System firewalls are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined and validated by the Information Security Operational Referent (ROSI) or appropriate validator.
		NET-09. Virtual hosts are behind software firewalls which are configured to prevent TCP/IP spoofing, packet sniffing, and restrict incoming connections to customer-specified ports.

Ref.	C5 Requirement	OVHcloud Control
		NET-01. End user and server workload network traffic is segmented to support isolation. Moreover, there are dedicated networks for the administrative management of the infrastructure. These networks are separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication.
COS-05	There are separate networks for the administrative management of the infrastructure and for the operation of management consoles. These networks are logically or physically separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication (cf. IDM-09). Networks used by the Cloud Service Provider to migrate or create virtual machines are also physically or logically separated from other networks	**NET-01.** End user and server workload network traffic is segmented to support isolation. Moreover, there are dedicated networks for the administrative management of the infrastructure. These networks are separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication.
COS-07	The documentation of the logical structure of the network used to provision or operate the Cloud Service, is traceable and up-to-date, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions in accordance with contractual obligations. The documentation shows how the subnets are allocated and how the network is zoned and segmented. In addition, the geographical locations in which the cloud customers' data is stored are indicated.	**NET-10.** The documentation of the logical structure of the network used to provision and operate the service is traceable and up-to-date and made available to the employees on the internal documentation system. The documentation shows how the subnets are allocated and how the network is zoned and segmented.
COS-08	Policies and instructions with technical and organizational safeguards in order to protect the transmission of data against unauthorized interception, manipulation, copying, modification, redirection or destruction are documented, communicated and provided according to SP-01. The policy and instructions establish a reference to the classification of information (cf. AM-06).	**IAM-07.** OVHcloud permits remote access to production systems by authorized employees, using authorized devices, with multi-factor authentication (MFA) and over encrypted virtual private network (VPN) connection.
		SEC-09. Policies and procedures for data encryption are documented and include: • Usage of strong and trusted encryption procedures and secure network protocols that correspond to the state-of-the-art, such as trusted symmetric encryption algorithms, trusted hashing algorithms, trusted one-way password encryption algorithms, trusted key exchange algorithms, trusted SSL/TLS Protocols and certificates... etc. • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys.
		NET-13. OVHcloud permits the connection to its internal network via VPN and only to authorized equipment using host-based certificates.
		NET-06. OVHcloud has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information.

Ref.	C5 Requirement	OVHcloud Control
		NET-01. End user and server workload network traffic is segmented to support isolation. Moreover, there are dedicated networks for the administrative management of the infrastructure. These networks are separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication.
		NET-02. Firewall configuration files are automatically promoted to production firewall devices. Thus, firewall rules are regularly reviewed by peers before approving any change in the corresponding configuration files in production, thanks to CI/CD processes and tools.
		NET-03. Intrusion detection systems and other technical measures are implemented in order to detect and response to network-based attacks, including network monitoring and traffic filtering.
		NET-07. Incoming and outgoing traffic is formally identified and limited to what is strictly necessary according to the firewall rules. System firewalls are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined and validated by the Information Security Operational Referent (ROSI) or appropriate validator.

PI: Portability and Interoperability
Control Objective: Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider.

Ref.	C5 Requirement	OVHcloud Control
PI-01	The cloud service can be accessed by other cloud services or IT systems of cloud customers through documented inbound and outbound interfaces. Further, the interfaces are clearly documented for subject matter experts on how they can be used to retrieve the data. Communication takes place through standardized communication protocols that ensure the confidentiality and integrity of the transmitted information according to its protection requirements. Communication over untrusted networks is encrypted according to CRY-02. The type and scope of the documentation on the interfaces is geared to the needs of the cloud customers' subject matter experts in order to enable the use of these interfaces. The information is maintained in such a way that it is applicable for the cloud service's version which is intended for productive use.	**CUS-04.** OVHcloud has developed application programming interfaces (API) allowing its customers to interact with OVHcloud products without using the graphical customer interface. The interfaces are clearly documented for subject matter experts on how they can be used to retrieve the data. The interfaces use the RESTful standard and can be used with different programming languages.

Ref.	C5 Requirement	OVHcloud Control
PI-02	In contractual agreements, the following aspects are defined with regard to the termination of the contractual relationship, insofar as these are applicable to the cloud service: • Type, scope and format of the data the Cloud Service Provider provides to the cloud customer; • Definition of the timeframe, within which the Cloud Service Provider makes the data available to the cloud customer • Definition of the point in time as of which the Cloud Service Provider makes the data inaccessible to the cloud customer and deletes these; and • The cloud customers' responsibilities and obligations to cooperate for the provision of the data. The definitions are based on the needs of subject matter experts of potential customers who assess the suitability of the cloud service with regard to a dependency on the Cloud Service Provider as well as legal and regulatory requirements.	**CUS-05.** OVHcloud has defined in customer contractual agreements, the aspects related to the termination of the contractual relationship. The customer is responsible of taking all the necessary measures in order to ensure the conservation of their data before the cancellation of the service. All content and data stored by the customer as part of the service are deleted within an agreed duration from the expiration date of the service or end of payment.
PI-03	The Cloud Service Provider's procedures for deleting the cloud customers' data upon termination of the contractual relationship ensure compliance with the contractual agreements (cf. PI-02). The deletion includes data in the cloud customer's environment, metadata and data stored in the data backups. The deletion procedures prevent recovery by forensic means.	**CUS-01.** When a customer terminates his contract, a logical erasure, is performed on all the servers concerned. If this logical erasure fails, the concerned hard drives are destroyed according to a defined secure destruction process.

DEV: Procurement, Development and Modification of Information Systems
Control Objective: Ensure information security in the development cycle of information systems.

Ref.	C5 Requirement	OVHcloud Control
DEV-01	Policies and instructions with technical and organizational measures for the secure development of the cloud service are documented, communicated and provided in accordance with SP-01. The policies and instructions contain guidelines for the entire life cycle of the cloud service and are based on recognized standards and methods with regard to the following aspects: • Security in Software Development (Requirements, Design, Implementation, Testing and Verification); • Security in software deployment (including continuous delivery); and • Security in operation (reaction to identified faults and vulnerabilities).	**CHG-07.** OVHcloud has documented policies and procedures for the secure development process that include review and approval, testing, implementation and maintenance.
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.

Ref.	C5 Requirement	OVHcloud Control
DEV-03	Policies and instructions with technical and organizational safeguards for change management of system components of the cloud service within the scope of software deployment are documented, communicated and provided according to SP-01 with regard to the following aspects: • Criteria for risk assessment, categorization and prioritization of changes and related requirements for the type and scope of testing to be performed, and necessary approvals for the development/implementation of the change and releases for deployment in the production environment by authorized personnel or system components; • Requirements for the performance and documentation of tests; / • Requirements for segregation of duties during development, testing and release of changes; / • Requirements for the proper information of cloud customers about the type and scope of the change as well as the resulting obligations to cooperate in accordance with the contractual agreements; • Requirements for the documentation of changes in system, operational and user documentation; and • Requirements for the implementation and documentation of emergency changes that must comply with the same level of security as normal changes.	**CHG-01.** OVHcloud protects confidential and personal information during system design, development, testing, implementation and change processes to meet the OVHcloud's objectives related to confidentiality and privacy.
		CHG-02. OVHcloud requires all changes, including maintenance activities, to be documented and tracked from initiation through change validation and deployment. Moreover, OVHcloud have a troubleshooting procedure through which operations teams monitor configuration files changes and other changes in the production environment.
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are:
		CHG-04. Separate environments are used for development and production. Moreover, data contained in the production environments is not used in development environment in order not to compromise their confidentiality.
		CHG-05. During the development process, all pull requests must be approved by at least one peer reviewer before being pushed to production.
		CHG-06. Planned changes to system components that affect the service availability are communicated to clients through the OVHcloud's website. This communication is made 72 hours before the change implementation.
DEV-04	The Cloud Service Provider provides a training program for regular, target group-oriented security training and awareness for internal and external employees on standards and methods of secure software development and provision as well as on how to use the tools used for this purpose. The program is regularly reviewed and updated with regard to the applicable policies and instructions, the assigned roles and responsibilities and the tools used.	**HR-08.** OVHcloud provides security and awareness training to employees based on identified needs and security hot topics. Target group-oriented awareness and training are addressed on a regular basis providing: - best security practices including references to applicable policies and instructions such as programming good practices, training on internal practices for secure infrastructure and on advanced security including current threat situation; - regular security communications and updates on security news as needed; - secure development communications and training.

Ref.	C5 Requirement	OVHcloud Control
DEV-05	In accordance with the applicable policies (cf. DEV-03), changes are subjected to a risk assessment with regard to potential effects on the system components concerned and are categorized and prioritized accordingly.	**CHG-03.** OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
DEV-06	Changes to the cloud service are subject to appropriate testing during software development and deployment. The type and scope of the tests correspond to the risk assessment. The tests are carried out by appropriately qualified personnel of the Cloud Service Provider or by automated test procedures that comply with the state-of-the-art. Cloud customers are involved into the tests in accordance with the contractual requirements. The severity of the errors and vulnerabilities identified in the tests, which are relevant for the deployment decision, is determined according to defined criteria and actions for timely remediation or mitigation are initiated.	**CHG-03.** OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
DEV-07	System components and tools for source code management and software deployment that are used to make changes to system components of the cloud service in the production environment are subject to a role and rights concept according to IDM-01 and authorization mechanisms. They must be configured in such a way that all changes are logged and can therefore be traced back to the individuals or system components executing them.	**CHG-02.** OVHcloud requires all changes, including maintenance activities, to be documented and tracked from initiation through change validation and deployment. Moreover, OVHcloud have a troubleshooting procedure through which operations teams monitor configuration files changes and other changes in the production environment.
		CHG-04. Separate environments are used for development and production. Moreover, data contained in the production environments is not used in development environment in order not to compromise their confidentiality.
		CHG-09. OVHcloud uses dedicated tools for source code management and software deployment into production. Each developer has specific accesses to the repositories and all changes are logged.
		HR-08. OVHcloud provides security and awareness training to employees based on identified needs and security hot topics. Target group-oriented awareness and training are addressed on a regular basis providing:

Ref.	C5 Requirement	OVHcloud Control
		CHG-05. During the development process, all pull requests must be approved by at least one peer reviewer before being pushed to production.
DEV-08	Version control procedures are set up to track dependencies of individual changes and to restore affected system components back to their previous state as a result of errors or identified vulnerabilities.	**CHG-08.** OVHcloud development teams use version control systems to track changes to the source code and allow to undo the changes in case of errors or identified vulnerabilities.
		CHG-09. OVHcloud uses dedicated tools for source code management and software deployment into production. Each developer has specific accesses to the repositories and all changes are logged.
DEV-09	Authorized personnel or system components of the Cloud Service Provider approve changes to the cloud service based on defined criteria (e.g. test results and required approvals) before these are made available to the cloud customers in the production environment. Cloud customers are involved in the release according to contractual requirements.	**CHG-09.** OVHcloud uses dedicated tools for source code management and software deployment into production. Each developer has specific accesses to the repositories and all changes are logged.
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
		CHG-06. Planned changes to system components that affect the service availability are communicated to clients through the OVHcloud's website. This communication is made 72 hours before the change implementation.
DEV-10	Production environments are physically or logically separated from test or development environments to prevent unauthorized access to cloud customer data, the spread of malware, or changes to system components. Data contained in the production environments is not used in test or development environments in order not to compromise their confidentiality.	**CHG-04.** Separate environments are used for development and production. Moreover, data contained in the production environments is not used in development environment in order not to compromise their confidentiality.
		CHG-05. During the development process, all pull requests must be approved by at least one peer reviewer before being pushed to production.

SSO: Control and Monitoring of Service Providers and Suppliers
Control Objective: Ensure the protection of information that service providers or suppliers of the Cloud Service Provider (subcontractors) can access and monitor the agreed services and security requirements.

Ref.	C5 Requirement	OVHcloud Control
SSO-01	Policies and instructions for controlling and monitoring third parties (e.g. service providers or suppliers) whose services contribute to the provision of the cloud service are documented, communicated and provided in accordance with SP-01 with respect to the following aspects: • Requirements for the assessment of risks resulting from the procurement of third-party services; • Requirements for the classification of third parties based on the risk assessment by the Cloud Service Provider and the determination of whether the third party is a subcontractor (cf. Supplementary Information); • Information security requirements for the processing, storage or transmission of information by third parties based on recognized industry standards; • Information security awareness and training requirements for staff; • applicable legal and regulatory requirements; • Requirements for dealing with vulnerabilities, security incidents and malfunctions; • Specifications for the contractual agreement of these requirements; • Specifications for the monitoring of these requirements; and • Specifications for applying these requirements also to service providers used by the third parties, insofar as the services provided by these service providers also contribute to the provision of the cloud service.	**THP-05.** A security policy with third parties has been implemented by OVHcloud that includes: • Signature of agreements with third parties that define business activities and security requirements; • Background check of third parties; • Audit and monitoring of third parties; • Security training and awareness of third parties.
		THP-03. OVHcloud limits the risk related to the intervention of service providers in the perimeter of its provided services and products. Service providers do not contribute to the processes of development, change and incident management of the services provided by OVHcloud and thus, do not have access to confidential information. If a third party develops software for a perimeter, a development guideline based on OWASP is provided to them and their employees must be trained accordingly.
		THP-04. Third-party relationships are formalized with agreements that identify the critical business activities performed by the third party and the security requirements. Moreover, OVHcloud keeps a file for the monitoring of third parties that includes: • Company name; • Address; • Date of contract signature and contract end; • Description of the service; • Responsible contact person at OVHcloud and at the service provider.

Ref.	C5 Requirement	OVHcloud Control
SSO-02	Service providers and suppliers of the Cloud Service Provider undergo a risk assessment in accordance with the policies and instructions for the control and monitoring of third parties prior to contributing to the delivery of the cloud service. The adequacy of the risk assessment is reviewed regularly, at least annually, by qualified personnel of the Cloud Service Provider during service usage. The risk assessment includes the identification, analysis, evaluation, handling and documentation of risks with regard to the following aspects: • Protection needs regarding the confidentiality, integrity, availability and authenticity of information processed, stored or transmitted by the third party; • Impact of a protection breach on the provision of the cloud service; • The Cloud Service Provider's dependence on the service provider or supplier for the scope, complexity and uniqueness of the service purchased, including the consideration of possible alternatives.	**THP-03.** OVHcloud limits the risk related to the intervention of service providers in the perimeter of its provided services and products. Service providers do not contribute to the processes of development, change and incident management of the services provided by OVHcloud and thus, do not have access to confidential information. If a third party develops software for a perimeter, a development guideline based on OWASP is provided to them and their employees must be trained accordingly.
SSO-03	The Cloud Service Provider maintains a directory for controlling and monitoring the service providers and suppliers who contribute services to the delivery of the cloud service. The following information is maintained in the directory: • Company name; • Address; • Locations of data processing and storage; • Responsible contact person at the service provider/supplier; • Responsible contact person at the cloud service provider; • Description of the service; • Classification based on the risk assessment; • Beginning of service usage; and • Proof of compliance with contractually agreed requirements. The information in the list is checked at least annually for completeness, accuracy and validity.	**THP-04.** Third-party relationships are formalized with agreements that identify the critical business activities performed by the third party and the security requirements. Moreover, OVHcloud keeps a file for the monitoring of third parties that includes: • Company name; • Address; • Date of contract signature and contract end; • Description of the service; • Responsible contact person at OVHcloud and at the service provider.

Ref.	C5 Requirement	OVHcloud Control
SSO-04	The Cloud Service Provider monitors compliance with information security requirements and applicable legal and regulatory requirements in accordance with policies and instructions concerning controlling and monitoring of third-parties. Monitoring includes a regular review of the following evidence to the extent that such evidence is to be provided by third parties in accordance with the contractual agreements: • reports on the quality of the service provided; • certificates of the management systems' compliance with international standards; • independent third-party reports on the suitability and operating effectiveness of their service-related internal control systems; and • Records of the third parties on the handling of vulnerabilities, security incidents and malfunctions. The frequency of the monitoring corresponds to the classification of the third party based on the risk assessment conducted by the Cloud Service Provider (cf. SSO-02). The results of the monitoring are included in the review of the third party's risk assessment. Identified violations and deviations are subjected to analysis, evaluation and treatment in accordance with the risk management procedure (cf. OIS-07).	**THP-01.** OVHcloud annually monitors the compliance of service providers with its security requirements and internal policies through annual audits. These audits include: • The review and renewal of service agreements; • Background check on the company providing the service; • Review of provided services and activities; • Review of certificates of the management systems' compliance with international standards (when applicable); Identified violations and deviations are subjected to analysis, evaluation and treatment.
SSO-05	The Cloud Service Provider has defined and documented exit strategies for the purchase of services where the risk assessment of the service providers and suppliers regarding the scope, complexity and uniqueness of the purchased service resulted in a very high dependency (cf. Supplementary Information). Exit strategies are aligned with operational continuity plans and include the following aspects: • Analysis of the potential costs, impacts, resources and timing of the transition of a purchased service to an alternative service provider or supplier; • Definition and allocation of roles, responsibilities and sufficient resources to perform the activities for a transition; • Definition of success criteria for the transition; • Definition of indicators for monitoring the performance of services, which should initiate the withdrawal from the service if the results are unacceptable.	**THP-03.** OVHcloud limits the risk related to the intervention of service providers in the perimeter of its provided services and products. Service providers do not contribute to the processes of development, change and incident management of the services provided by OVHcloud and thus, do not have access to confidential information. If a third party develops software for a perimeter, a development guideline based on OWASP is provided to them and their employees must be trained accordingly.

SIM: Security Incident Management
Control Objective: Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.

Ref.	C5 Requirement	OVHcloud Control
SIM-01	Policies and instructions with technical and organizational safeguards are documented, communicated and provided in accordance with SP-01 to ensure a fast, effective and proper response to all known security incidents. The Cloud Service Provider defines guidelines for the classification, prioritization and escalation of security incidents and creates interfaces to the incident management and business continuity management. In addition, the Cloud Service Provider has set up a "Computer Emergency Response Team" (CERT), which contributes to the coordinated resolution of occurring security incidents. Customers affected by security incidents are informed in a timely and appropriate manner.	**IM-03.** Employees, customers and providers have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel. OVHcloud also provides user guides, security alerts and known issues on its websites and client portal with information to improve security knowledge and awareness.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.

Ref.	C5 Requirement	OVHcloud Control
SIM-02	Subject matter experts of the Cloud Service Provider, together with external security providers where appropriate, classify, prioritize and perform root-cause analyses for events that could constitute a security incident.	**IM-05.** When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.
SIM-03	After a security incident has been processed, the solution is documented in accordance with the contractual agreements and the report is sent to the affected customers for final acknowledgement or, if applicable, as confirmation.	**IM-01.** After a security incident has been identified and analyzed for root cause analysis and impact, the action plan is carried out and documented. In the case, the security incident has an impact on the cloud services, a communication is sent to the affected customers. The security incident is formalized within a post-mortem detailing all security incident processing steps.
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.
SIM-04	The Cloud Service Provider informs employees and external business partners of their obligations. If necessary, they agree to or are contractually obliged to report all security events that become known to them and are directly related to the cloud service provided by the Cloud Service Provider to a previously designated central office of the Cloud Service Provider promptly. In addition, the Cloud Service Provider communicates that "false reports" of events that do not subsequently turn out to be incidents do not have any negative consequences.	**IM-03.** Employees, customers and providers have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel. OVHcloud also provides user guides, security alerts and known issues on its websites and client portal with information to improve security knowledge and awareness.

Ref.	C5 Requirement	OVHcloud Control
SIM-05	Mechanisms are in place to measure and monitor the type and scope of security incidents and to report them to support agencies. The information obtained from the evaluation is used to identify recurrent or significant incidents and to identify the need for further protection.	**IM-01.** After a security incident has been identified and analyzed for root cause analysis and impact, the action plan is carried out and documented. In the case, the security incident has an impact on the cloud services, a communication is sent to the affected customers. The security incident is formalized within a post-mortem detailing all security incident processing steps.
		IM-05. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.
		IM-02. On an annual basis, a crisis unit simulation is performed to ensure the incident response procedures are up-to-date and accurate. When updating the incident response plan, lessons learned are used to implement changes to ensure that incident response procedures are effective.

BCM: Business Continuity Management
Control Objective: Plan, implement, maintain and test procedures and measures for business continuity and emergency management.

Ref.	C5 Requirement	OVHcloud Control
BCM-01	The top management (or a member of the top management) of the Cloud Service Provider is named as the process owner of business continuity and emergency management and is responsible for establishing the process within the company as well as ensuring compliance with the guidelines. They must ensure that sufficient resources are made available for an effective process. People in management and other relevant leadership positions demonstrate leadership and commitment to this issue by encouraging employees to actively contribute to the effectiveness of continuity and emergency management.	**GOV-02.** A business continuity plan is documented for the Public Cloud perimeter that describes: • The key architecture components and systems; • The high availability, rescue and takeover mechanisms for these components ; • Tests of the high availability, rescue and takeover mechanisms for these components when applicable. In case of major incident, the incident management process is followed and the crisis unit is triggered.
BCM-02	Policies and instructions to determine the impact of any malfunction to the cloud service or enterprise are documented, communicated and made available in accordance with SP-01. The following aspects are considered as minimum: • Possible scenarios based on a risk analysis; • Identification of critical products and services • Identify dependencies, including processes (including resources required), applications, business partners and third parties; • Capture threats to critical products and services; • Identification of effects resulting from planned and unplanned malfunctions and changes over time; • Determination of the maximum acceptable duration of malfunctions; • Identification of restoration priorities; • Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (RTO); • Determination of time targets for the maximum reasonable period during which data can be lost and not recovered (RPO); and • Estimation of the resources needed for resumption.	**GOV-06.** A complete inventory of assets located at all geographical locations is maintained and updated regularly. Moreover, during its risk assessment process, OVHcloud identifies the list of assets which may be impacted by each risk scenario. A Business Impact Assessment (BIA) is performed to quantify the consequences of the confidentiality, integrity, or availability loss on the assets impacted by the risk scenario analysed. The asset's criticality depends on the result of the assessment.
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		GOV-01. A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.);

Ref.	C5 Requirement	OVHcloud Control
		• Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
BCM-03	Based on the business impact analysis, a single framework for operational continuity and business plan planning will be implemented, documented and enforced to ensure that all plans are consistent. Planning is based on established standards, which are documented in a "Statement of Applicability". Business continuity plans and contingency plans take the following aspects into account: • Defined purpose and scope with consideration of the relevant dependencies; • Accessibility and comprehensibility of the plans for persons who are to act accordingly; • Ownership by at least one designated person responsible for review, updating and approval; • Defined communication channels, roles and responsibilities including notification of the customer; • Recovery procedures, manual interim solutions and reference information (taking into account prioritization in the recovery of cloud infrastructure components and services and alignment with customers); • Methods for putting the plans into effect; • Continuous process improvement; and • Interfaces to Security Incident Management.	**GOV-02.** A business continuity plan is documented for the Public Cloud perimeter that describes: • The key architecture components and systems; • The high availability, rescue and takeover mechanisms for these components ; • Tests of the high availability, rescue and takeover mechanisms for these components when applicable. In case of major incident, the incident management process is followed and the crisis unit is triggered.
		GOV-01. A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
BCM-04	The business impact analysis, business continuity plans and contingency plans are reviewed, updated and tested on a regular basis (at least annually) or after significant organizational or environmental changes. Tests involve affected customers (tenants) and relevant third parties. The tests are documented and results are taken into account for future operational continuity measures.	**GOV-20** Business continuity mechanisms are reviewed and tested at least annually or after significant organizational or environmental changes. The tests are documented and results are taken into account for future operational continuity measures.

COM: Compliance
Control Objective: Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.

Ref.	C5 Requirement	OVHcloud Control
COM-01	The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the cloud service as well as the Cloud Service Provider's procedures for complying with these requirements are explicitly defined and documented.	**GOV-01.** A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.
		GOV-13. OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure;

Ref.	C5 Requirement	OVHcloud Control
		• physical security; • backup, business continuity and disaster recovery.
COM-02	Policies and instructions for planning and conducting audits are documented, communicated and made available in accordance with SP-01 and address the following aspects: • Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the activities; • Activities that may result in malfunctions to the cloud service or breaches of contractual requirements are performed during scheduled maintenance windows or outside peak periods; and • Logging and monitoring of activities.	**GOV-07.** A procedure for planning and conducting audits is documented and communicated through the intranet. OVHcloud has established a formal audit plan that includes internal and external assessments to validate the implementation and operating effectiveness of the OVHcloud control environment and to assess compliance with the relevant and applicable legal, regulatory or contractual requirements as well as compliance with the policies and procedures. The audit results are reviewed during the monthly ISMS meetings for monitoring of corrective actions.
COM-03	Subject matter experts check the compliance of the information security management system at regular intervals, at least annually, with the relevant and applicable legal, regulatory, self-imposed or contractual requirements (cf. COM-01) as well as compliance with the policies and instructions (cf. SP-01) within their scope of responsibility (cf. OIS-01) through internal audits (cf. § 9.3 of ISO/IEC 27001). Identified vulnerabilities and deviations are subject to risk assessment in accordance with the risk management procedure (cf. OIS-06) and follow-up measures are defined and tracked (cf. OPS-18).	**SEC-02.** Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		GOV-07. A procedure for planning and conducting audits is documented and communicated through the intranet. OVHcloud has established a formal audit plan that includes internal and external assessments to validate the implementation and operating effectiveness of the OVHcloud control environment and to assess compliance with the relevant and applicable legal, regulatory or contractual requirements as well as compliance with the policies and procedures. The audit results are reviewed during the monthly ISMS meetings for monitoring of corrective actions.
COM-04	The top management of the Cloud Service Provider is regularly informed about the information security performance within the scope of the ISMS in order to ensure its continued suitability, adequacy and effectiveness. The information is included in the management review of the ISMS at is performed at least once a year.	**GOV-07.** A procedure for planning and conducting audits is documented and communicated through the intranet. OVHcloud has established a formal audit plan that includes internal and external assessments to validate the implementation and operating effectiveness of the OVHcloud control environment and to assess compliance with the relevant and applicable legal, regulatory or contractual requirements as well as compliance with the policies and procedures. The audit results are reviewed during the monthly ISMS meetings for monitoring of corrective actions.

Ref.	C5 Requirement	OVHcloud Control
		GOV-08. OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.

INQ: Dealing with investigation requests from government agencies
Control Objective: Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.

Ref.	C5 Requirement	OVHcloud Control
INQ-01	Investigation requests from government agencies are subjected to a legal assessment by subject matter experts of the Cloud Service Provider. The assessment determines whether the government agency has an applicable and legally valid legal basis and what further steps need to be taken.	**CUS-06.** Investigation requests from government agencies are checked by the Legal Team in order to assess their authenticity and their compliance with the applicable legal framework. Access to or disclosure of customer data to the government agency is performed only after the Legal Team has confirmed the request's authenticity and legal basis.
INQ-02	The Cloud Service Provider informs the affected Cloud Customer(s) without undue delay, unless the applicable legal basis on which the government agency is based prohibits this or there are clear indications of illegal actions in connection with the use of the Cloud Service.	**CUS-07.** OVHcloud informs the concerned customer during an investigation or request for evidence by a government agency, unless it is prohibited by the applicable law.
INQ-03	Access to or disclosure of cloud customer data in connection with government investigation requests is subject to the proviso that the Cloud Service Provider's legal assessment has shown that an applicable and valid legal basis exists and that the investigation request must be granted on that basis.	**CUS-06.** Investigation requests from government agencies are checked by the Legal Team in order to assess their authenticity and their compliance with the applicable legal framework. Access to or disclosure of customer data to the government agency is performed only after the Legal Team has confirmed the request's authenticity and legal basis.
INQ-04	The Cloud Service Provider's procedures for setting up access to or disclosure of cloud customer data as part of an investigation requests, ensure that government agencies only have access to the data they need to investigate. If no clear limitation of the data is possible, the Cloud Service Provider anonymizes or pseudonymizes the data so that government agencies can only assign it to those cloud customers who are subject of the investigation request.	**CUS-08.** In case of disclosure of customer data to a government agency as part of an investigation, the disclosure is strictly limited to the data requested by the authority.

PSS: Product Safety and Security
Control Objective: Provides up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorization of users of cloud customers.

Ref.	C5 Requirement	OVHcloud Control
PSS-01	Basic Criterion The Cloud Service Provider provides cloud customers with guidelines and recommendations for the secure use of the cloud service provided. The information contained therein is intended to assist the cloud customer in the secure configuration, installation and use of the cloud service, to the extent applicable to the cloud service and the responsibility of the cloud user. The type and scope of the information provided will be based on the needs of subject matter experts of the cloud customers who set information security requirements, implement them or verify the implementation (e.g. IT, Compliance, Internal Audit). The information in the guidelines and recommendations for the secure use of the cloud service address the following aspects, where applicable to the cloud service: • Instructions for secure configuration; • Information sources on known vulnerabilities and update mechanisms; • Error handling and logging mechanisms; • Authentication mechanisms; • Roles and rights concept including combinations that result in an elevated risk; and • Services and functions for administration of the cloud service by privileged users. The information is maintained so that it is applicable to the cloud service provided in the version intended for productive use.	**CUS-09.** OVHcloud provides the Public Cloud customers with guidelines and recommendations for the configuration and use of the cloud service provided. The information is publicly available on OVHcloud's website and includes: • Instructions for secure configuration; • Authentication mechanisms; • Access and access rights management; and • Services and functions for administration of the cloud service.

Ref.	C5 Requirement	OVHcloud Control
PSS-02	The Cloud Service Provider applies appropriate measures to check the cloud service for vulnerabilities which might have been integrated into the cloud service during the software development process. The procedures for identifying such vulnerabilities are part of the software development process and, depending on a risk assessment, include the following activities: • Static Application Security Testing; • Dynamic Application Security Testing; • Code reviews by the Cloud Service Provider's subject matter experts; and • Obtaining information about confirmed vulnerabilities in software libraries provided by third parties and used in their own cloud service. The severity of identified vulnerabilities is assessed according to defined criteria and measures are taken to immediately eliminate or mitigate them.	**SEC-02.** Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.
		SEC-06. OVHcloud uses CVSS (Common Vulnerability Scoring System) for the scoring of vulnerabilities and relies on the online NIST database as well as other sources for the discovery of vulnerabilities. Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities are based on a list of assets ordered by criticality that relies on product-specific criteria for each Public Cloud product. Security patches are then deployed within a time-frame based on asset criticality.
		CHG-03. OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel Major security changes go through a risk analysis, penetration tests are then performed on an as needed basis.
PSS-03		**SEC-02.** Internal and external vulnerability scans are performed quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.

Ref.	C5 Requirement	OVHcloud Control
	The Cloud Service Provider operates or refers to a daily updated online register of known vulnerabilities that affect the Cloud Service Provider and assets provided by the Cloud Service Provider that the cloud customers have to install, provide or operate themselves under the customers responsibility. The presentation of the vulnerabilities follows the Common Vulnerability Scoring System (CVSS). The online register is easily accessible to any cloud customer. The information contained therein forms a suitable basis for risk assessment and possible follow-up measures on the part of cloud users. For each vulnerability, it is indicated whether software updates (e.g. patch, update) are available, when they will be rolled out and whether they will be deployed by the Cloud Service Provider, the cloud customer or both of them together.	**SEC-06.** OVHcloud uses CVSS (Common Vulnerability Scoring System) for the scoring of vulnerabilities and relies on the online NIST database as well as other sources for the discovery of vulnerabilities. Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities are based on a list of assets ordered by criticality that relies on product-specific criteria for each Public Cloud product. Security patches are then deployed within a time-frame based on asset criticality.
PSS-04	The cloud service provided is equipped with error handling and logging mechanisms. These enable cloud users to obtain security-related information about the security status of the cloud service as well as the data, services or functions it provides. The information is detailed enough to allow cloud users to check the following aspects, insofar as they are applicable to the cloud service: • Which data, services or functions available to the cloud user within the cloud service, have been accessed by whom and when (Audit Logs); • Malfunctions during processing of automatic or manual actions; and • Changes to security-relevant configuration parameters, error handling and logging mechanisms, user authentication, action authorization, cryptography, and communication security. The logged information is protected from unauthorized access and modification and can be deleted by the Cloud Customer. If the cloud customer is responsible for the activation or type and scope of logging, the Cloud Service Provider must provide appropriate logging capabilities.	**CUS-10.** OVHcloud provides its customers with dedicated tools for monitoring and supervision of their Public Cloud. These tools provide information regarding system performance and availability and include alerts and error handling mechanisms.

Ref.	C5 Requirement	OVHcloud Control
PSS-05	The Cloud Service Provider provides authentication mechanisms that can force strong authentication (e.g. two or more factors) for users, IT components or applications within the cloud users' area of responsibility. These authentication mechanisms are set up at all access points that allow users, IT components or applications to interact with the cloud service. For privileged users, IT components or applications, these authentication mechanisms are enforced.	**IAM-04.** In-scope system components require unique username, passwords or authorized SSH keys prior to user authentication.
		IAM-07. OVHcloud permits remote access to production systems by authorized employees, using authorized devices and over encrypted virtual private network (VPN) connection.
		NET-13. OVHcloud permits the connection to its internal network via VPN and only to authorized equipment using host-based certificates.
PSS-06	To protect confidentiality, availability, integrity and authenticity during interactions with the cloud service, a suitable session management system is used that at least corresponds to the state-of-the-art and is protected against known attacks. Mechanisms are implemented that invalidate a session after it has been detected as inactive. The inactivity can be detected by time measurement. In this case, the time interval can be configured by the Cloud Service Provider or - if technically possible - by the cloud customer.	**SEC-11.** A session management mechanism is used on system components in order to deactivate the user's session after a defined time interval, depending on the component.
PSS-07	If passwords are used as authentication information for the cloud service, their confidentiality is ensured by the following procedures: • Users can initially create the password themselves or must change an initial password when logging in to the cloud service for the first time. An initial password loses its validity after a maximum of 14 days. • When creating passwords, compliance with the length and complexity requirements of the Cloud Service Provider (cf. IDM-09) or the cloud customer is technically enforced. • The user is informed about changing or resetting the password. • The server-side storage takes place using state-of-the-art cryptographically strong hash functions in combination with at least 32-bit long salt values.	**IAM-12.** OVHcloud has established a secure password configuration policy for in-scope system components that includes: • Restriction on password length and complexity (use of alphanumeric, upper- and lower-case characters); • Password age must not exceed 90 days; • The server-side storage takes place using cryptographically strong hash functions; • Guidelines and instructions on the secure handling and protection of passwords.

Ref.	C5 Requirement	OVHcloud Control
PSS-08	The Cloud Service Provider provides cloud users with a roles and rights concept for managing access rights. It describes rights profiles for the functions provided by the cloud service. The rights profiles are suitable for enabling cloud users to manage access authorizations and permissions in accordance with the principle of least-privilege and how it is necessary for the performance of tasks ("need-to-know principle") and to implement the principle of functional separation between operational and controlling functions ("separation of duties").	**CUS-02.** OVHcloud provides the Public Cloud customers with access rights mechanisms to manage customer users' access rights on the Public Cloud.
PSS-09	Access to the functions provided by the cloud service is restricted by access controls (authorization mechanisms) that verify whether users, IT components, or applications are authorized to perform certain actions. The Cloud Service Provider validates the functionality of the authorization mechanisms before new functions are made available to cloud users and in the event of changes to the authorization mechanisms of existing functions (cf. DEV-06). The severity of identified vulnerabilities is assessed according to defined criteria based on industry standard metrics (e.g. Common Vulnerability Scoring System) and measures for timely resolution or mitigation are initiated. Vulnerabilities that have not been fixed are listed in the online register of known vulnerabilities (cf. PSS-02).	**CUS-02.** OVHcloud provides the Public Cloud customers with access rights mechanisms to manage customer users' access rights on the Public Cloud.
PSS-10	If the Cloud Service offers functions for software-defined networking (SDN), the confidentiality of the data of the cloud user is ensured by suitable SDN procedures. The Cloud Service Provider validates the functionality of the SDN functions before providing new SDN features to cloud users or modifying existing SDN features. Identified defects are assessed and corrected in a risk-oriented manner.	**CUS-11.** OVHcloud provides its customers with a software-defined networking (SDN) tool that allows the customers to implement network access rules and other network services.

Ref.	C5 Requirement	OVHcloud Control
PSS-11	If cloud customers operate virtual machines or containers with the cloud service, the Cloud Service Provider must ensure the following aspects: • The cloud customer can restrict the selection of images of virtual machines or containers according to his specifications, so that users of this cloud customer can only launch the images or containers released according to these restrictions. • If the Cloud Service Provider provides images of virtual machines or containers to the Cloud Customer, the Cloud Service Provider appropriately inform the Cloud Customer of the changes made to the previous version. • In addition, these images provided by the Cloud Service Provider are hardened according to generally accepted industry standards.	**CUS-12.** OVHcloud provides its customers with the ability to restrict the access to a virtual machine via the administration console.
PSS-12	The cloud customer is able to specify the locations (location/country) of the data processing and storage including data backups according to the contractually available options. This must be ensured by the cloud architecture.	**CUS-13.** During the process of subscription to a Public Cloud, OVHcloud provides the Public Cloud customer with the ability to specify the locations (location/country) of the data processing and storage.

5. Part D: OVHcloud's Control Description, KPMG's Tests of Controls and KPMG's Results of Tests

GOV: Governance			
Control ID.	**OVHcloud's Control Activity**	**KPMG's Tests of Controls**	**KPMG's Results of Tests**
GOV-01	A risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).	Inspected risk assessment methodology to determine whether a risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer); • Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization). For a selection of risks inspected risk analysis tickets to determine whether a risk assessment is performed annually (and in conjunction with any major changes to information systems), and includes the following: • Involving appropriate levels of management; • Identifying threats to operations arising from the use of information technology and including threats from internal and external sources (employees, third parties, etc.); • Analyzing risks associated with the threats, using qualitative and quantitative methods and determining the likelihood and impact associated with inherent and residual risks; • Determining a risk treatment strategy (acceptance, avoidance, mitigation, and transfer);	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
		• Designing controls to address identified risks (manual/automated, preventive/detective and at various levels of the organization).	
GOV-02	A business continuity plan is documented for the Public Cloud perimeter that describes: • The key architecture components and systems; • The high availability, backup and recovery mechanisms for these components; • Tests of the high availability, backup and recovery mechanisms when applicable. In case of major incident, the incident management process is followed and the crisis unit is triggered.	Inspected the business continuity plan for the Public Cloud perimeter to determine whether a business continuity plan is documented for the Public Cloud perimeter that describes: • The key architecture components and systems; • The high availability, rescue and takeover mechanisms for these components ; • Tests of the high availability, rescue and takeover mechanisms for these components when applicable. In case of major incident, the incident management process is followed and the crisis unit is triggered.	No exceptions noted.
GOV-03	During its ongoing and periodic business planning and budgeting process, management evaluates the need for additional tools and resources in order to achieve business objectives.	Inspected Public Cloud's projects roadmap as well as the latest risk assessment report to determine whether during its ongoing and periodic business planning and budgeting process, OVHcloud's management evaluates the need for additional tools and resources in order to achieve business objectives.	No exceptions noted.
GOV-04	Management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.	Inspected the ISMS organization, roles and responsibilities to determine whether management has established defined roles and responsibilities to implement and oversee the compliance with information security policies. These roles and responsibilities are formally documented in job descriptions and in the policies.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
GOV-05	OVHcloud has a defined information classification scheme according to information security needs. OVHcloud classifies information based on the TLP protocol: - TLP:WHITE or "Public" refers to OVHcloud official information made publicly available by communication instances; - TLP:GREEN refers to information that can freely communicated within OVHcloud community; - TLP:AMBER or "Confidential" refers to confidential data communicated internally and to specific interested parties under NDA; - TLP:RED or "Highly confidential" refers to highly confidential data disclosed on the "need to know" basis only. Security measures for labelling, access, storage, disclosure and communication means depend on the information confidentiality level.	Inspected the latest risk assessment report and the information classification policy to determine whether OVHcloud has a defined information classification scheme according to information security needs. OVHcloud classifies information based on the TLP protocol: • TLP:WHITE or "Public" refers to OVHcloud official information made publicly available by communication instances; • TLP:GREEN refers to information that can freely be communicated within OVHcloud community; • TLP:AMBER or "Confidential" refers to confidential data communicated internally and to specific interested parties under NDA; • TLP:RED or "Highly confidential" refers to highly confidential data disclosed on the "need to know" basis only. Security measures for labelling, access, storage, disclosure and communication means depend on the information confidentiality level.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
GOV-06	A complete inventory of assets located at all geographical locations is maintained and updated regularly. Moreover, during its risk assessment process, OVHcloud identifies the list of assets which may be impacted by each risk scenario. A Business Impact Assessment (BIA) is performed to quantify the consequences of the confidentiality, integrity, or availability loss on the assets impacted by the risk scenario analysed. The asset's criticality depends on the result of the assessment.	Inspected assets inventory and the latest risk assessment report to determine whether a complete inventory of assets located at all geographical locations is maintained and updated regularly. Moreover, during its risk assessment process, OVHcloud identifies the list of assets which may be impacted by each risk scenario. A Business Impact Assessment (BIA) is performed to quantify the consequences of the confidentiality, integrity, or availability loss on the assets impacted by the risk scenario analysed. The asset's criticality depends on the result of the assessment.	No exceptions noted.
GOV-07	A procedure for planning and conducting audits is documented and communicated through the intranet. OVHcloud has established a formal audit plan that includes internal and external assessments to validate the implementation and operating effectiveness of the OVHcloud control environment and to assess compliance with the relevant and applicable legal, regulatory or contractual requirements as well as compliance with the policies and procedures. The audit results are reviewed during the monthly ISMS meetings for monitoring of corrective actions.	Inspected the audit plan and the Monitoring and Reassessment Process to determine whether a procedure for planning and conducting audits is documented and communicated through the intranet. OVHcloud has established a formal audit plan that includes internal and external assessments to validate the implementation and operating effectiveness of the OVHcloud control environment and to assess compliance with the relevant and applicable legal, regulatory or contractual requirements as well as compliance with the policies and procedures. The audit results are reviewed during the monthly ISMS meetings for monitoring of corrective actions. For a selection of in scope audits, inspected the related audit reports and evidence of follow-up on action plans to determine whether a procedure for planning and conducting audits is documented and communicated through the intranet. OVHcloud has established a formal audit plan that includes internal and external assessments to validate the implementation and operating effectiveness of the OVHcloud control environment and to assess compliance with the relevant and applicable legal, regulatory or contractual requirements as well as compliance with the policies and procedures. The audit results are reviewed during the monthly ISMS meetings for monitoring of corrective actions.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
GOV-08	OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance.	Inspected the risk assessment methodology to determine whether OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers. Risk treatment options include acceptance, avoidance, mitigation, and transfer. The risk assessment is reviewed annually and updated upon significant changes or incidents. OVHcloud management acknowledges risk treatment decisions and formally approves risk acceptance. For a selection of risks inspected risk analysis tickets to determine whether OVHcloud maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact OVHcloud's business objectives, regulatory requirements, and customers.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
GOV-09	OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.	Inspected the Information and Communication Charter to determine whether OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms. Inspected the mobile devices extraction from the mobile devices management solution to determine whether OVHcloud provides guidance on mobile device / BYOD usage through its Information and Communication Charter, its Phone Policy and general detailed policies including: • Use of mobile devices; • Requirements and conditions for usage of BYOD; • Protection of devices that access content for which OVHcloud is responsible (use of encryption to protect sensitive data stored on the device, automatic lockout screen); • The use of a centralized mobile management solution (for inventory, monitoring, enrollment, remote wipe capability and remote synchronization...); • Use and protection of password / PIN and other authentication mechanisms.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
GOV-10	OVHcloud posts a description of its system, system boundaries, and system processes on its intranet for employees. Moreover, OVHcloud posts the documentation for the use and configuration of its services on its website for its customers.	Inspected the architecture design documentation as well as OVHcloud's website to determine whether OVHcloud posts a description of its system, system boundaries, and system processes on its intranet for employees. Moreover, OVHcloud posts the documentation for the use and configuration of its services on its website for its customers.	No exceptions noted.
GOV-11	OVHcloud's confidentiality commitments and the associated system requirements, are documented and reviewed when necessary. These commitments and system requirements as well as their changes are communicated to employees, customers and providers, as appropriate which must accept them.	Inspected the IT charter, service providers agreements and the general terms of service as well as the last review of confidentiality commitments to determine whether OVHcloud's confidentiality commitments and the associated system requirements, are documented and reviewed when necessary. These commitments and system requirements as well as their changes are communicated to employees, customers and providers, as appropriate which must accept them.	No exceptions noted.
GOV-12	OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedures for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.	Inspected the information security policy as well as the ISMS policies and procedures to determine whether OVHcloud's management reviews and approves annually, or as a result of changes to the organization, the information security policy, policies and procedure for consistency with the organization's risk mitigation strategy. Policies and procedures are updated as necessary, considering changes in the strategy, the organization, laws and regulations.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
GOV-13	OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.	Inspected OVHcloud policies and procedures to determine whether OVHcloud has developed, documented and approved an Information Security Management Program that includes policies and procedures on the following topics: • information classification and associated protection requirements; • risk management; • access protection and user provisioning and deprovisioning; • security organization and responsibility for security; • acquisition, development and change management; • complaint intake and resolution; • security and other incidents management; • security training; • commitment identification and compliance measurement; • information sharing and disclosure; • physical security; • backup, business continuity and disaster recovery.	No exceptions noted.
GOV-14	OVHcloud's security and privacy commitments and changes to these commitments, are communicated to customers and are available on OVHcloud's website.	Inspected the OVHcloud's customer-facing website to determine whether OVHcloud's security and privacy commitments and changes to these commitments, are communicated to customers and are available on OVHcloud's website.	No exceptions noted.
GOV-15	Reporting relationships and organizational structures are defined and reviewed periodically by senior management and adjusted as needed based on changing entity commitments and requirements relevant to security, availability, confidentiality and privacy.	Inspected the organization and management procedures to determine whether reporting relationships and organizational structures are defined and reviewed periodically by senior management and adjusted as needed based on changing entity commitments and requirements relevant to security, availability, confidentiality and privacy.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
GOV-16	Exceptions to the policies and procedures for information security as well as respective controls go through the risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners.	Inspected the Information Security Policy, ISMS policies, as well as the risk management methodology to determine whether exceptions to the policies and procedures for information security as well as respective controls go through the risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners. For a selection of exceptions to information security policies, inspected records of their approval and inclusion in the risk assessment to determine whether exceptions to the policies and procedures for information security as well as respective controls go through the risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners.	No exceptions noted. There was no exception to information security policies during the examination period. As such, KPMG was unable to test the operating effectiveness of this control because the circumstances that warrant the operation of the control did not occur during the examination period.
GOV-17	OVHcloud management has adopted a global information security policy that is communicated to employees, third parties and customers as appropriate. The information security policy describes OVHcloud's objectives, requirements and commitments to information security and refers to specific and detailed security policies that are used as a reference in the implementation of the operational security management system.	Inspected OVHcloud's information security policy and records of its communication to employees, third parties and customers to determine whether OVHcloud management has adopted a global information security policy that is communicated to employees, third parties and customers as appropriate. The information security policy describes OVHcloud's objectives, requirements and commitments to information security and refers to specific and detailed security policies that are used as a reference in the implementation of the operational security management system.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
GOV-18	Policies and procedures for acceptable use and safe handling of assets are documented, communicated and address the following aspects: • Inventory; • Risk and business impact assessment; • Restriction of software installations or use of services; • Protection against malware; • Remote deactivation, deletion or blocking; • Dealing with incidents and vulnerabilities; and • Complete and irrevocable deletion of the data upon decommissioning.	Inspected the policies and procedures for asset management to determine whether policies and procedures for acceptable use and safe handling of assets are documented, communicated and address the following aspects: • Inventory; • Risk and business impact assessment; • Restriction of software installations or use of services; • Protection against malware; • Remote deactivation, deletion or blocking; • Dealing with incidents and vulnerabilities; and • Complete and irrevocable deletion of the data upon decommissioning.	No exceptions noted.
GOV-19	As part of contract execution, the metadata collected by OVHcloud is used for the purposes of business management, information and support, claims management, invoicing and accounting, payment management, process improvement and customer relationship management. The collected data, its usage and its retention period are documented.	Inspected the procedures for handling metadata to determine whether as part of contract execution, the metadata collected by OVHcloud is used for the purposes of business management, information and support, claims management, invoicing and accounting, payment management, process improvement and customer relationship management. The collected data, its usage and its retention period are documented. The collected data, its usage and its retention period are documented.	No exceptions noted.
GOV-20	Business continuity mechanisms are reviewed and tested at least annually or after significant organizational or environmental changes. The tests are documented and results are taken into account for future operational continuity measures.	Inspected business continuity plans, the test report of the crisis unit simulations and of the backup restoration and infrastructure reconstruction mechanisms to determine whether business continuity mechanisms are reviewed and tested at least annually or after significant organizational or environmental changes. The tests are documented and results are taken into account for future operational continuity measures.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
GOV-21	Information Security and Operations teams hold periodic meetings to monitor and manage respective department's progress or lack thereof as it relates to their achievement of department's responsibilities.	For a selection of weeks and months, we requested and obtained the monthly security meeting minutes, to determine whether Information Security and Operations teams hold periodic meetings to monitor and manage respective department's progress or lack thereof as it relates to their achievement of department's responsibilities.	No exceptions noted.

PHY: Physical Security

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
PHY-01	A clear desk and screen policy for information processing facilities and OVHcloud offices are adopted.	Inspected the clear desk policy and visited OVHcloud's offices and datacenters to determine whether a clear desk policy and a clear screen policy for information processing facilities are adopted.	No exceptions noted.
PHY-02	A monitoring process exists to monitor entry and exit points. Measures such as surveillance cameras and trained security guards are adopted. Logs and video surveillance recordings are maintained for an agreed period of time for future reference. For DC Tape Saint-Pierre-des-Corps and DC Tape Villenave d'Ornon, there are no permanent security guards at the entrance of the datacenter. However, physical security measures are implemented, including access control systems and continuous video surveillance, as well as remote security guard who can be contacted at the entrance of the site and who is responsible of the barrier opening and remote monitoring.	Inspected physical access management procedures to determine whether a monitoring process exists to monitor entry and exit points. Measures such as surveillance cameras and trained security guards are adopted. Logs and video surveillance recordings are maintained for an agreed to period of time for future reference. For DC Tape Saint-Pierre-des-Corps and DC Tape Villenave d'Ornon, there are no permanent security guards at the entrance of the datacenter. However, physical security measures are implemented, including access control systems and continuous video surveillance, as well as remote security guard who can be contacted at the entrance of the site and who is responsible of the barrier opening and remote monitoring. Visited the data centers to determine whether a monitoring process exists to monitor entry and exit points. Measures such as surveillance cameras and trained security guards are adopted. Logs and video surveillance recordings are maintained for an agreed to period of time for future reference. For DC Tape Saint-Pierre-des-Corps and DC Tape Villenave d'Ornon, there are no permanent security guards at the entrance of the datacenter. However, physical security measures are implemented, including access control systems and continuous video surveillance, as well as remote security guard who can be contacted at the entrance of the site and who is responsible of the barrier opening and remote monitoring.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
PHY-03	A security level classification system is used to define zones for access security.	Inspected physical access management procedures to determine whether a security level classification system is used to define zones for access security. Visited the datacenters to determine whether a security level classification system is used to define zones for access security.	Exception noted: During the visit of DC Tape Saint-Pierre-des-Corps, KPMG noted that the level of classification of the zones is not displayed as required by the zoning policy defined by OVHcloud for all its datacenters *Refer to section V for management's response*
PHY-04	Access points such as delivery and loading areas where unauthorized persons could enter the premises are controlled and isolated from information processing facilities to avoid unauthorized access. For MiniDCs, physical isolation is not feasible. However, security measures such as the use of access badges are implemented to prevent unauthorized access.	Inspected physical access management procedures to determine whether access points such as delivery and loading areas where unauthorized persons could enter the premises are controlled and isolated from information processing facilities to avoid unauthorized access. For MiniDCs, physical isolation is not feasible. However, security measures such as the use of access badges are implemented to prevent unauthorized access. Visited the data centers to determine whether access points such as delivery and loading areas where unauthorized persons could enter the premises are controlled and isolated from information processing facilities to avoid unauthorized access. For MiniDCs, physical isolation is not feasible. However, security measures such as the use of access badges are implemented to prevent unauthorized access.	No exceptions noted.
PHY-05	Access to the datacenter is revoked in a timely manner as part of the termination process.	Inspected the physical access management procedure to determine whether access to the datacenter is revoked in a timely manner as part of the termination process. Inspected the leavers extraction and the system extraction of active users to determine whether access to the datacenter is revoked in a timely manner as part of the termination process.	No exceptions noted

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
PHY-06	Access to the datacenter perimeter for employees and third parties requires an access request and manager approval prior to access being provisioned. Once in the perimeter, access to the physical locations according to the person's access rights is granted by authorized and approved granters and is synchronized with the person's badge.	Inspected the physical access management procedure to determine whether access to the datacenter perimeter for employees and third parties requires an access request and manager approval prior to access being provisioned. Once in the perimeter, access to the physical locations according to the person's access rights is granted by authorized and approved granters and is synchronized with the person's badge. For a selection of access rights granted in 2024, inspected the access attribution records to determine whether access to the datacenter perimeter for employees and third parties requires an access request and manager approval prior to access being provisioned. Once in the perimeter, access to the physical locations according to the person's access rights is granted by authorized and approved granters and is synchronized with the person's badge.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
PHY-07	All personnel are required to wear badges at all times. Visitor badges are clearly distinguishable from employee badges.	Inspected physical access management procedures to determine whether all personnel are required to wear badges at all times. Visitor badges are clearly distinguishable from employee badges. Visited the datacenters to determine whether all personnel are required to wear badges at all times. Visitor badges are clearly distinguishable from employee badges.	No exceptions noted
PHY-08	Visitors' access to OVHcloud's datacenters requires approval by the appropriate manager in the access rights management tool before access being granted. A check is performed at the entrance in order to ensure that the visitor's access is approved.	Inspected physical access management procedures to determine whether visitors' access to OVHcloud's datacenters requires approval by the appropriate manager in the access rights management tool before access being granted. A check is performed at the entrance in order to ensure that the visitor's access is approved. For a selection of visitors, inspected the access validation records to determine whether visitors' access to OVHcloud's datacenters requires approval by the appropriate manager in the access rights management tool before access being granted. A check is performed at the entrance in order to ensure that the visitor's access is approved.	No exceptions noted
PHY-09	A card-based physical access control system is implemented at the entry and exit points of the datacenter and critical areas within the facilities. Two-factor authentication mechanism is used for access to Critical+ areas.	Inspected the physical access management procedure to determine whether a card-based physical access control system is implemented at the entry and exit points of the datacenter and critical areas within the facilities. Two-factor authentication mechanism is used for access to Critical+ areas. Visited the data centers to determine whether a card-based physical access control system is implemented at the entry and exit points of the datacenter and critical areas within the facilities. Two-factor authentication mechanism is used for access to Critical+ areas.	No exceptions noted

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
PHY-10	Computer rooms are separated according to the level of criticality of the contents except for some DC Tapes where all the rooms are considered critical implementing all security measures associated to this level.	Inspected physical access management procedures to determine whether computer rooms are separated according to the level of criticality of the contents except for some DC Tapes where all the rooms are considered critical implementing all security measures associated to this level.. Visited OVHcloud's datacenters to determine whether computer rooms are separated according to the level of criticality of the contents except for some DC Tapes where all the rooms are considered critical implementing all security measures associated to this level.	No exceptions noted
PHY-11	Detection measures and alerts that are communicated to personnel are implemented to identify anomalies that could result from environmental threat events.	Inspected the physical access procedures, Environmental security management, infrastructure monitoring procedure, Video surveillance management to determine whether detection measures and alerts that are communicated to personnel are implemented to identify anomalies that could result from environmental threat events. Visited OVHcloud's datacenters to determine whether detection measures and alerts that are communicated to personnel are implemented to identify anomalies that could result from environmental threat events.	Exception noted: During the visit LIM datacenter, KPMG noted that flood detection sensors were not installed in front of all server racks due to ongoing expansion work. A test was performed at two locations by applying a wet cloth to the aluminum strips meant to detect water, but no alert was triggered, indicating that the flood detection system was not functioning as expected in those areas. *Refer to section V for management's response*

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
PHY-12	Environmental protections have been installed including the following: • Cooling systems, • Air conditioning units, • Redundant communications lines, • Fire extinguishers, • Smoke detectors, • Redundant electric arrival, • UPS, • Diesel generator.	Inspected the business continuity plan for the Public Cloud, infrastructure monitoring procedure, Environmental security management, Cooling Systems Continuity procedure, Electricity provision continuity procedure to determine whether environmental protections have been installed including the following: • Cooling systems, • Air conditioning units, • Redundant communications lines, • Fire extinguishers, • Smoke detectors, • Redundant electric arrival, • UPS, • Diesel generator. Visited OVHcloud's datacenters to determine whether environmental protections have been installed including the following: • Cooling systems, • Air conditioning units, • Redundant communications lines, • Fire extinguishers, • Smoke detectors, • Redundant electric arrival, • UPS, • Diesel generator.	Exception noted. During the visit of LIM datacenter, KPMG noted that some manual CO_2 fire extinguishers did not have valid inspection stickers. Additionally, none of the locks securing access to the diesel generators were locked at the time of inspection. During the visit of the DC Tape Saint-Pierre-des-Corps, KPMG noted that there is no Diesel Generator. During the visit of the DC Tape Croix, KPMG noted the absence of a Diesel Generator and redundant electric arrival. *Refer to section V for management's response*
PHY-13	Datacenter equipment receives maintenance on at least an annual basis. Generators are tested every 30 days and corrective action taken by the data center manager. *The following equipment are maintained every 3 years which are: the High Voltage Cell, TGBT, the HTA/BT transformer and the fire doors.	Inspected the Equipment Maintenance Schedule to determine whether datacenter equipment receive maintenance on at least an annual basis. Generators are tested every 30 days and corrective action taken by the data center manager. For a sample of equipment inventoried in the CMMS system, inspected the latest maintenance reports to determine whether datacenter equipment receive maintenance on at least an annual basis. Generators are tested every 30 days and corrective action taken by the data center manager.	No exceptions noted

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
PHY-14	Mantraps are used for controlling access to the datacenter. For DC Tapes, alternative access security controls are in place including the use of access badges, CCTV monitoring, security guards.	Inspected the physical access management procedure to determine whether mantraps are used for controlling access to the datacenter. For DC Tapes, alternative access security controls are in place including the use of access badges, CCTV monitoring, security guards. Visited the data centers to determine whether mantraps are used for controlling access to the datacenter. For DC Tapes, alternative access security controls are in place including the use of access badges, CCTV monitoring, security guards.	No exceptions noted
PHY-15	Security perimeters are defined and used to protect areas that contain either restricted or critical information and processing facilities. The outer doors, windows and other construction elements reach a level appropriate to the security requirements. The surrounding wall constructions as well as the locking mechanisms meet the associated requirements.	Inspected physical security procedures to determine whether security perimeters are defined and used to protect areas that contain either restricted or critical information and processing facilities. The outer doors, windows and other construction elements reach a level appropriate to the security requirements. The surrounding wall constructions as well as the locking mechanisms meet the associated requirements. Visited the data centers to determine whether security perimeters are defined and used to protect areas that contain either restricted or critical information and processing facilities. The outer doors, windows and other construction elements reach a level appropriate to the security requirements. The surrounding wall constructions as well as the locking mechanisms meet the associated requirements.	No exceptions noted

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
PHY-16	Rights are managed on the basis of least privilege and need to know. For access to buildings, access permissions are automatically disabled after 3 weeks of inactivity. For perimeters, access permissions are automatically removed when the person leaves.	Inspected datacenter access rights procedure to determine whether the rights are managed on the basis of least privilege and need to know. For access to buildings, access permissions are automatically disabled after 3 weeks of inactivity. For perimeters, access permissions are automatically removed when the person leaves. Inspected datacenter access rights evidence to determine whether the rights are managed on the basis of least privilege and need to know. For access to buildings, access permissions are automatically disabled after 3 weeks of inactivity. For perimeters, access permissions are automatically removed when the person leaves.	No exceptions noted
PHY-17	The sharing of access badges and tailgating are prohibited by policy.	Inspected physical access management procedures to determine whether the sharing of access badges and tailgating are prohibited by policy.	No exceptions noted

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
PHY-18	Power and telecommunications cabling carrying data or supporting information services are protected from interception, interference or damage. Where physical protection of cabling is not feasible (e.g., in some DC Tapes), logical controls and encryption are implemented as compensating measures. The 4 DC Tapes work together and are designed to compensate for the complete or partial loss of power or communication for two of them at the same time, without interrupting the service and while maintaining the protection of customer data.	Inspected physical security procedures to determine whether power and telecommunications cabling carrying data or supporting information services are protected from interception, interference or damage. Where physical protection of cabling is not feasible (e.g., in some DC Tapes), logical controls and encryption are implemented as compensating measures. The 4 DC Tapes work together and are designed to compensate for the complete or partial loss of power or communication for two of them at the same time, without interrupting the service and while maintaining the protection of customer data. Visited OVHcloud's datacenters to determine whether power and telecommunications cabling carrying data or supporting information services are protected from interception, interference or damage. Where physical protection of cabling is not feasible (e.g., in some DC Tapes), logical controls and encryption are implemented as compensating measures. The 4 DC Tapes work together and are designed to compensate for the complete or partial loss of power or communication for two of them at the same time, without interrupting the service and while maintaining the protection of customer data.	No exceptions noted
PHY-19	The datacenters interior layout has been designed for the purpose of maximum prevention.	Inspected the physical access procedures to determine whether the datacenters interior layout has been designed for the purpose of maximum prevention (no false ceilings, cable trays, etc.). Visited OVHcloud's datacenters to determine whether the datacenters interior layout has been designed for the purpose of maximum prevention (no false ceilings, cable trays, etc.).	No exceptions noted

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
PHY-20	Security guards perform a shift round to inspect the facility and document any abnormal incidents. If not, distant security guards monitor the facility H24 7/7 through CCTV and on-site technicians make the ambiguity resolution.	Inspected physical security procedures to determine whether security guards perform a shift round to inspect the facility and document any abnormal incident. If not, distant security guards monitor the facility H24 7/7 through CCTV and on-site technicians make the ambiguity resolution. Visited the datacenters and inspected shift rounds reports to determine whether security guards perform a shift round to inspect the facility and document any abnormal incidents. If not, distant security guards monitor the facility H24 7/7 through CCTV and on-site technicians make the ambiguity resolution.	No exceptions noted
PHY-21	Datacenter staff use the monitoring system to monitor datacenter equipment such as UPS, cooling and air conditioning equipment, etc. Rooms temperature and humidity levels are also monitored.	Inspected the infrastructure monitoring procedure to determine whether datacenter staff use the monitoring system to monitor datacenter equipment such as UPS, cooling and air conditioning equipment, etc. Rooms temperature and humidity levels are also monitored. Visited OVHcloud's datacenters to determine whether datacenter staff use the monitoring system to monitor datacenter equipment such as UPS, cooling and air conditioning equipment, etc. Rooms temperature and humidity levels are also monitored.	No exceptions noted

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
PHY-22	OVHcloud has implemented structural, technical and organizational measures for protection against fire and smoke. These measures include: • Fire and smoke detection systems; • Fire extinguishers located in accessible spots and periodically checked and maintained; • Regular fire protection exercises.	Inspected the Environmental security management to determine whether OVHcloud has implemented structural, technical and organizational measures for protection against fire and smoke. These measures include: • Fire and smoke detection systems; • Fire extinguishers located in accessible spots and periodically checked and maintained; • Regular fire protection exercises. Visited OVHcloud's datacenters to determine whether OVHcloud has implemented structural, technical and organizational measures for protection against fire and smoke. These measures include: • Fire and smoke detection systems; • Fire extinguishers located in accessible spots and periodically checked and maintained; • Regular fire protection exercises.	No exceptions noted
PHY-23	Measures have been implemented by OVHcloud to prevent the failure of cooling and power supplies, including: • Appropriate redundancy of power arrivals; • Appropriate redundancy of cooling and air conditioning systems; • Use of alternative power supplies such as UPS and generators; Regular maintenance of the equipment in accordance with the manufacturer's recommendations.	Inspected the Cooling Systems Continuity procedures, Electricity provision continuity procedures to determine whether measures have been implemented by OVHcloud to prevent the failure of cooling and power supplies, including: • Appropriate redundancy of power arrivals; • Appropriate redundancy of cooling and air conditioning systems; • Use of alternative power supplies such as UPS and generators; • Regular maintenance of the equipment in accordance with the manufacturer's recommendations. Visited OVHcloud's datacenters to determine whether measures have been implemented by OVHcloud to prevent the failure of cooling and power supplies, including: • Appropriate redundancy of power arrivals; • Appropriate redundancy of cooling and air conditioning systems; • Use of alternative power supplies such as UPS and generators; Regular maintenance of the equipment in accordance with the manufacturer's recommendations.	Exception noted. During the visit of the DC Tape Croix, KPMG noted the absence of a Diesel Generator and redundant electric arrival. *Refer to section V for management's response*

Inspected the flowchart describing the process of moving equipment off-site, to determine whether the transfer of equipment to offsite locations is tracked on system and by the

edition of transfer vouchers allowing to identify the transferred equipment. The edition of transfer vouchers is restricted to the storekeepers.

For a selection of equipment moved off-site, inspected the related transfer vouchers, to determine whether the transfer of equipment to offsite locations is tracked on system and by the edition of transfer vouchers allowing to identify the transferred equipment. The edition of transfer vouchers is restricted to the storekeepers.No exceptions notedPHY-24	The transfer of equipment to offsite locations is tracked on system and by the edition of transfer vouchers allowing to identify the transferred equipment. The edition of transfer vouchers is restricted to the storekeepers.	Inspected the Cooling Systems Continuity procedures, Electricity provision continuity procedures to determine whether measures have been implemented by OVHcloud to prevent the failure of cooling and power supplies, including: • Appropriate redundancy of power arrivals; • Appropriate redundancy of cooling and air conditioning systems; • Use of alternative power supplies such as UPS and generators; • Regular maintenance of the equipment in accordance with the manufacturer's recommendations. Visited OVHcloud's datacenters to determine whether measures have been implemented by OVHcloud to prevent the failure of cooling and power supplies, including: • Appropriate redundancy of power arrivals; • Appropriate redundancy of cooling and air conditioning systems; • Use of alternative power supplies such as UPS and generators; Regular maintenance of the equipment in accordance with the manufacturer's recommendations.	No exceptions noted

CHG: Change management

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
CHG-01	OVHcloud protects confidential and personal information during system design, development, testing, implementation and change processes to meet the OVHcloud's objectives related to confidentiality and privacy.	Inspected the development, proofreading and production process to determine whether OVHcloud protects confidential and personal information during system design, development, testing, implementation and change processes to meet the OVHcloud's objectives related to confidentiality and privacy.	No exceptions noted.
CHG-02	OVHcloud requires all changes, including maintenance activities, to be documented and tracked from initiation through change validation and deployment. Moreover, OVHcloud has deployed a SIEM solution that allows operation teams to monitor configuration files changes and other changes in the production environment.	Inspected the change management procedures to determine whether OVHcloud requires all changes, including maintenance activities, to be documented and tracked from initiation through change validation and deployment. Moreover, whether OVHcloud has deployed a SIEM solution that allows operation teams to monitor configuration files changes and other changes in the production environment. For a selection of changes, inspected the related Doctechs and JIRA tickets to determine whether OVHcloud requires all changes, including maintenance activities, to be documented and tracked from initiation through change validation and deployment. Moreover, whether OVHcloud has deployed a SIEM solution that allows operation teams to monitor configuration files changes and other changes in the production environment.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
CHG-03	OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel. Major security changes go through a risk analysis, penetration tests are then performed on n as needed basis.	Inspected the change management procedure to determine whether OVHcloud's software and infrastructure change management process (including emergency change management) requires that changes are: • Formally documented, risk assessed, categorized and prioritized; • Tested prior to migration to production, including code review; • Reviewed and approved by appropriate personnel. Major security changes go through a risk analysis, penetration tests are then performed on n as needed basis. For a selection of changes, inspected the related Doctechs and JIRA tickets to determine whether OVHcloud's applies the defined change management process.	No exceptions noted.
CHG-04	Separate environments are used for development and production. Moreover, data contained in the production environments is not used in development environment in order not to compromise their confidentiality.	Inspected the development procedures and the procedure for development and production environments segregation to determine whether separate environments are used for development and production. Moreover, data contained in the production environments is not used in development environment in order not to compromise their confidentiality.	No exceptions noted.
CHG-05	During the development process, all pull requests must be approved by at least one peer reviewer before being pushed to production.	Inspected the development procedures to determine whether during the development process, all pull requests must be approved by at least one peer reviewer before being pushed to production. For a selection of production development repositories, inspected the extraction of pull requests pushed to production to determine whether during the development process, all pull requests must be approved by at least one peer reviewer before being pushed to production.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
CHG-06	Planned changes to system components that affect the service availability are communicated to customers through the OVHcloud's website. This communication is made 72 hours before the change implementation.	Inspected the OVHcloud customer-facing website to determine whether planned changes to system components that affect the service availability are communicated to customers through the OVHcloud's website. This communication is made 72 hours before the change implementation.	No exceptions noted.
CHG-07	OVHcloud has documented policies and procedures for the secure development process that include review and approval, testing, implementation and maintenance.	Inspected the development policies and procedures to determine whether OVHcloud has documented policies and procedures for the secure development process that include review and approval, testing, implementation and maintenance.	No exceptions noted.
CHG-08	OVHcloud development teams use version control systems to track changes to the source code and allow to undo the changes in case of errors or identified vulnerabilities.	Inspected the development policies and procedures as well as the version control tool to determine whether OVHcloud development teams use version control systems to track changes to the source code and allow to undo the changes in case of errors or identified vulnerabilities.	No exceptions noted.
CHG-09	OVHcloud uses dedicated tools for source code management and software deployment prior deployment into production. Each developer has specific accesses to the repositories and all changes are logged.	Inspected the development policies and procedures as well as the development tools to determine whether OVHcloud uses dedicated tools for source code management and software deployment prior deployment into production. Each developer has specific accesses to the repositories and all changes are logged.	No exceptions noted.

IAM: Identity Access Management

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
IAM-01	Logical access is revoked in a timely manner as part of the termination process and any assets handed over are provably returned upon termination of employment.	Inspected the access management procedures to determine whether logical access is revoked in a timely manner as part of the termination process and any assets handed over are provably returned upon termination of employment. Inspected the leavers extraction and the system extraction of active users to determine whether logical access is revoked in a timely manner as part of the termination process and any assets handed over are provably returned upon termination of employment.	No exceptions noted.
IAM-02	Perimeter entrance requires a documented access request and manager approval prior to access being provisioned. Logical access rights within a perimeter are granted by authorized and approved granters based on rules of need to know and least privilege.	Inspected the access management procedures to determine whether perimeter entrance requires a documented access request and manager approval prior to access being provisioned. Logical access rights within a perimeter are granted by authorized and approved granters based on rules of need to know and least privilege. For a selection of logical access granted in 2024, inspected the related access requests and approvals to determine whether perimeter entrance requires a documented access request and manager approval prior to access being provisioned and these accesses were granted by authorized and approved granters.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
IAM-03	Generic accounts are used on OVHcloud servers used to manage the cloud service. Access to and use of the generic accounts is traced in the bastions and users are clearly identifiable. Logs of the usage of generic accounts contain the following information: source IP address, username of the accessor, type of access, request made. In addition, a capture of the session is made and can be replayed. Bastion logs are saved for at least one year.	Inspected the mechanisms to use and protect generic accounts to determine whether generic accounts are used on OVHcloud servers used to manage the cloud service. Access to and use of the generic accounts is traced in the bastions and users are clearly identifiable. Logs of the usage of generic accounts contain the following information: source IP address, username of the accessor, type of access, request made. In addition, a capture of the session is made and can be replayed. Bastion logs are saved for at least one year. For the entire population of generic accounts, inspected a justification for each account to determine whether the use of generic accounts is appropriate.	No exceptions noted.
IAM-04	In-scope system components require unique username, passwords or authorized SSH keys prior to user authentication.	Inspected the authentication and access management policy to determine whether in-scope system components require unique username, passwords or authorized SSH keys prior to user authentication. Observed the authentication process for in-scope components to determine whether in-scope system components require unique username, passwords or authorized SSH keys prior to user authentication.	No exceptions noted.
IAM-05	OVHcloud has designed a set of business roles corresponding to users' job functions to provide with the strict authorizations to access relevant systems and components they need to complete their functions.	Inspected the extraction of employees having access to the audit tools to determine whether OVHcloud has designed a set of business roles corresponding to users' job functions to provide with the strict authorizations to access relevant systems and components they need to complete their functions	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
IAM-06	Business roles are reviewed on a bi-annual basis by the business role owners ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities.	Inspected the access management procedures as well as evidence of business roles review to determine whether business roles are reviewed on a bi-annual basis by the business role owners ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities. For a selection of attested Business Roles granted in 2024, Inspected evidence of business roles review to determine whether business roles are reviewed on a bi-annual basis by the business role owners ensuring roles remain relevant over time, based on the principle of least privilege and exempt of conflicting responsibilities	No exceptions noted.
IAM-07	OVHcloud permits remote access to production systems by authorized employees, using authorized devices, with multi-factor authentication (MFA) and over encrypted virtual private network (VPN) connection.	Observed the process of access to production to determine whether OVHcloud permits remote access to production systems by authorized employees, using authorized devices , with multi-factor authentication (MFA) and over encrypted virtual private network (VPN) connection.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
IAM-08	Privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties.	Inspected the access rights management procedures to determine whether privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and are personalized as necessary for the execution of tasks ("need-to-know principle"). Access administration is limited to authorized personnel ensuring segregation of duties. Inspected the extraction of privileged access rights as well as the extraction of access rights granters to determine whether privileged access rights are assigned in accordance to the policy for managing user accounts and access rights and access administration is limited to authorized personnel ensuring segregation of duties.	No exceptions noted.
IAM-10	Passwords for in-scope system components are configured according to OVHcloud's password policy.	Inspected OVHcloud's password policy to determine whether there is a password policy in place. Inspected in-scope system components password configuration to determine whether passwords for in-scope system components are configured according to OVHcloud's password policy.	No exceptions noted.
IAM-11	OVHcloud employees' accounts are automatically deactivated if they have not been used for a period of 90 days. Locked accounts are reactivated by authorized users.	Inspected user accounts deactivation configuration to determine whether OVHcloud employees' accounts are automatically deactivated if they have not been used for a period of 90 days. Locked accounts are reactivated by authorized users.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
IAM-12	OVHcloud has established a secure password configuration policy for in-scope system components that includes: • Restriction on password length and complexity (use of alphanumeric, upper- and lower-case characters); • Password age must not exceed 90 days; • The server-side storage takes place using cryptographically strong hash functions; Guidelines and instructions on the secure handling and protection of passwords.	Inspected OVHcloud's password policy to determine whether OVHcloud has established a secure password configuration policy for in-scope system components that includes: • Restriction on password length and complexity (use of alphanumeric, upper- and lower-case characters); • Password age must not exceed 90 days; • The server-side storage takes place using cryptographically strong hash functions; • Guidelines and instructions on the secure handling and protection of passwords. Inspected system components password configurations to determine whether passwords for in-scope system components are configured according to OVHcloud's password policy.	No exceptions noted.
IAM-13	Access to customer data and infrastructure by OVHcloud employees is traced through bastions.	Inspected the logical access policy and bastion configuration to determine whether access to customer data and infrastructure by OVHcloud employees is traced through bastions.	No exceptions noted.

HR: Human Resources

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
HR-01	OVHcloud has documented an Information and Communiation Charter, a Code of Ethics and depending on geographic locations, an Employee Handbook which are reviewed, updated when necessary, and approved by management. Personnel are required to read and accept these documents upon their recruitment. Acceptance of information security policy is formally reaffirmed annually through perimeter membership renewal. Disciplinary measures and sanctions are established for employees who have violated security policies and procedures, internal regulations or the IT charter.	Inspected the Code of Ethics, Internal Regulations, Information Security Policy, Group Information Security Policy, IT charter, Disciplinary process to determine whether OVHcloud has documented an Information and Communication Charter, a Code of Ethics and depending on geographic locations, an Employee Handbook which are reviewed, updated when necessary, and approved by management. Personnel are required to read and accept these documents upon their recruitment. Acceptance of information security policy is formally reaffirmed annually through perimeter membership renewal. Disciplinary measures and sanctions are established for employees who have violated security policies and procedures, internal regulations or the IT charter.	No exceptions noted.

Inspected the documented procedure outlining the annual employee performance evaluation process, conducted via a dedicated platform that assesses past performance and identifies development areas, to determine whether OVHcloud management performs annual performance evaluations of employees where past performance and future developments are assessed and discussed. Annual performance evaluations also include review of skills to be further developed and actions to do so such specific projects or roles to take up or trainings to follow.
The performance evaluation is validated by the manager and the employee. Corrective actions, including training when necessary, are planned.

For a selection of OVHcloud collaborators, inspected evidence of performance evaluations conducted during the attestation period, to determine whether OVHcloud management performs annual performance evaluations of employees where past performance and future developments are assessed and discussed. Annual performance evaluations also include review of skills to be further developed and actions to do so such specific projects or roles to take up or trainings to follow.

The performance evaluation is validated by the manager and the employee. Corrective actions, including training when necessary, are planned.HR-02	OVHcloud management performs annual performance evaluations of employees where past performance and future developments are assessed and discussed. Annual performance evaluations also include review of skills to be further developed and actions to do so such specific projects or roles to take up or trainings to follow. The performance evaluation is validated by the manager and the employee. Corrective actions, including training when necessary, are planned.	Inspected the documented procedure outlining the annual employee performance evaluation process, conducted via a dedicated platform that assesses past performance and identifies development areas, to determine whether OVHcloud management performs annual performance evaluations of employees where past performance and future developments are assessed and discussed. Annual performance evaluations also include review of skills to be further developed and actions to do so such specific projects or roles to take up or trainings to follow. The performance evaluation is validated by the manager and the employee. Corrective actions, including training when necessary, are planned. For a selection of OVHcloud collaborators, inspected evidence of performance evaluations conducted during the attestation period, to determine whether OVHcloud management performs annual performance evaluations of employees where past performance and future developments are assessed and discussed. Annual performance evaluations also include review of skills to be further developed and actions to do so such specific projects or roles to take up or trainings to follow. The performance evaluation is validated by the manager and the employee. Corrective actions, including training when necessary, are planned.	No exceptions noted.

HR-03	OVHcloud provides continued training about its security commitments and requirements for personnel to support the achievement of objectives. Security training includes: • Handling system components and information assets; • Correct behavior in the event of security incidents. Regarding third parties, service providers undertake on the contract signature to train their employees with the training materials provided by OVHcloud.	Inspected the organization and management procedures to determine whether OVHcloud provides continued training about its security commitments and requirements for personnel, to support the achievement of objectives. Security training includes: • Handling system components and information assets; • Correct behavior in the event of security incidents. Regarding third parties, service providers undertake on the contract signature to train their employees with the training materials provided by OVHcloud. For a selection of employees and service providers, inspected respectively the training records and the contracts to determine whether OVHcloud provides continued training about its security commitments and requirements for personnel to support the achievement of objectives.	No exceptions noted.
HR-04	Prior to recruitment, a background screening of personnel is performed. Personnel are verified against regulatory screening databases and their experience as well as training are evaluated (if applicable, depending on the country). For third parties, OVHcloud performs a background check of the enterprise during the third parties audit. Moreover, the third party undertakes on the contract signature to perform a background check of its employees.	Inspected the background check procedure to determine whether prior to recruitment, a background screening of personnel is performed. Personnel are verified against regulatory screening databases and their experience as well as training are evaluated (if applicable, depending on the country). For third parties, OVHcloud performs a background check of the enterprise during the third parties audit. Moreover, the third party undertakes on the contract signature to perform a background check of its employees. For a selection of new employees and providers, inspected respectively the related background check records, contracts and audit reports to determine whether prior to recruitment, a background screening of personnel is performed. Personnel are verified against regulatory screening databases and their experience as well as training are evaluated (if applicable, depending on the country). For third parties, OVHcloud performs a background check of the enterprise during the third parties audit. Moreover, the third party undertakes on the contract signature to perform a background check of its employees.	No exceptions noted.

HR-05	OVHcloud IT Security team members are members of special interest groups specialized in information security, as appropriate for their functions.	Inspected records of membership in information security specialized groups to determine whether OVHcloud IT Security team members are members of special interest groups specialized in information security, as appropriate for their functions.	No exceptions noted.
HR-06	Employees and service providers have been informed about which responsibilities related to confidentiality, will remain in place when their employment is terminated or changed and for how long.	Inspected records of membership in information security specialized groups to determine whether OVHcloud IT Security team members are members of special interest groups specialized in information security, as appropriate for their functions.	No exceptions noted.
HR-07	OVHcloud's employees are provably committed to the IT Charter that defines the guidelines on the acceptable use and safe handling of information assets. Any assets handed over are provably returned upon termination of employment.	Inspected the IT charter to determine whether OVHcloud's employees are provably committed to the IT Charter that defines the guidelines on the acceptable use and safe handling of information assets. Any assets handed over are provably returned upon termination of employment. For a selection of new joiners and leavers, inspected the records related to the IT charter signature and the handing over of assets upon departure to determine whether OVHcloud's employees are provably committed to the IT Charter that defines the guidelines on the acceptable use and safe handling of information assets. Any assets handed over are provably returned upon termination of employment.	No exceptions noted.

HR-08	OVHcloud provides security and awareness training to employees based on identified needs and security hot topics. Target group-oriented awareness and training are addressed on a regular basis providing: • best security practices including references to applicable policies and instructions such as programming good practices, training on internal practices for secure infrastructure and on advanced security including current threat situation; • regular security communications and updates on security news as needed; • secure development communications and training.	Inspected the security training material, as well as supporting evidence obtained from the dedicated secure development training solution provided to OVHcloud's developers to determine whether OVHcloud provides security and awareness training to employees based on identified needs and security hot topics. Target group-oriented awareness and training are addressed on a regular basis providing: • best security practices including references to applicable policies and instructions such as programming good practices, training on internal practices for secure infrastructure and on advanced security including current threat situation; • regular security communications and updates on security news as needed; secure development communications and training. For a selection of developers, inspected evidence of secure development training completed via the dedicated training platform provided to the audited entity's developers, to determine whether OVHcloud provides security and awareness training to employees based on identified needs and security hot topics. Target group-oriented awareness and training are addressed on a regular basis providing: • best security practices including references to applicable policies and instructions such as programming good practices, training on internal practices for secure infrastructure and on advanced security including current threat situation; • regular security communications and updates on security news as needed; • secure development communications and training.	No exceptions noted.
HR-09	Roles and responsibilities for performing employment termination or change in employment are described in the perimeter exit procedure.	Inspected the procedure describing the perimeter exit process to determine whether roles and responsibilities for performing employment termination or change in employment are described in the perimeter exit procedure	No exceptions noted.

BAC: Backup and Recovery

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
BAC-01	Backup restoration tests are performed at least annually for internal data related to the Public Cloud solution administration. Potential errors are immediately investigated and corrected during restoration tests.	Inspected the backup and restoration procedures to determine whether backup restoration tests are performed at least annually for internal data related to the Public Cloud solution administration, and whether potential errors are immediately investigated and corrected during restoration tests. For a selection of quarters, inspected backup restoration test reports to determine whether backup restoration tests are performed at least annually for internal data related to the Public Cloud solution administration, and whether potential errors are immediately investigated and corrected during restoration tests.	No exceptions noted.
BAC-02	Procedures for data backup and recovery are documented and include the frequency of data backup as well as the data retention duration. Backups are performed and monitored using an automated system and corrective actions are taken in a timely manner in case of anomaly.	Inspected policies and instructions for data backup to determine whether procedures for data backup and recovery are documented and include the frequency of data backup as well as the data retention duration, and whether backups are performed and monitored using an automated system and corrective actions are taken in a timely manner in case of anomaly. For a selection of internal and customer servers, inspected the backup execution logs to determine whether procedures for data backup and recovery are documented and include the frequency of data backup as well as the data retention duration, and whether backups are performed and monitored using an automated system and corrective actions are taken in a timely manner in case of anomaly.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
BAC-03	For each Public Cloud product, the redundancy model is based on risk assessment, technical specifications and operational constraints. These elements define the choices for replication locally or at remote sites and the different possible failure scales (network, room, DC). The infrastructure of Public Cloud products is based on scalability and Software Design Storage principles, meaning that the configuration of the control plane can change at will, depending on the customers needs and the technical constraints. Moreover, as the control planes use stateless components, they can be created or modified by simply redeploying the altered components from the code repositories. Geo-redundancy of the control plane is assured for most Public Cloud products on two locations at least (Compute, Block Storage, Kubernetes and Data). On the other side, Object Storage is a mono-datacenter offer, that does not provide yet geo-redundancy of the control plane. However, resilience is assured thanks to the OpenIO and Swift software model.	Inspected the backups and infrastructure and data replication documentation to determine whether: - for each Public Cloud product, the redundancy model is based on risk assessment, technical specifications and operational constraints. These elements define the choices for replication locally or at remote sites and the different possible failure scales (network, room, DC), - the infrastructure of Public Cloud products is based on scalability and Software Design Storage principles, meaning that the configuration of the control plane can change at will, depending on the customers needs and the technical constraints. Moreover, as the control planes use stateless components, they can be created or modified by simply redeploying the altered components from the code repositories, - geo-redundancy of the control plane is assured for most Public Cloud products on two locations at least (Compute, Block Storage, Kubernetes and Data). Moreover whether, Object Storage is a mono-datacenter offer, that does not provide yet geo-redundancy of the control plane, and whether, resilience is assured thanks to the OpenIO and Swift software model.	No exceptions noted.
BAC-04	The ability to modify backup schedules is restricted to the authorized personnel.	Inspected the roles giving access to the backup schedulers to determine whether the ability to modify backup schedules is restricted to the authorized personnel.	No exceptions noted.

NET: Network Security

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
NET-01	End user and server workload network traffic is segmented to support isolation. Moreover, there are dedicated networks for the administrative management of the infrastructure. These networks are separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication.	Inspected the system architecture documentation describing the OVHcloud infrastructure, to determine whether end user and server workload network traffic is segmented to support isolation. Moreover, whether there are dedicated networks for the administrative management of the infrastructure. And finally if networks are separated from the cloud customer's network and protected from unauthorized access by multi-factor authentication.	No exceptions noted.
NET-02	Firewall configuration files are automatically promoted to production firewall devices. Thus, firewall rules are regularly reviewed by peers before approving any change in the corresponding configuration files in production, thanks to CI/CD processes and tools.	Inspected the network security policy and the process for updating firewall rules to determine whether firewall configuration files are automatically promoted to production firewall devices, and whether firewall rules are regularly reviewed by peers before approving any change in the corresponding configuration files in production, thanks to CI/CD processes and tools. For a selection of firewall rules changes, inspected the related JIRA tickets to determine whether firewall configuration files are automatically promoted to production firewall devices, and whether firewall rules are regularly reviewed by peers before approving any change in the corresponding configuration files in production, thanks to CI/CD processes and tools.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
NET-03	Intrusion detection systems and other technical measures are implemented in order to detect and response to network-based attacks, including network monitoring and traffic filtering.	Inspected the network protection mechanisms to determine whether intrusion detection systems and other technical measures are implemented in order to detect and response to network-based attacks, including network monitoring and traffic filtering.	No exceptions noted.
NET-06	OVHcloud has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information.	Inspected the network security policy and the cryptographic means policy to determine whether OVHcloud has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information. Inspected system configuration settings and TLS certificate details for a selected system to determine whether OVHcloud has deployed Transport Layer Security (TLS) for transmission of confidential and/or sensitive information.	No exceptions noted.
NET-07	Incoming and outgoing traffic is formally identified and limited to what is strictly necessary according to the firewall rules. System firewalls are configured to limit unnecessary ports, protocols and services. The only ports open into the environment are defined and validated by the Information Security Operational Referent (ROSI).	Inspected the documented network security management as well as the documented firewall rules review, to determine whether incoming and outgoing traffic is formally identified and limited to what is strictly necessary according to the firewall rules, system firewalls are configured to limit unnecessary ports, protocols and services, and fincally whether the only ports open into the environment are defined and validated by the Information Security Operational Referent (ROSI). For a selection of firewalls, inspected configured rules, to determine whether incoming and outgoing traffic is formally identified and limited to what is strictly necessary according to the firewall rules, system firewalls are configured to limit unnecessary ports, protocols and services, and finally whether the only ports open into the environment are defined and validated by the Information Security Operational Referent (ROSI).	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
NET-09	Virtual hosts are behind software firewalls which are configured to prevent TCP/IP spoofing, packet sniffing, and restrict incoming connections to customer-specified ports.	Inspected the network architecture to determine whether virtual hosts are behind software firewalls which are configured to prevent TCP/IP spoofing, packet sniffing, and restrict incoming connections to customer-specified ports.	No exceptions noted.
NET-10	The documentation of the logical structure of the network used to provision and operate the service is traceable and up-to-date and made available to the employees on the internal documentation system. The documentation shows how the subnets are allocated and how the network is zoned and segmented.	Inspected the Public Cloud network architecture to determine whether the documentation of the logical structure of the network used to provision and operate the service is traceable and up-to-date and made available to the employees on the internal documentation system. The documentation shows how the subnets are allocated and how the network is zoned and segmented.	No exceptions noted.
NET-11	OVHcloud uses NTP servers in order to synchronize the system clocks of all relevant components.	Inspected the time management policy as well as NTP servers to determine whether OVHcloud uses NTP servers in order to synchronize the system clocks of all relevant Public Cloud administration components.	No exceptions noted.
NET-12	OVHcloud has established policies, procedures and technical measures to protect wireless network environments, including the following: • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel.	Inspected the wireless network protection procedures to determine whether OVHcloud has established policies, procedures and technical measures to protect wireless network environments, including the following: • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel.	No exceptions noted.
NET-13	OVHcloud permits the connection to its internal network via VPN and only to authorized equipment using host-based certificates.	Inspected the mechanisms for access to internal network to determine whether OVHcloud permits the connection to its internal network via VPN and only to authorized equipment using host-based certificates.	No exceptions noted.

MON: Logging and Monitoring			
Control ID.	**OVHcloud's Control Activity**	**KPMG's Tests of Controls**	**KPMG's Results of Tests**
MON-01	External access by OVHcloud personnel is logged by the VPN with the following information: accessor IP address, date and event type. Logs are retained for at least 1 year.	Inspected OVHcloud's external access logs to determine whether external access by OVHcloud personnel is logged by the VPN with the following information: accessor IP address, date and event type. Logs are retained for at least 1 year.	No exceptions noted.
MON-02	Use of system components is monitored against acceptable tolerance levels using dedicated tools. Moreover, provisioning and de-provisioning of cloud services are monitored continuously in order to adapt hardware orders and equipment availability. Actual capacity and service provision levels are monitored according to specificities of teams and products.	Inspected capacity management procedure to determine whether use of system components is monitored against acceptable tolerance levels using dedicated tools. Moreover, provisioning and de-provisioning of cloud services are monitored continuously in order to adapt hardware orders and equipment availability. Actual capacity and service provision levels are monitored according to specificities of teams and products. For a selection of weeks, inspected the weekly capacity follow-up reports to determine whether use of system components is monitored against acceptable tolerance levels using dedicated tools. Moreover, provisioning and de-provisioning of cloud services are monitored continuously in order to adapt hardware orders and equipment availability. Actual capacity and service provision levels are monitored according to specificities of teams and products.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
MON-03	Activity logs on the administration infrastructure are centralized on dedicated syslog servers and are automatically monitored according to defined scenarios in order to detect potential security events. Detected events are raised through alerts to the appropriate departments for investigation and corrective action. Access logs on the bastions are monitored automatically and alerts are raised when suspicious events occur according to predefined patterns. Investigations and corrective actions are performed in a timely manner.	Inspected the log management procedures to determine whether activity logs on the administration infrastructure are centralized on dedicated syslog servers and are automatically monitored according to defined scenarios in order to detect potential security events, whether detected events are raised through alerts to the appropriate departments for investigation and corrective action, and finally whether access logs on the bastions are monitored automatically and alerts are raised when suspicious events occur according to predefined patterns. Investigations and corrective actions are performed in a timely manner. Inspected the monitoring activity records to determine whether activity logs on the administration infrastructure are centralized on dedicated syslog servers and are automatically monitored according to defined scenarios in order to detect potential security events, whether detected events are raised through alerts to the appropriate departments for investigation and corrective action, and finally whether access logs on the bastions are monitored automatically and alerts are raised when suspicious events occur according to predefined patterns. Investigations and corrective actions are performed in a timely manner.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
MON-04	As part of its monitoring processes, OVHcloud monitors the logging and monitoring components in order to detect any failure that could cause the logging to stop or that could alter the logs. Failures are automatically reported, and corrective actions are taken in a timely manner.	Inspected the log management procedures as well as the supervision of the infrastructure procedure to determine whether as part of its monitoring processes, OVHcloud monitors the logging and monitoring components in order to detect any failure that could cause the logging to stop or that could alter the logs. Moreover, whether failures are automatically reported, and corrective actions are taken in a timely manner. For a selection of weeks, inspected logs review reports to determine whether as part of its monitoring processes to determine whether as part of its monitoring processes, OVHcloud monitors the logging and monitoring components in order to detect any failure that could cause the logging to stop or that could alter the logs. Moreover, whether failures are automatically reported, and corrective actions are taken in a timely manner.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
MON-05	OVHcloud has documented policies and procedures regarding the logging and monitoring of events on system components, that include: • Operational aspects of logging and monitoring (logs generation, lifecycle, retention, review and alerting); • Time synchronization of system components; and • Compliance with legal and regulatory frameworks.	Inspected the log management procedures as well as the logging and monitoring systems to determine whether OVHcloud has documented policies and procedures regarding the logging and monitoring of events on system components, that include: • Operational aspects of logging and monitoring (logs generation, lifecycle, retention, review and alerting); • Time synchronization of system components; and • Compliance with legal and regulatory frameworks.	No exceptions noted.
MON-06	OVHcloud has documented policies and procedures regarding protection requirements, lifecycle and retention of logs on its systems, that include: • Access only to authorized users and systems; • Backup and retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.	Inspected the mechanisms for logs protection to determine whether OVHcloud has documented policies and procedures regarding protection requirements, lifecycle and retention of logs on its systems, that include: • Access only to authorized users and systems; • Backup and retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
MON-07	Users access and activities on the production environment are logged by a bastion. The logged information is used to detect events that may indicate misuse. When such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.	Inspected logging procedures as well as the bastion logging mechanisms to determine whether users access and activities on the production environment are logged by a bastion, the logged information is used to detect events that may indicate misuse. And in case such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken. For a selection of alert tickets, inspected the bastion logging mechanisms as well as the associated activity logs, to determine whether to determine whether users access and activities on the production environment are logged by a bastion, the logged information is used to detect events that may indicate misuse. And in case such an event is identified, the responsible personnel are informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken.	No exceptions noted.

IM: Incident Management

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
IM-01	After a security incident has been identified and analyzed for root cause analysis and impact, the action plan is carried out and documented. In the case, the security incident has an impact on the cloud services, a communication is sent to the affected customers. The security incident is formalized within a post-mortem detailing all security incident processing steps.	Inspected the incident management procedures to determine whether after a security incident has been identified and analyzed for root cause analysis and impact, the action plan is carried out and documented. In the case, the security incident has an impact on the cloud services, a communication is sent to the affected customers. The security incident is formalized within a post-mortem detailing all security incident processing steps. For a selection of security incidents and events, inspected the related tickets and the communications sent to the affected customers to determine whether after a security incident has been identified and analyzed for root cause analysis and impact, the action plan is carried out and documented. In the case, the security incident has an impact on the cloud services, a communication is sent to the affected customers. The security incident is formalized within a post-mortem detailing all security incident processing steps.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
IM-02	On an annual basis, a crisis unit simulation is performed to ensure the incident response procedures are up-to-date and accurate. When updating the incident response plan, lessons learned are used to implement changes to ensure that incident response procedures are effective.	Inspected the incident management procedures to determine whether on an annual basis, a crisis unit simulation is performed to ensure the incident response procedures are up-to-date and accurate. When updating the incident response plan, lessons learned are used to implement changes to ensure that incident response procedures are effective. Inspected the report of Cyber Crisis Exercise to determine whether on in 2024 a crisis unit simulation was performed to ensure the incident response procedures are up-to-date and accurate.	No exceptions noted.
IM-03	Employees, customers and providers have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel. OVHcloud also provides user guides, security alerts and known issues on its websites and client portal with information to improve security knowledge and awareness.	Inspected OVHcloud policies, procedures, agreements with providers, general terms of service as well as the customer-facing website to determine whether employees, customers and providers have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel. OVHcloud also provides user guides, security alerts and known issues on its websites and client portal with information to improve security knowledge and awareness.	No exceptions noted.
IM-04	OVHcloud has a whistle blowing platform available to employees and customers. Management monitors customers and employees' complaints reported via the platform.	Inspected the whistle blowing platform follow-up records to determine whether OVHcloud has a whistle blowing platform available to employees and customers. Management monitors customers and employees' complaints reported via the platform.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
IM-05	When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.	Inspected the incident management procedure to determine whether when a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis. For a selection of security incidents and events, inspected the related tickets to determine whether when a potential security incident is detected, a defined incident management process is initiated by authorized personnel. All incidents related to security are logged, tracked and communicated to affected parties by management as appropriate. The root cause is determined, and the event is given a classification and a level of impact. Corrective actions are implemented in accordance with defined policies and procedures, by a dedicated team. All security incidents are reported to the CISO and security incidents that may affect security compliance are reported to the ISMS Management Team based on the need-to-know basis.	No exceptions noted.

SEC: Logical Security

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
SEC-01	OVHcloud's procedures on antivirus and anti-malware protection are documented and communicated through its intranet. An antivirus and anti-malware program is implemented and kept updated on workstations, laptops, and servers, to provide for the interception or detection and remediation of malware.	Inspected the procedure related to antivirus and anti-malware management to determine whether OVHcloud's procedures on antivirus and anti-malware protection are documented and communicated through its intranet, and whether an antivirus and anti-malware program is implemented and kept updated on workstations, laptops, and servers, to provide for the interception or detection and remediation of malware. For a selection of workstations, laptops and servers, inspected the antivirus configuration to determine whether OVHcloud's procedures on antivirus and anti-malware protection are documented and communicated through its intranet, and whether an antivirus and anti-malware program is implemented and kept updated on workstations, laptops, and servers, to provide for the interception or detection and remediation of malware.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
SEC-02	Internal and external vulnerability scans are performed respectively monthly and quarterly. Penetration tests are performed at least annually and on major changes. Tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity. A remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.	Inspected the monitoring and reassessment procedure to determine whether internal and external vulnerability scans are performed respectively monthly and quarterly, penetration tests are performed at least annually and on major changes, tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity, and finally whether remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality. For a selection of vulnerability scans and penetration tests, inspected the related reports and corrective actions to determine whether internal and external vulnerability scans are performed respectively monthly and quarterly, penetration tests are performed at least annually and on major changes, tools used during vulnerability scans and penetration tests are compatible with virtualization technologies. Identified vulnerabilities are classified by level of severity, and finally whether remediation plan is developed, and patches are deployed to remediate identified vulnerabilities according to their criticality.	No exceptions noted.
SEC-03	Storage for laptops and workstations having access to the production environment is encrypted.	Inspected the documented workstation and laptop management policies, to determine whether storage for laptops and workstations having access to the production environment is encrypted. For a selection of laptops and workstations, inspected the encryption configurations, to determine whether storage for laptops and workstations having access to the production environment is encrypted.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
SEC-04	The use of removable media on workstations is disabled.	Inspected the workstation security policy to determine whether the use of removable media on workstations is disabled. For a selection of workstations, inspected their configurations to determine whether the use of removable media on workstations is disabled.	No exceptions noted.
SEC-05	System components used to provide the services on the Public Cloud perimeter are hardened according to generally accepted industry standards. The use of a hardened operating system known as the Hardened Debian distribution provided by Digit Core (based on CIS configuration) is encouraged. Moreover, for CI/CD, the use of collaborative tools like Puppet or Bitbucket is mandatory to ensure versioning or integrity monitoring..	Inspected the documentation related to the hardening of system components to determine whether : - system components used to provide the services on the Public Cloud perimeter are hardened according to generally accepted industry standards., - the use of a hardened operating system known as the Hardened Debian distribution provided by Digit Core (based on CIS configuration) is encouraged, - for CI/CD, the use of collaborative tools like Puppet or Bitbucket is mandatory to ensure versioning or integrity monitoring.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
SEC-06	OVHcloud uses CVSS (Common Vulnerability Scoring System) for the scoring of vulnerabilities and relies on the online NIST database as well as other sources for the discovery of vulnerabilities. Prioritization and implementation of actions to promptly remediate or mitigate identified vulnerabilities are based on a list of assets ordered by criticality that relies on product-specific criteria for each Public Cloud product. Security patches are then deployed within a time-frame based on asset criticality.	Inspected the documented vulnerability management procedure to determine whether : - OVHcloud uses CVSS (Common Vulnerability Scoring System) for the scoring of vulnerabilities and relies on the online NIST database as well as other sources for the discovery of vulnerabilities, - prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities are based on a list of assets ordered by criticality that relies on product-specific criteria for each Public Cloud product. Security patches are then deployed within a time-frame based on asset criticality. For a selection of vulnerability scans and penetration tests, inspected the related reports and corrective actions to determine whether : - OVHcloud uses CVSS (Common Vulnerability Scoring System) for the scoring of vulnerabilities and relies on the online NIST database as well as other sources for the discovery of vulnerabilities, - prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities are based on a list of assets ordered by criticality that relies on product-specific criteria for each Public Cloud product. Security patches are then deployed within a time-frame based on asset criticality.	No exceptions noted.
SEC-07	Employees can only install trusted software available in defined stores for MAC, Windows and Linux workstations and laptops.	Inspected the workstations security policy to determine whether employees can only install trusted software available in defined stores for MAC, Windows and Linux workstations and laptops.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
		Inspected users' ability to install software on workstations to determine whether employees can only install trusted software available in defined stores for MAC, Windows and Linux workstations and laptops.	
SEC-08	OVHcloud has a hardware conformity check process to test the servers when they are assembled and before being used by a customer. The performed tests include tests on CPU, RAM, Motherboard, Network, disks, etc. in order to ensure that the server is fully operational before being put in production.	Inspected the hardware conformity check procedure, to determine whether OVHcloud has a hardware conformity check process to test the servers when they are assembled and before being used by a customer. The performed tests include tests on CPU, RAM, Motherboard, Network, disks, etc. in order to ensure that the server is fully operational before being put in production. For a selection of new commissioned servers, inspected the conformity check results, to determine whether OVHcloud has a hardware conformity check process to test the servers when they are assembled and before being used by a customer. The performed tests include tests on CPU, RAM, Motherboard, Network, disks, etc. in order to ensure that the server is fully operational before being put in production.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
SEC-09	Policies and procedures for data encryption are documented and include: • Usage of strong and trusted encryption procedures and secure network protocols that correspond to the state-of-the-art, such as trusted symmetric encryption algorithms, trusted hashing algorithms, trusted one-way password encryption algorithms, trusted key exchange algorithms, trusted SSL/TLS Protocols and certificates... etc. • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys.	Inspected the cryptographic means policy to determine whether policies and procedures for data encryption are documented and include: • Usage of strong and trusted encryption procedures and secure network protocols that correspond to the state-of-the-art, such as trusted symmetric encryption algorithms, trusted hashing algorithms, trusted one-way password encryption algorithms, trusted key exchange algorithms, trusted SSL/TLS Protocols and certificates... etc. • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys.	No exceptions noted.

Inspected the cryptographic means policy to determine whether OVHcloud has documented a key management policy that describes the process of secure key management that include:

- Keys generation in a secure Locker / Vault using trusted and secure algorithms;
- Key storage and communication over secure channels;

Key lifecycle and disposal. SEC-10	OVHcloud has documented a key management policy that describes the process of secure key management that include: • Keys generation in a secure Locker / Vault using trusted and secure algorithms; • Key storage and communication over secure channels; • Key lifecycle and disposal.	Inspected the cryptographic means policy to determine whether OVHcloud has documented a key management policy that describes the process of secure key management that include: • Keys generation in a secure Locker / Vault using trusted and secure algorithms; • Key storage and communication over secure channels; • Key lifecycle and disposal.	No exceptions noted.
SEC-11	A session management mechanism is used on system components in order to deactivate the user's session after a defined time interval, depending on the component.	Inspected system components configuration to determine whether a session management mechanism is used on system components in order to deactivate the user's session after a defined time interval, depending on the component.	No exceptions noted.

SEC-12	The Public Cloud solution is based on OpenStack technologies. It is a market-recognized open-source tool offering standardized virtualization tools and features that are compatible with other solutions.	Inspected the Public Cloud solutions and documentation to determine whether the Public Cloud solution is based on OpenStack technologies. It is a market-recognized open-source tool offering standardized virtualization tools and features that are compatible with other solutions.	No exceptions noted.

PCY: Privacy

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
PCY-01	Data subjects are able to determine whether OVHcloud maintains personal information about them and may obtain access to and update their personal information. When data access is denied, data subjects are informed, in writing, of the reason a request was denied.	Inspected OVHcloud's data protection agreement and general terms of service to determine whether data subjects are able to determine whether OVHcloud maintains personal information about them and may obtain access to and update their personal information. When data access is denied, data subjects are informed, in writing, of the reason a request was denied. For a selection of access requests to personal information, inspected the requests and the communications sent to the individuals to determine whether data subjects are able to determine whether OVHcloud maintains personal information about them and may obtain access to and update their personal information. When data access is denied, data subjects are informed, in writing, of the reason a request was denied.	No exceptions noted.
PCY-02	Events that resulted in unauthorized use or disclosure of personal information are communicated to the data subjects, legal and regulatory authorities, and others as required.	Inspected the incident management procedures as well as the communication records related to privacy incidents to determine whether events that resulted in unauthorized use or disclosure of personal information are communicated to the data subjects, legal and regulatory authorities, and others as required	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
PCY-03	OVHcloud records customers access requests to their personal information to maintain a complete, accurate, and timely record of such requests.	Inspected documentation related to the handling of data subject requests to determine whether OVHcloud records customers access requests to their personal information to maintain a complete, accurate, and timely record of such requests.	No exceptions noted.
PCY-04	A data protection agreement is provided to data subjects, which addresses the following topics: • Purpose for collecting personal information • Choice and consent • Types of personal information collected • Methods of collection • Use, retention, and disposal • Access • Disclosure to third parties • Security for privacy	Inspected the data protection agreement to determine whether a data protection agreement is provided to data subjects, which addresses the following topics: • Purpose for collecting personal information • Choice and consent • Types of personal information collected • Methods of collection • Use, retention, and disposal • Access • Disclosure to third parties • Security for privacy	No exceptions noted.
PCY-05	An objective description of the activities covered is included in the OVHcloud's Privacy policy.	Inspected the documented privacy policy to determine whether an objective description of the activities covered is included in the OVHcloud's Privacy policy.	No exceptions noted.
PCY-06	Notice is provided by OVHcloud to data subjects before the time personal information is collected on its website.	Inspected OVHcloud's customer-facing website to determine whether a notice is provided by OVHcloud to data subjects before the time personal information is collected on its website.	No exceptions noted.

Inspected the general terms of service and the data protection agreement as well as the records of consent before collection of personal data, to determine whether data subjects are informed about the choices available to them with respect to the collection, use and disclosure of personal information for which OVHcloud is controller. Moreover, OVHcloud obtains consent from data subjects before personal information is collected on its website. Documentation	Data subjects are informed about the choices available to them with respect to the collection, use and disclosure of personal information for which OVHcloud is controller. Moreover, OVHcloud obtains consent from data subjects before personal information is collected on its website. Documentation of explicit consent is retained in accordance with objectives related to privacy.	Inspected the general terms of service and the data protection agreement as well as the records of consent before collection of personal data, to determine whether data subjects are informed about the choices available to them with respect to the collection, use and disclosure of personal information for which OVHcloud is controller. Moreover, OVHcloud obtains consent from data subjects before personal information is collected on its website. Documentation of explicit consent is retained in accordance with objectives related to privacy.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
of explicit consent is retained in accordance with objectives related to privacy.PCY-07			
PCY-08	The collection, use and disclosure of personal information is limited to that necessary to meet OVHcloud's objectives.	Inspected the data processing agreement, to determine whether the collection, use and disclosure of personal information is limited to that necessary to meet OVHcloud's objectives.	No exceptions noted.
PCY-09	Personal information is retained for no longer than necessary to fulfill the stated purposes, unless a law or regulation specifically requires otherwise.	Inspected records of personal data deletion, to determine whether personal information is retained for no longer than necessary to fulfill the stated purposes, unless a law or regulation specifically requires otherwise.	No exceptions noted.
PCY-10	OVHcloud has designed and implemented policies and procedures to protect personal information from erasure or destruction during the specified retention period of the information.	Inspected information protection policies and procedures, to determine whether OVHcloud has designed and implemented policies and procedures to protect personal information from erasure or destruction during the specified retention period of the information.	No exceptions noted.
PCY-11	Requests for deletion of personal information are captured, and information related to the requests is identified and flagged for destruction to meet OVHcloud's objectives related to privacy.	Inspected the documented process for handling data subject rights to determine whether requests for deletion of personal information are captured, and information related to the requests is identified and flagged for destruction to meet OVHcloud's objectives related to privacy.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
		For a selection of requests for deletion of personal data, inspected the requests and related actions, to determine whether requests for deletion of personal information are captured, and information related to the requests is identified and flagged for destruction to meet OVHcloud's objectives related to privacy.	
PCY-12	OVHcloud destroys personal information that is no longer retained. Policies and procedures are implemented to erase or otherwise destroy personal information in a manner that prevents loss, theft, misuse, or unauthorized access.	Inspected records of personal data deletion, to determine whether OVHcloud destroys personal information that is no longer retained. Policies and procedures are implemented to erase or otherwise destroy personal information in a manner that prevents loss, theft, misuse, or unauthorized access.	No exceptions noted.
PCY-13	The identity of data subjects who request access to their personal information is authenticated before they are given access to that information. Personal information is provided to data subjects in an understandable form, in a reasonable time frame.	Inspected the process for handling data subjects' requests, to determine whether the identity of data subjects who request access to their personal information is authenticated before they are given access to that information. Personal information is provided to data subjects in an understandable form, in a reasonable time frame. For a selection of requests of access to personal data, inspected the requests and the communications sent to the individuals, to determine whether the identity of data subjects who request access to their personal information is authenticated before they are given access to that information. Personal information is provided to data subjects in an understandable form, in a reasonable time frame.	No exceptions noted.
PCY-14	OVHcloud maintains a record of detected unauthorized disclosures of personal information that is complete, accurate, and timely.	Inspected records of unauthorized disclosures of personal information, to determine whether OVHcloud maintains a record of detected unauthorized disclosures of personal information that is complete, accurate, and timely.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
PCY-15	OVHcloud takes remedial action in response to misuse of personal data by a third party to whom OVHcloud has transferred such information.	Inspected the procedure for handling personal data by a third party, to determine whether OVHcloud takes remedial action in response to misuse of personal data by a third party to whom OVHcloud has transferred such information. For a selection of cases of misuse of personal information by a third party, inspected the records of incident handling to determine whether OVHcloud takes remedial action in response to misuse of personal data by a third party to whom OVHcloud has transferred such information.	No exceptions noted. There was no cases of misuse of personal information by a third party during the examination period. As such, KPMG was unable to test the operating effectiveness of this control because the circumstances that warrant the operation of the control did not occur during the examination period.
PCY-16	The processes, systems, and third parties involved in the handling of personal information are identified.	Inspected the personal information processing register, to determine whether the processes, systems, and third parties involved in the handling of personal information are identified.	No exceptions noted.
PCY-17	OVHcloud has a process in place to address inquiries, complaints, and disputes raised by customers or legal authorities. Each complaint is addressed, and the resolution is documented and communicated to the individual.	Inspected the documented procedure along with OVHcloud's publicly available resources, to determine whether OVHcloud has a process in place to address inquiries, complaints, and disputes raised by customers or legal authorities. Each complaint is addressed, and the resolution is documented and communicated to the individual. For a selection of inquiries and complaints, inspected the related records to determine whether OVHcloud has a process in place to address inquiries, complaints, and disputes raised by customers or legal authorities. Each complaint is addressed, and the resolution is documented and communicated to the individual.	No exceptions noted.
PCY-18	OVHcloud's top management follows-up annually on the progress of the GDPR program in order to ensure compliance with privacy objectives.	Inspected the latest GDPR program review, to determine whether OVHcloud's top management follows-up annually on the progress of the GDPR program in order to ensure compliance with privacy objectives.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
PCY-19	OVHcloud performs ongoing procedures for monitoring the effectiveness of controls over personal information and for taking timely corrective actions when necessary.	Inspected privacy controls effectiveness reviews, to determine whether OVHcloud performs ongoing procedures for monitoring the effectiveness of controls over personal information and for taking timely corrective actions when necessary.	No exceptions noted.
PCY-20	Personal information is disclosed only to third parties who have agreements with OVHcloud to protect personal information in a manner consistent with OVHcloud's privacy requirements. OVHcloud has procedures in place to evaluate that the third parties meet these requirements. Moreover, personal information is disclosed only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject.	Inspected the third parties control procedure, to determine whether Personal information is disclosed only to third parties who have agreements with OVHcloud to protect personal information in a manner consistent with OVHcloud's privacy requirements. OVHcloud has procedures in place to evaluate that the third parties meet these requirements. Moreover, personal information is disclosed only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject. For a selection of third parties to whom personal data is disclosed, inspected the related data protection agreements and evidence of verification of the third party's compliance with data protection requirements to determine whether personal information is disclosed only to third parties who have agreements with OVHcloud to protect personal information in a manner consistent with OVHcloud's privacy requirements. OVHcloud has procedures in place to evaluate that the third parties meet these requirements. Moreover, personal information is disclosed only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject.	No exceptions noted.
PCY-21	Personal information is accurate, complete and relevant for the purposes for which it is to be used.	Inspected the data processing agreement, to determine whether personal information is accurate, complete and relevant for the purposes for which it is to be used.	No exceptions noted.

THP: Third Parties

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
THP-01	OVHcloud ensures the compliance of service providers with its security requirements and internal policies through regular reviews based on contractual agreements. These contractual agreements include obligations of service providers such as: • Compliance with OVHcloud security measures; • Background checks of personnel involved in providing the service; • Confidentiality, intellectual property and personal data measures; • Reporting security incidents. Identified violations and deviations are subjected to analysis, evaluation and treatment	Inspected the third party's security management policy to determine whether OVHcloud ensures the compliance of service providers with its security requirements and internal policies through regular reviews based on contractual agreements. These contractual agreements include obligations of service providers such as: • Compliance with OVHcloud security measures; • Background checks of personnel involved in providing the service; • Confidentiality, intellectual property and personal data measures; • Reporting security incidents. Identified violations and deviations are subjected to analysis, evaluation and treatment For a selection of service providers, inspected contractual clauses to determine whether OVHcloud ensures the compliance of service providers with its security requirements and internal policies through regular reviews based on contractual agreements. These contractual agreements include obligations of service providers such as: • Compliance with OVHcloud security measures; • Background checks of personnel involved in providing the service; • Confidentiality, intellectual property and personal data measures; • Reporting security incidents. Identified violations and deviations are subjected to analysis, evaluation and treatment	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
THP-02	OVHcloud has clauses in its agreements with providers to terminate relationships when necessary.	Inspected the documented provider agreement to determine whether OVHcloud has clauses in its agreements with providers to terminate relationships when necessary. For a selection of providers, inspected the related agreements to determine whether OVHcloud has clauses in its agreements with providers to terminate relationships when necessary	No exceptions noted.
THP-03	OVHcloud limits the risk related to the intervention of service providers in the perimeter of its provided services and products. Service providers do not contribute to the processes of development, change and incident management of the services provided by OVHcloud and thus, do not have access to confidential information. If a third party develops software for a perimeter, a development guideline based on OWASP is provided to them and its employees must be trained accordingly.	Inspected the third parties security policy to determine whether OVHcloud limits the risk related to the intervention of service providers in the perimeter of its provided services and products. Service providers do not contribute to the processes of development, change and incident management of the services provided by OVHcloud and thus, do not have access to confidential information. If a third party develops software for a perimeter, a development guideline based on OWASP is provided to them and their employees must be trained accordingly. For a selection of providers, inspected the third parties security policy to determine whether OVHcloud limits the risk related to the intervention of service providers in the perimeter of its provided services and products. Service providers do not contribute to the processes of development, change and incident management of the services provided by OVHcloud and thus, do not have access to confidential information. If a third party develops software for a perimeter, a development guideline based on OWASP is provided to them and their employees must be trained accordingly.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
THP-04	Third-party relationships are formalized with agreements that identify the critical business activities performed by the third party and the security requirements. Moreover, OVHcloud keeps a file for the monitoring of third parties that includes: • Company name; • Address; • Date of contract signature and contract end; • Description of the service; • Responsible contact person at OVHcloud and at the service provider.	Inspected the third parties security policy to determine whether third-party relationships are formalized with agreements that identify the critical business activities performed by the third party and the security requirements. Moreover, OVHcloud keeps a file for the monitoring of third parties that includes: • Company name; • Address; • Date of contract signature and contract end; • Description of the service; • Responsible contact person at OVHcloud and at the service provider. Inspected the third-parties inventory and third-party agreements for a selection of providers to determine whether third-party relationships are formalized with agreements that identify the critical business activities performed by the third party and the security requirements. Moreover, OVHcloud keeps a file for the monitoring of third parties that includes: • Company name; • Address; • Date of contract signature and contract end; • Description of the service; • Responsible contact person at OVHcloud and at the service provider	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
THP-05	A security policy with third parties has been implemented by OVHcloud that includes: • Signature of agreements with third parties that define business activities and security requirements; • Background check of third parties; • Audit and monitoring of third parties; • Security training and awareness of third parties.	Inspected the third-parties security policy to determine whether a security policy with third parties has been implemented by OVHcloud that includes: • Signature of agreements with third parties that define business activities and security requirements; • Background check of third parties; • Audit and monitoring of third parties; • Security training and awareness of third parties.. For a selection of providers, inspected the related agreements and audit reports to determine whether a security policy with third parties has been implemented by OVHcloud that includes: • Signature of agreements with third parties that define business activities and security requirements; • Background check of third parties; • Audit and monitoring of third parties; • Security training and awareness of third parties.	No exceptions noted.

CUS: Customer

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
CUS-01	When a customer terminates his contract, a logical erasure, is performed on all the servers concerned. If this logical erasure fails, the concerned hard drives are destroyed according to a defined secure destruction process.	Inspected the documented "Data Recycling" procedure to gain a better understanding and determine whether upon termination of an OVHcloud customer's contract, a logical erasure, is performed on all the servers concerned. If this logical erasure fails, the hard drives concerned are destroyed according to a defined secure destruction process. Inspected records for a selection of deletion operations, to determine whether upon an OVHcloud customer's contract termination, a logical erasure, is performed for all the servers concerned. If this logical erasure fails, the concerned hard drives are destroyed according to a defined secure destruction process.	No exceptions noted.
CUS-02	OVHcloud provides the Public Cloud customers with access rights mechanisms to manage customer users' access rights on the Public Cloud products.	Inspected the Public Cloud access management documentation provided to customers to determine whether OVHcloud provides the Public Cloud customers with access rights mechanisms to manage customer users' access rights on the Public Cloud products.	No exceptions noted.
CUS-03	OVHcloud deletes customer data following termination of the customer's contract	Inspected the publicly available terms and conditions documents for OVHcloud services/products included in the attestation scope to determine whether contractual provisions require deletion of customer data following termination of the customer's contract. Inspected records for a selection of deletion operations, to determine whether the deletion of customer data was performed on all relevant servers upon contract termination.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
CUS-04	OVHcloud has developed application programming interfaces (API) allowing its customers to interact with OVHcloud products without using the graphical customer interface. The interfaces are clearly documented for subject matter experts on how they can be used to retrieve the data. The interfaces use the RESTful standard and can be used with different programming languages.	Inspected application programming interfaces (API) descriptions to determine whether OVHcloud has developed application programming interfaces (API) allowing its customers to interact with OVHcloud products without using the graphical customer interface. The interfaces are clearly documented for subject matter experts on how they can be used to retrieve the data. The interfaces use the RESTful standard and can be used with different programming languages.	No exceptions noted.
CUS-05	OVHcloud has defined in customer contractual agreements, the aspects related to the termination of the contractual relationship. The customer is responsible of taking all the necessary measures in order to ensure the conservation of their data before the cancellation of the service. All content and data stored by the customer as part of the service are deleted within an agreed duration from the expiration date of the service or end of payment.	Inspected the general terms of service and the specific terms related to the Public Cloud offer to determine whether OVHcloud has defined in customer contractual agreements, the aspects related to the termination of the contractual relationship. The customer is responsible of taking all the necessary measures in order to ensure the conservation of their data before the cancellation of the service. All content and data stored by the customer as part of the service are deleted within an agreed duration from the expiration date of the service or end of payment.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
CUS-06	Investigation requests from government agencies are checked by the Legal Team in order to assess their authenticity and their compliance with the applicable legal framework. Access to or disclosure of customer data to the government agency is performed only after the Legal Team has confirmed the request's authenticity and legal basis.	Inspected the procedure for authority requests handling to determine whether investigation requests from government agencies are checked by the Legal Team in order to assess their authenticity and their compliance with the applicable legal framework. Access to or disclosure of customer data to the government agency is performed only after the Legal Team has confirmed the request's authenticity and legal basis. For a selection of requests for investigation, inspected the request handling records to determine whether OVHcloud informs the concerned customer during an investigation or request for evidence by a government agency, unless it is prohibited by the applicable law.	No exceptions noted. There were no requests for investigation during the examination period. As such, KPMG was unable to test the operating effectiveness of this control because the circumstances that warrant the operation of the control did not occur during the examination period.
CUS-07	OVHcloud informs the concerned customer during an investigation or request for evidence by a government agency, unless it is prohibited by the applicable law.	Inspected the procedure for authority requests handling to determine whether OVHcloud informs the concerned customer during an investigation or request for evidence by a government agency, unless it is prohibited by the applicable law.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
CUS-08	In case of disclosure of customer data to a government agency as part of an investigation, the disclosure is strictly limited to the data requested by the authority.	Inspected the procedure for authority requests handling as well as the documentation describing the process for handling requests from government authorities, to determine whether in case of disclosure of customer data to a government agency as part of an investigation, the disclosure is strictly limited to the data requested by the authority.	No exceptions noted.
CUS-09	OVHcloud provides the Public Cloud customers with guidelines and recommendations for the configuration and use of the cloud service provided. The information is publicly available on OVHcloud's website and includes: • Instructions for secure configuration; • Authentication mechanisms; • Access and access rights management; and • Services and functions for administration of the cloud service.	Inspected OVHcloud's customer facing website to determine whether OVHcloud provides the Public Cloud customers with guidelines and recommendations for the configuration and use of the cloud service provided. The information is publicly available on OVHcloud's website and includes: • Instructions for secure configuration; • Authentication mechanisms; • Access and access rights management; and • Services and functions for administration of the cloud service.	No exceptions noted.
CUS-10	OVHcloud provides its customers with dedicated tools for monitoring and supervision of their Public Cloud. These tools provide information regarding system performance and availability and include alerts and error handling mechanisms.	Inspected the monitoring tools provided to the Public Cloud customers to determine whether OVHcloud provides its customers with dedicated tools for monitoring and supervision of their Public Cloud, moreover whether these tools provide information regarding system performance and availability and include alerts and error handling mechanisms.	No exceptions noted.
CUS-11	OVHcloud provides its customers with a software-defined networking (SDN) tool that allows the customers to implement network access rules and other network services.	Inspected the SDN tools user guides provided to Public Cloud customers to determine whether OVHcloud provides its customers with a software-defined networking (SDN) tool that allows the customers to implement network access rules and other network services.	No exceptions noted.

Control ID.	OVHcloud's Control Activity	KPMG's Tests of Controls	KPMG's Results of Tests
CUS-12	OVHcloud provides its customers with the ability to restrict the access to a virtual machine via the administration console.	Inspected the Public Cloud user guides on OVHcloud's customer facing website to determine whether OVHcloud provides its customers with the ability to restrict the access to a virtual machine via the administration console.	No exceptions noted.
CUS-13	During the process of subscription to a Public Cloud, OVHcloud provides the Public Cloud customer with the ability to specify the locations (location/country) of the data processing and storage.	Inspected the process of subscribing to a Public Cloud, to determine whether the Public Cloud customer is able to specify the locations (location/country) of the data processing and storage according to the contractually available options.	No exceptions noted.
CUS-14	OVHcloud provides Public Cloud customers with mechanisms to control and monitor the capacity and allocation of resources using dedicated tools in order to ensure sufficient performance and efficient use of resources.	Inspected OVHcloud's tools provided to the customers to monitor and control capacity and resource allocation, to determine whether OVHcloud provides Public Cloud customers with mechanisms to control and monitor the capacity and allocation of resources using dedicated tools in order to ensure sufficient performance and efficient use of resources.	No exceptions noted.
CUS-15	During the process of subscribing to a Public Cloud, customers must accept the general terms of service and the specific terms of the Public Cloud offer. The general and specific terms of service describe the service, security and contractual commitments and requirements.	Inspected the general terms of service and the process of granting customer access to OVHcloud services as well as documents related to the process of granting customer access to OVHcloud services, to determine whether during the process of subscribing to a Public Cloud, customers must accept the general terms of service and the specific terms of the Public Cloud offer. The general and specific terms of service describe the service, security and contractual commitments and requirements.	No exceptions noted.

SECTION V Other Information Provided by Management of OVH Groupe S.A.

The information in Section V is presented by OVH Groupe S.A. to provide additional information to its user entities and is not part of OVH Groupe S.A.'s description of its system and controls included in Section III. This information has not been subjected to the procedures applied in the examination of the description of the Company's System and suitability of design and operating effectiveness of controls to achieve the Company's service commitments and system requirements based on the applicable trust services criteria, CCM and C5, and accordingly, KPMG SA expresses no opinion on it.

Management's response to exceptions noted

The table below contains Management's response to the exceptions identified in section IV Management's Description of its Relevant Criteria and Related Controls, and Independent Service Auditors' Description of Tests of Controls and Results above.

Control ID	Control Description	Exception Noted	Management Response
PHY-03	A security level classification system is used to define zones for access security.	During the visit of DC Tape Saint-Pierre-des-Corps, KPMG noted that the level of classification of the zones is not displayed as required by the zoning policy defined by OVHcloud for all its datacenters	Management noted that the exception identified relates to the planned implementation of signage within DC Tape Saint-Pierre-des-Corps, which had been scheduled but was set to occur after the auditors' visit. As of January 3rd, 2025, the control was remediated. As part of remediation, the signage has since been properly installed.

Control ID	Control Description	Exception Noted	Management Response
PHY-11	Detection measures and alerts that are communicated to personnel are implemented to identify anomalies that could result from environmental threat events.	During the visit to LIM datacenter, KPMG noted that flood detection sensors were not installed in front of all server racks due to ongoing expansion work. A test was performed at two locations by applying a wet cloth to the aluminum strips meant to detect water, but no alert was triggered, indicating that the flood detection system was not functioning as expected in those areas.	Management noted that the exception identified was due to a malfunction of environmental monitoring probes in a limited number of rooms within the LIM datacenter. As of May 15th, 2025, the control was remediated. As part of remediation, all probes within the LIM datacenter have been tested and replaced if malfunctioning. All probes are now up and running in the monitoring tools.

Control ID	Control Description	Exception Noted	Management Response
PHY-12	Environmental protections have been installed including the following: • Cooling systems, • Air conditioning units, • Redundant communications lines, • Fire extinguishers, • Smoke detectors, • Redundant electric arrival, • UPS, Diesel generator.	During the visit of LIM datacenter, KPMG noted that some manual CO_2 fire extinguishers did not have valid inspection stickers. Additionally, none of the locks securing access to the diesel generators were locked at the time of inspection.	Management noted that the exception identified relates to certain manual CO_2 fire extinguishers that did not display valid inspection stickers at the time of the auditors' walkthrough. As of May 15th, 2025, the control was remediated. As part of remediation, the process related to inspection stickers was reviewed and improved in order to ensure that all manual extinguishers are properly inspected. Regarding the locks that were not locked, reminders have been sent to the concerned datacenter team members.

Control ID	Control Description	Exception Noted	Management Response
		During the visit of the DC Tape Saint-Pierre-des-Corps, KPMG noted that there is no Diesel Generator. During the visit of the DC Tape Croix, KPMG noted the absence of a Diesel Generator and redundant electric arrival.	Management noted that the exception identified relates to the absence of a diesel generator within the DC Tape Croix and DC Tape Saint-Pierre-des-Corps . Additionally, the DC Tape Croix lacks redundant electric arrival. However, batteries are in place to compensate for the loss of power for at least 3 hours. **Management's Evaluation of the Exception:** As stated in section 3, chapter 6. "Changes to the System", compensatory measures are in place to ensure customer data security: • Availability: data is replicated between the 4 DC Tapes to ensure redundancy. • Integrity: with an Erasure Coding system that distributes data between DC Tapes and rebuilds it losslessly with checksum verification throughout the lifecycle, even in the event of a datacenter or tape failure/loss. • Confidentiality: ensured by strong encryption for data in transit and at rest. These compensatory measures were implemented based on a risk analysis performed by OVHcloud, taking into account the following scenarios related to the loss or destruction of data in the DC Tapes.

Control ID	Control Description	Exception Noted	Management Response
PHY-23	Measures have been implemented by OVHcloud to prevent the failure of cooling and power supplies, including: • Appropriate redundancy of power arrivals; • Appropriate redundancy of cooling and air conditioning systems; • Use of alternative power supplies such as UPS and generators; • Regular maintenance of the equipment in accordance with the manufacturer's recommendations.	During the visit of the DC Tape Croix, KPMG noted the absence of a Diesel Generator and redundant electric arrival.	Management noted that the exception identified relates to the absence of redundant electric arrival within the DC Tape Croix. However, batteries are in place to compensate for the loss of power for at least 3 hours. **Management's Evaluation of the Exception:** As stated in section 3, chapter 6. "Changes to the System", compensatory measures are in place to ensure customer data security: • Availability: data is replicated between the 4 DC Tapes to ensure redundancy. • Integrity: with an Erasure Coding system that distributes data between DC Tapes and rebuilds it losslessly with checksum verification throughout the lifecycle, even in the event of a datacenter or tape failure/loss. • Confidentiality: ensured by strong encryption for data in transit and at rest. These compensatory measures were implemented based on a risk analysis performed by OVHcloud, considering the following scenarios related to the loss or destruction of data in the DC Tapes.

OVHcloud

OVHcloud

System and Organization Controls (SOC 3) Report

On Security, Availability, Confidentiality and Privacy

Covering the Public Cloud System of OVHcloud

For the Period January 1, 2024 to December 31, 2024

Table of content

-Intentionally left blank-

SECTION I
Independent Service Auditor's Report

KPMG

KPMG S.A.
Tour EQHO
2 Avenue Gambetta
CS 60055
92066 Paris La Défense Cedex

To the Board of Directors of

OVH Groupe S.A., Roubaix, France

-hereinafter also referred to as “OVHcloud“ or “the Company“-

Scope

We have examined management of OVH Groupe S.A.’s accompanying assertion titled "Management of OVHcloud’s Assertion" (the Assertion) that the controls within OVH Groupe S.A.'s Public Cloud system (the System) were suitably designed and operating effectively throughout the period January 1, 2024 to December 31, 2024to provide reasonable assurance that OVH Groupe S.A.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality and Privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Management of OVH Groupe S.A.’s Attachment 3 - OVHcloud*’s Complementary User Entity Controls (Attachment 3)* indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at OVH Groupe S.A., to achieve OVH Groupe S.A.’s service commitments and system requirements based on the applicable trust services criteria. Management of OVH Groupe S.A.’s Attachment 3 presents the complementary user entity controls assumed in the design of OVH Groupe S.A.’s System. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

OVH Groupe S.A. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the System to provide reasonable assurance that OVH Groupe S.A.’s service commitments and system requirements were achieved. Management of OVH Groupe S.A. has provided the accompanying Assertion about the suitability of the design and operating effectiveness of controls within the System. OVH Groupe S.A. is also responsible for preparing the Assertion, including the completeness, accuracy, and method of presentation of the Assertion; providing the services covered by the Assertion; selecting, and identifying in the Assertion, the applicable trust services criteria; identifying the risks that threaten the achievement of OVH Groupe S.A.’s service commitments and system requirements; and having a reasonable basis for the Assertion by performing an assessment of the suitability of the design and operating effectiveness of the controls within the System.

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on the Assertion that controls within the System were suitably designed and operating effectively throughout the period to provide reasonable assurance that OVH Groupe S.A.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and in accordance with International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether the Assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- obtaining an understanding of the System and OVH Groupe S.A.'s service commitments and system requirements
- assessing the risks that controls were not suitably designed or did not operate effectively to achieve OVH Groupe S.A.'s service commitments and system requirements based on the applicable trust services criteria
- performing procedures to obtain evidence about whether controls within the System were suitably designed to provide reasonable assurance that OVH Groupe S.A. would achieve its service commitments and system requirements based on the applicable trust services criteria if those controls operated effectively
- testing the operating effectiveness of controls within the System to provide reasonable assurance that OVH Groupe S.A. achieved its service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with the relevant ethical requirements in the United States of America relating to the examination engagement. We have complied with those requirements. We have also applied the statements on quality control standards established by the American Institute of Certified Public Accountants and accordingly maintain a comprehensive system of quality control. The firm also applies International Standard on Quality Management 1 which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, the Assertion that the controls within OVH Groupe S.A.'s System were suitably designed and operating effectively throughout the period January 1, 2024, to December 31, 2024, to provide reasonable assurance that OVH Groupe S.A.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Paris,

September 10, 2025

KPMG S.A.

DocuSigned by:
Jacques Pierre
D7BAF5238B3D401...

Jacques Pierre
Partner, Audit

DocuSigned by:
Fayçal El BELGHAMI
59CA3F59EF5440C...

Fayçal El Belghami
Partner, IT

SECTION II Management of OVHcloud's Assertion

Management of OVH Groupe S.A.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within OVH Groupe S.A.'s Public Cloud system (the System) throughout the period January 1, 2024 to December 31, 2024 to provide reasonable assurance that OVH Groupe S.A.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality and Privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*. Our description of the boundaries of the System is presented in our Attachment 1 - *OVH Groupe S.A.'s Overview of Services and the System (Attachment 1)* and identifies the aspects of the System covered by the Assertion.

Our Attachment 3 - OVH Groupe S.A.*'s Complementary User Entity Controls (Attachment 3)* indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at OVH Groupe S.A., to achieve OVH Groupe S.A.'s service commitments and system requirements based on the applicable trust services criteria. Our Attachment 3 presents the complementary user entity controls assumed in the design of OVH Groupe S.A.'s System.

We have performed an evaluation of the suitability of the design and operating effectiveness of the controls within the System throughout the period January 1, 2024 to December 31, 2024 to provide reasonable assurance that OVH Groupe S.A.'s service commitments and system requirements were achieved based on the applicable trust services criteria. OVH Groupe S.A.'s objectives for the System in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in our Attachment 2 - *OVH Groupe S.A.'s Principal Service Commitments and System Requirements (Attachment 2)*.

We assert that the controls within the System were suitably designed and operating effectively throughout the period January 1, 2024 to December 31, 2024 to provide reasonable assurance that OVH Groupe S.A.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

OVH Groupe S.A

Mathieu Delobelle

Chief Information Officer

Signé par :
Mathieu Delobelle
FA645F25290F435...

September 10, 2025

SECTION III
Attachments

Attachment 1 - OVH Groupe S.A.'s Overview of Services and the System

1. Company Overview and Services Provided

OVH Groupe S.A ("OVHcloud") was founded in 1999 as an internet hosting company in France. Over the last 20 years, OVHcloud has developed its infrastructure and expanded its presence in Europe, North America and Asia, diversifying its cloud offerings and expanding its activities globally.

OVHcloud is a cloud provider supported by a vertically integrated production model that provides enterprises with a comprehensive suite of solutions for multi-cloud and hybrid cloud strategies distributed into four core cloud categories:

- **Bare Metal Cloud:** with dedicated physical servers to customers;
- **Hosted Private Cloud:** in a fully dedicated environment to its business customers;
- **Public Cloud:** based on open-source technologies such as OpenStack and Kubernetes;
- **Web Cloud:** with website hosting and domain registration, telecommunications, and internet access.

1.1. A Vertically Integrated Model, Based on Exclusive Technology

1.1.1.A Server and Data Center Integrated Model

OVHcloud has developed an integrated model to fully manage in-house each step of both server and data center lifecycles limiting the dependency on subservice organizations.

OVHcloud's vertically integrated supply chain includes server manufacturing, data center operations, network provisioning and IT infrastructure management. By designing and assembling all its servers in-house, OVHcloud fully owns server design, production and management. OVHcloud has built its strong vertical integration through proprietary technology and in-house operations in various geographies.

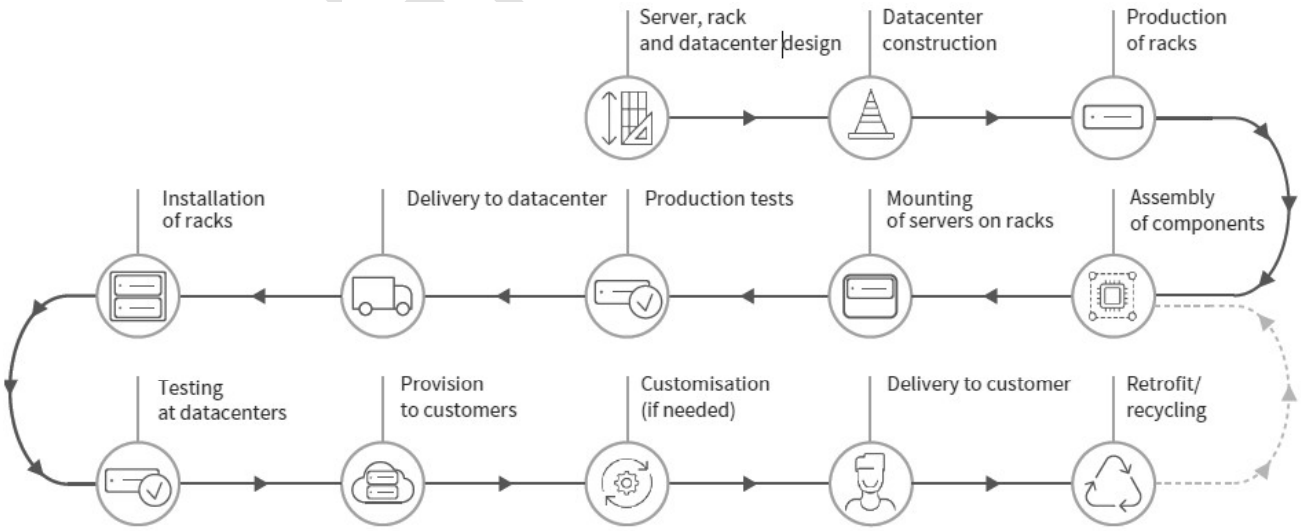


Figure 1: Integrated model for server and data center lifecycle

OVHcloud has two dedicated production sites—in France and in Canada—for assembling different
hardware components into servers. Once the various components have been assembled, they

are
transported to the data center and customized as necessary prior to delivery to the customer.

OVHcloud reduces the risk of supply chain disruption by manufacturing its servers in-house and removing dependencies on a third-party manufacturer.

The capacity to manufacture servers proved to be essential in allowing OVHcloud to respond rapidly to restore service in case of incidents.

1.1.2.A Data Center Proprietary Water-Cooling Technology

OVHcloud has developed and used over 20 years a proprietary water-cooling technology within its data centers. OVHcloud's water cooling technology combines water-cooled servers with air-cooled data centers, thereby removing the need for air conditioning. It uses direct water cooling to remove the heat from CPUs, and air—which is then cooled inside the rack using water through a heat exchanger—to remove the heat from other components. The heated water is then cooled using dry cooling towers. In addition to being highly energy and water efficient, OVHcloud's water cooling technology also has relatively low maintenance costs.

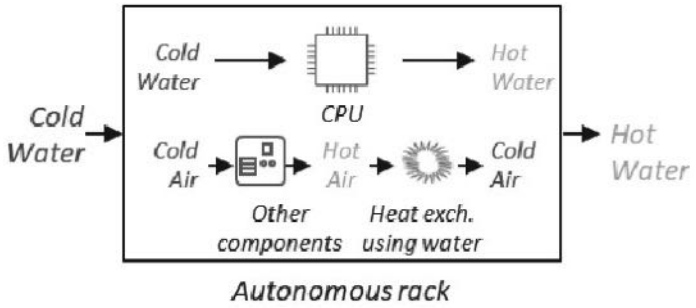


Figure 2: OVHcloud proprietary water-cooling technology principles

In addition, OVHcloud developed its own concept where air-conditioning units were replaced by a natural ventilation system that, thanks to hot and cold airflow, ensured that temperatures were regulated. This concept complemented water-cooling to participate in energy saving.

1.2. OVHcloud Universe of Cloud Offerings

Cloud computing means providing users with storage, computing and network resources, over the internet, on demand. Cloud resources are in data centers that house servers and equipment used to process, store and transmit data. User entities of cloud computing services can access stored data and instruct processing units to perform computing functions automatically, without the need for human interaction, minimizing the computing and storage capacities needed on their devices (such as personal computers, tablets and mobile phones). Wherever they are located, so long as they have an internet connection, user entities can access IT services through the cloud.

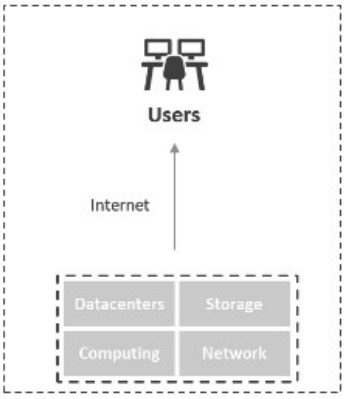


Figure 3: Basic structure of a cloud computing system

Servers maintained in data centers can be used for multiple functions, each of which is accessed through a "virtual machine" created on the server. The virtual machines are operated and separated from one another through a software platform known as a "virtualization stack." Each virtual machine can have its own operating system that permits user entities to develop and run applications. Through a function known as a "hypervisor," the server's capacity is allocated to the virtual machines in accordance with the demands of user entities. More recently, software applications have been written to be bundled in "containers" that run directly on the operating system of the server itself, coordinated through platforms known as "orchestration" systems, which generally take less space and can provide better performance than hypervisor-based virtualization stacks.

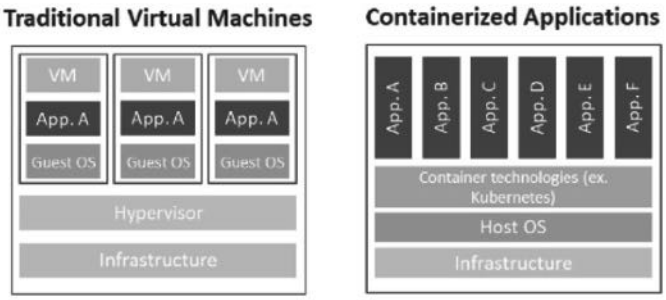


Figure 4: Traditional virtual machine structure and containerized application structure

The ability to create multiple virtual machines on each server or to deploy container-based systems allows a cloud service organization to allocate its capacity among multiple user groups or user entities in a secure manner. Service organizations can dedicate a server to a single user entity (a "private cloud" system), allocating the server's capacity among user groups authorized by the user entity. Alternatively, a server can be shared among multiple user entities (a "public cloud" system). Private cloud user entities generally pay monthly charges for dedicated capacity, whether or not they use that capacity. Public cloud user entities generally pay for the capacity they use.

To optimize the cost of cloud services, many businesses are deploying "hybrid cloud" strategies, in which they combine on-premises or outsourced private cloud capacity for their most sensitive functions and data, with public cloud capacity for their less sensitive needs. User entities are also deploying "multi-cloud" strategies, purchasing cloud services from several user organizations.

The following table summarizes the key features of OVHcloud's main private cloud and public cloud offerings:

	Private Cloud		Public Cloud	
	Bare Metal Cloud	Hosted Private Cloud	Virtual Private Servers	Shared Public Cloud
Hardware	Dedicated to user entity		Shared	
Operating system	Selected and managed by user entity	Selected and managed by OVHcloud		
Virtualization Stack	Selected and managed by client (if any)	VMware Hosted and managed by OVHcloud		Hosted and managed by OVHcloud via OpenStack

Cloud computing encompasses a range of services that include providing access to infrastructure
(Infrastructure as a Service or “IaaS”), selecting and operating platforms such as operating systems,
virtualization stacks and security systems (Platform as a Service or “PaaS”), and offering applications
that are developed and can function on cloud platforms (Software as a Service or “SaaS”).

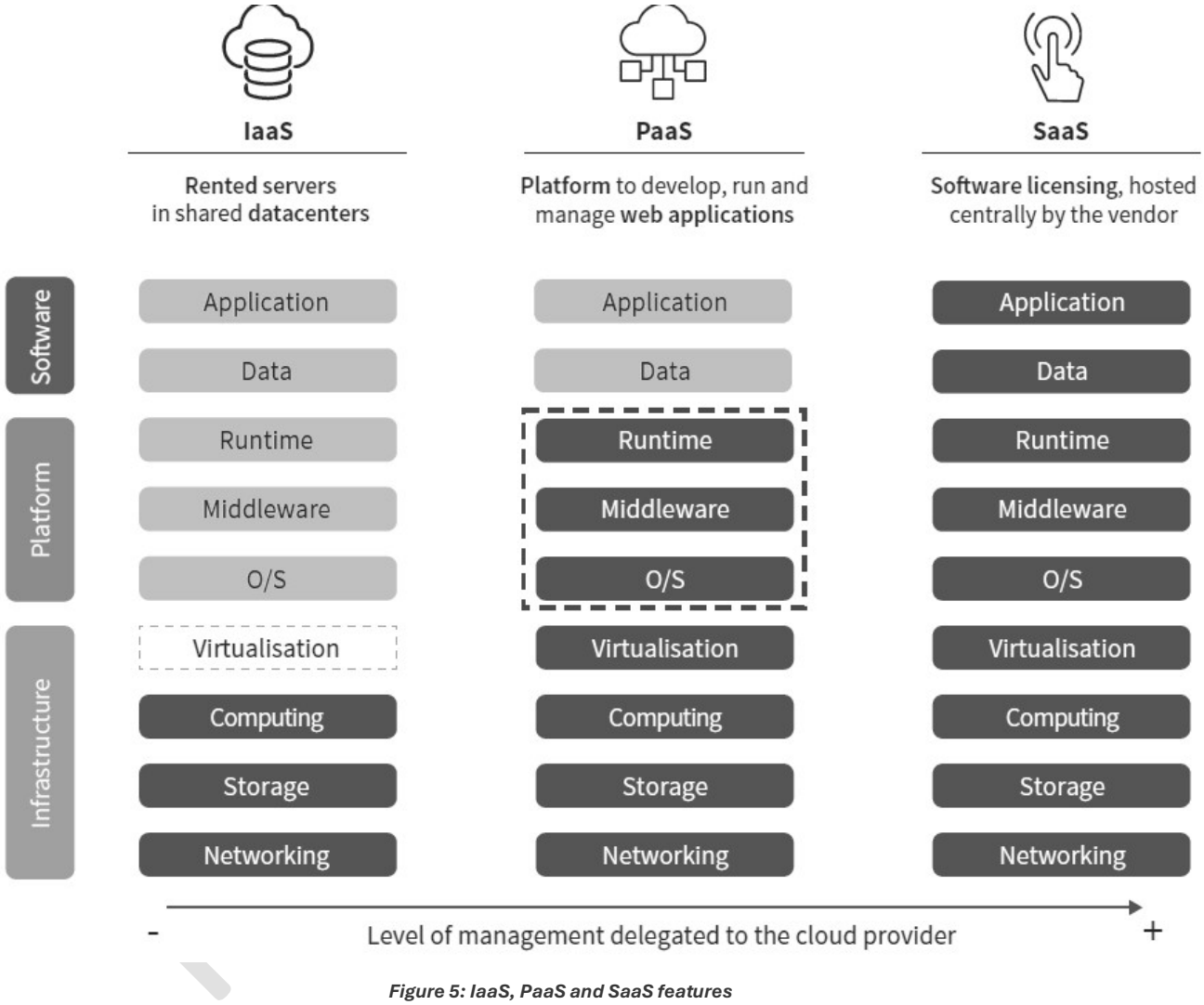


Figure 5: IaaS, PaaS and SaaS features

The cloud solutions market also includes the web cloud market largely consists of web and domain hosting, including renting servers for websites, selling secondary services (such as software packages) and domain name registration, renewal and transfer services.

1.2.1. Bare Metal Cloud

OVHcloud’s Bare Metal Cloud service provides dedicated physical servers to user entities, which have full control over the server, including the choice of operating system, which allows them to have an experience similar to what they would have with on-premises solutions managed by their internal IT staff, while taking advantage of the benefits offered by outsourcing.

Bare Metal Cloud offers high performance and high scalability with the best price/quality ratio in just a few minutes, for development, production and backup. Highly reliable, customizable and scalable, Bare Metal Cloud provides user entities with instant provisioning and fully automated access to dedicated servers on which the user entity operates and manages all software layers, including the operating system.

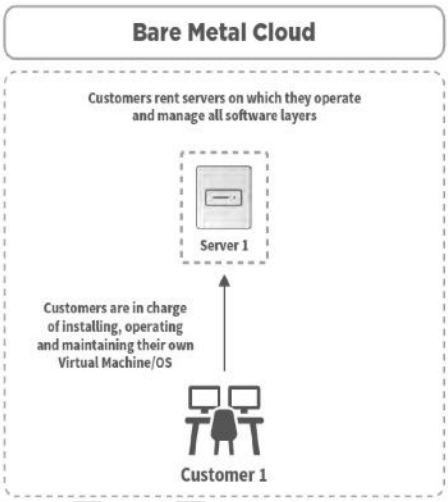


Figure 6: Bare Metal Cloud service

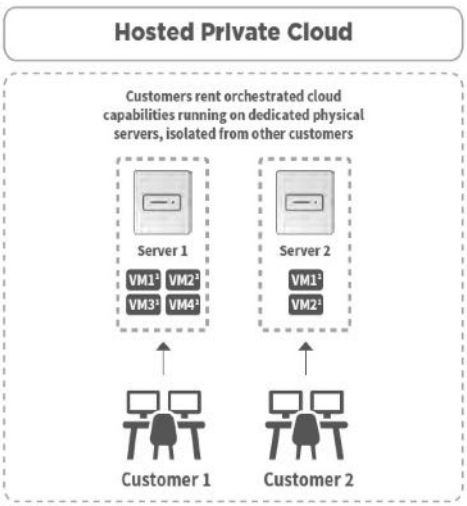
Bare Metal cloud services provide user entities with high-level computing power and strict Service Level Agreements, in a secure environment appropriate for data-sensitive applications. The server can be customized to meet user entity requirements and can be operated without a need to allocate the server's capacity to virtual machines through a hypervisor, which allows the customer to use the server's full capacity. Any unused capacity can be deployed within minutes, although the total capacity is limited by that of the dedicated server. Bare Metal user entities are typically responsible for making their own data backup arrangements, although they can also choose from several backup options offered by OVHcloud (with backed-up data stored within the same data center or at a different location). Bare Metal cloud user entities may choose various additional service options such as specific performance levels, server customization or data backup.

Bare Metal Cloud services provide security, performance, customization and cost effectiveness, and are typically used for data intensive operations such as media encoding (like 3D animation), media streaming, complex data-computing (such as analyzing oil and gas field seismic data), low latency operations such as high frequency trading, media streaming, online gaming and online advertising, critical corporate applications requiring high-security operations such as ERP and CRM system operations, specialized applications such as customized Internet-of-Things, and applications designed to meet strict regulatory compliance requirements in highly regulated sectors.

1.2.2.Hosted Private Cloud

OVHcloud offers hosted private cloud services in a fully dedicated environment providing dedicated servers and platforms fully managed by OVHcloud, including the operating system and the virtualization stack (using VMware technology).

OVHcloud's hosted private cloud services provide user entities with private access to servers that can be customized to meet the user entities' specific requirements. The server provides high performance, although slightly below that of high-end Bare Metal cloud service, because the hypervisor uses some of the server's capacity. It meets the needs of user entities seeking isolation and security, scalable resources (within the limits of the server's capacity) and resilience.



1. VM: Virtual Machine

Figure 7: Hosted Private Cloud service

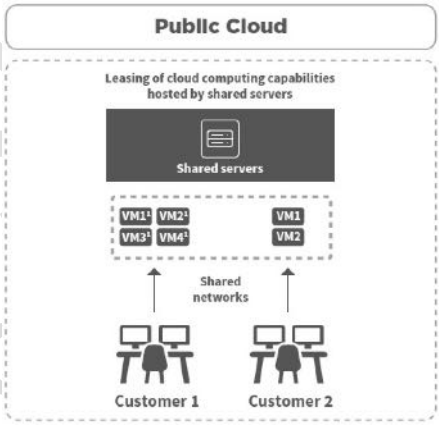
The main usages for hosted private cloud services include deployment in hybrid cloud strategies, media encoding, big data analytics and disaster recovery, as well as the storage and processing of sensitive data in key sectors such as healthcare, finance and the public sector.

1.2.3.Public Cloud

OVHcloud offers public cloud solutions based on open-source technologies such as OpenStack (a platform that controls diverse, multi-vendor pools of processing, storage, and networking resources) and Kubernetes (an industry standard container orchestration platform). The use of these standard platforms provides user entities with easy data transfer capability and access to source code, facilitating reversibility and eliminating "vendor lock-in". It is particularly adapted for user entities seeking to deploy hybrid cloud strategies.

Public cloud solutions provide users with virtually unlimited computing capacity, with the only constraint being the demands of other users and the total installed capacity of the cloud provider.

Capacity can generally be accessed automatically in seconds. Because public cloud service is based on shared servers offering user entities the highest degree of scalability and continuity, customization options are limited. OVHcloud provides high SLAs given the flexibility of the hardware architecture.



1. VM: Virtual Machine

Figure 8: Public Cloud service

Public cloud offering provides three core cloud computing services: computer performance, storage and network capabilities. It also provides five additional, high-level services: orchestration and containerization, including tools to manage processes and software stacks; data analytics, including data collection and processing services; artificial intelligence, including automated deployment, launch, training and evaluation of machine learning models; management interfaces; and project management solutions. User entities of OVHcloud public cloud solutions can choose a virtual private server option, providing computing capabilities located on shared servers, but with "virtual machines" isolated using virtual private networks.

The virtual private server option is particularly adapted for user entities seeking tailored resources, particularly for short-duration operations with volatile workloads and server demand across multiple access locations, and a high degree of resilience. Virtual private server solutions are used primarily for applications testing and other one-time projects, the management of short-duration peak loads and backup functions. OVHcloud also offers fully scalable public cloud services on virtual machines that are housed on share servers but are not isolated through virtual private networks.
This service is used for applications with high demand bursts (such as e-commerce websites) and services that use large volumes of data, such as video and music streaming. Public cloud services can also be used by user entities for workloads that are not sufficiently mission-critical to warrant the use of private cloud resources.

1.2.4.Platform-as-a-Service Solutions

OVHcloud provides PaaS offers on its private cloud and public cloud IaaS products, primarily in the following areas:

- **Artificial Intelligence and Analytics**: Artificial intelligence and analytics solutions include tools and services supporting data analysis and data presentation, such as the management of end user queries, data labelling, and image and text presentation. OVHcloud is active in providing high performance computing solutions for artificial intelligence and machine learning and intends to pursue its development in this area.
- **Data Management Software**: Data management software allows users such as database managers and developers to manage databases to allow for queries and random updates, and it represents the largest single segment of the PaaS market. It includes programs that execute queries on data and provide visual representation of the data in formats such as spreadsheets, enabling users to build applications faster and automate database management.
- **Application Platforms**: Application platforms are back-end server software solutions providing developers with a cohesive application execution environment (e.g. application execution, access to data, authentication coordination, session management). OVHcloud integrates key application platforms from VMWare.
- **Web cloud Platforms**: beyond its web cloud offer, OVHcloud provides an end-to-end web platform allowing developers to build, run and scale applications.
- **High Performance Storage**: including Block Storage, Object Storage and Cold Archive.
- **Security and Encryption**: including identity access management and encryption solutions, including end-to-end encryption.

1.2.5.Web Cloud

OVHcloud has offered web cloud services since its founding in 1999. OVHcloud provides user entities with web cloud services, including website hosting and domain registration, telecommunications and internet access, as well as a "marketplace" for third-party software solutions to help user entities empowering their digital journey.

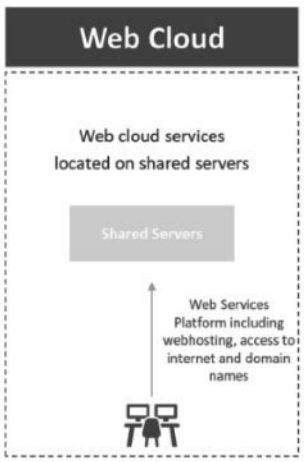


Figure 9: Web Cloud service

OVHcloud offers three principal solutions to web cloud user entities:

- **Web hosting and domain registration**: This includes the rental of capacity on web servers, allowing user entities to connect their websites to the internet, as well as domain name registration, renewal and transfers together with email addresses and storage options. OVHcloud offers web hosting customers additional services, such as Secure Socket Layer (SSL) certificates, which allow secure connections from a web server to a browser.
- **Telephony and Network**: User entities may purchase Voice over IP systems providing phone numbers and unlimited calls to fixed lines (and, in the high-end package, mobile lines), and enabling usages such as telephone switchboards and interactive voice response systems. OVHcloud also provides large-volume telephony options that are capable of handling video and other media. OVHcloud also offers customers internet access through ADSL and fiber networks, with basic and professional packages.
- **Software Marketplace**: Web cloud user entities have access to OVHcloud's software marketplace, providing more than 250 fully digital SaaS and PaaS solutions with 6 categories from third-party vendors that can run on OVH's infrastructure, in areas such as collaboration, emailing and social networking, managed services (such as outsourcing), corporate tools (business intelligence, CRM and ERP), coding and applications development, and solutions for specific industries such as e-learning, healthcare, legal and real estate.

1.3. Public Cloud's Scope Covered in this Report

Our service "Public Cloud Infrastructure" provides a wide variety of cloud services integrated with each other, forming a coherent offer of infrastructure as a service. The core of the service is built with Openstack and consists in compute, block storage and object storage. Specifically, it provides the following services and features:

- Public Cloud **Compute** is a platform that uses pooled virtual resources to build and manage public clouds. The tools that comprise the PCI platform, called "projects," handle the core cloud-computing services of computer, networking, storage, identity, and image services. PCI Compute service provides three kind of instances that aim at different goals:
  - balanced instances: Catalogue of top-range instances, with fully guaranteed resources. General Purpose instances have a balanced distribution of resources and suit most uses. CPU instances are particularly powerful in terms of computing capacity. As for RAM instances, they offer a very high volume of memory.
  - IOPS instances: IOPS instances deliver the fastest disk transactions in the Public Cloud range. They offer direct access to NVMe drives, each of which deliver at

least 400,000 read/write operations per second. These cloud solutions are designed to host database (DB) servers and big data applications.
    - GPU instances: GPU instances integrate NVIDIA Tesla V100S graphic processors to meet the requirements of massively parallel processing. These cloud servers are adapted to the needs of machine learning and deep learning.
- **Object Storage** (Swift / OpenIO) offers a high-performance, scalable and secure storage space. It allows the user to upload static files (videos, images, web files) to an unlimited space and use them from an application or make them accessible on the web via a S3 API. This storage space can be scaled up as the project grows, with no need to plan for it in advance. It can meet the requirements of big data, artificial intelligence (AI) and document catalogues, or simply help to get the most out of csutomers' data. Object Storage also includes **Cold Archive** service, which provides long-term, cost-efficient storage. Data is stored on an S3 buffer before being sent to magnetic tapes in smaller scale datacenters, dedicated to this service.
- **Block storage** Ceph-as-a-Service (CaaS) is a framework that can deploy and maintain Ceph based clusters. Ceph is a unified, distributed storage system designed for excellent performance, reliability and scalability and Ceph-as-a-Service is a system for complete life-cycle management of Ceph clusters. When persistent storage requirements increase, the user instantly meets growing demands by hot-adding extra disks to increase the instance's capacity. These volumes are securely hosted in OVH's clusters and can be used to meet the requirements of applications that handle large volumes of data.

The billing is based on the volume and typology of services consumed; a key component is pay-as-you-go, meaning that only resources consumed are billed, and hourly billing is available. See https://www.ovhcloud.com/fr/public-cloud/prices/ for details. Entry-level offers are affordable; therefore Public Cloud clients range from small entreprise to large accounts.

We also provide Platform-as-a-Service (PaaS) products that are built on top of Public Cloud Infrastructure products. These products are hosted on Public cloud instances and are preconfigured to provide specific services

Kubernetes products include two individual products:

- **Managed Kubernetes** (K8s) which is the industry-standard container orchestrator, used by companies of all sizes. It facilitates the deployment, resiliency and scalability of the customer's applications, even in hybrid or multi-cloud infrastructures. The "Managed Kubernetes" solution is powered by OVH's Public Cloud instances. OVH deploys, hosts and maintains all the components needed for Kubernetes to work, including updates linked to bugs and security patches. OVH also maintains the necessary components on the customer's nodes. Kubernetes launches containers and configures the Load Balancer for the customers, and they can instantly add new computing nodes. The customers can also define the health conditions for each service, after which Kubernetes will relaunch any pods and containers that do not meet these criteria. The customers' nodes can be monitored, and their services benefit from the high availability of OVH Infrastructure-as-a-Service (IaaS) solutions.
- **Private registry**, which enables customers to host helm charts and docker images. The ISMS covers the full set of these products / services.

Data products include two individual products:

- **Cloud Databases**: offers a fully managed database service. The customer is billed hourly according to the resources he ordered.
- **AI Products**: provide a fast and easy way to get through a Artificial Intelligence pipeline. This offer is split into three products AI Notebook, AI Training and AI Deploy. The computer engine is based on Kubernetes. The customer is billed by the minute and only for what resources he consumes. AI Products enables clients to leverage GPU hardware simply and without compatibility headaches.

Several services and features are included in the Openstack framework and thus available in all Public Cloud projects by default.

- Identity service (Keystone)
- Managed private registry and public catalog
- WebUI service
- Network connectivity (Neutron)
- Metering service (Ceilometer)
- Roles and Rights Management
- Workflow management (Mistral)

Public Cloud scope	Product name	ovhcloud.com page	Commercial offers
Public cloud Compute	Public Cloud Instance	https://www.ovhcloud.com/fr/public-cloud/compute/ https://www.ovhcloud.com/fr/public-cloud/metal-instances/	Instances: Guaranteed resources, GPU, IOPS, discovery VPS: Starter, value, comfort, essential, elite Metal Instances
Object Storage	Object Storage	https://www.ovhcloud.com/fr/public-cloud/object-storage/	Object storage, high performance object storage, cloud archive
	Cold Storage	https://www.ovhcloud.com/fr/public-cloud/cold-archive/	Cold Archive
Block Storage	Block Storage	Dedicated : https://www.ovh.com/fr/cloud-disk-array/ Public: https://www.ovhcloud.com/fr/public-cloud/block-storage/	Cloud disk Array, Block Storage

Kubernetes	Managed Orchestration	https://www.ovhcloud.com/fr/public-cloud/kubernetes/ https://www.ovhcloud.com/en/public-cloud/managed-rancher-service/	Managed Kubernetes Service, Managed Rancher Service
	Managed OCI artifact Registry	https://www.ovhcloud.com/fr/public-cloud/managed-private-registry/	Managed Private Registry
Data / Cloud Databases	Managed Search Engine Software Platform	https://www.ovhcloud.com/fr/public-cloud/opensearch/	Managed Opensearch
	Managed Timeseries	https://www.ovhcloud.com/fr/public-cloud/m3db/	Managed M3DB
	Managed In-Memory Database	https://www.ovhcloud.com/fr/public-cloud/redis/	Managed Redis
	Managed Document Database	https://www.ovhcloud.com/fr/public-cloud/mongodb/	Managed MongoDB
	Managed Relational Database	https://www.ovhcloud.com/fr/public-cloud/mysql/ https://www.ovhcloud.com/fr/public-cloud/postgresql/	Managed MySQL, Managed PostGreSQL
	Managed Column-Oriented Database	https://www.ovhcloud.com/fr/public-cloud/apache-cassandra/	Managed Cassandra
	Managed Message Broker	https://www.ovhcloud.com/fr/public-cloud/apache-kafka/	Managed Kafka
	Managed Data Visualisation	https://www.ovhcloud.com/fr/public-cloud/grafana/	Managed Grafana
Data / AI Products	Managed Containers	https://www.ovhcloud.com/fr/public-cloud/ai-deploy/	AI Deploy, AI Training

		https://www.ovhcloud.com/fr/public-cloud/ai-training/	
	Notebook Interface	https://www.ovhcloud.com/fr/public-cloud/ai-notebooks/	AI Notebooks, Quantum Notebooks

The following business processes are considered to be part of the scope:

- The provision, connectivity, maintenance in operational conditions and decommissioning of the infrastructure allocated to the customer.
  - Provision of the infrastructure allocated to the customer
  - Connectivity of the infrastructure allocated to the customer
  - Maintaining the infrastructure allocated to the customer in operational and security conditions
  - Decommissioning of the infrastructure allocated to the customer at the end of the service
- The means provided to the client for the configuration, use and monitoring of the allocated platform.
  - Configuration of the infrastructure and options by the customer
  - Use and administration of the infrastructure by the customer
  - Monitoring of the infrastructure by the customer

2. Components of the System Used to Provide the Services

Public Cloud Services System is comprised of the following components:

— **Infrastructure:** computer equipment (e.g., servers, network and storage devices) and physical technology upon which the system is hosted.

— **Software:** application programs and system software used to deliver the services.

— **People:** personnel involved in the governance, operation, and use of the system and delivery of services.

— **Procedures:** automated and manual procedures to operate, maintain, and secure the services.

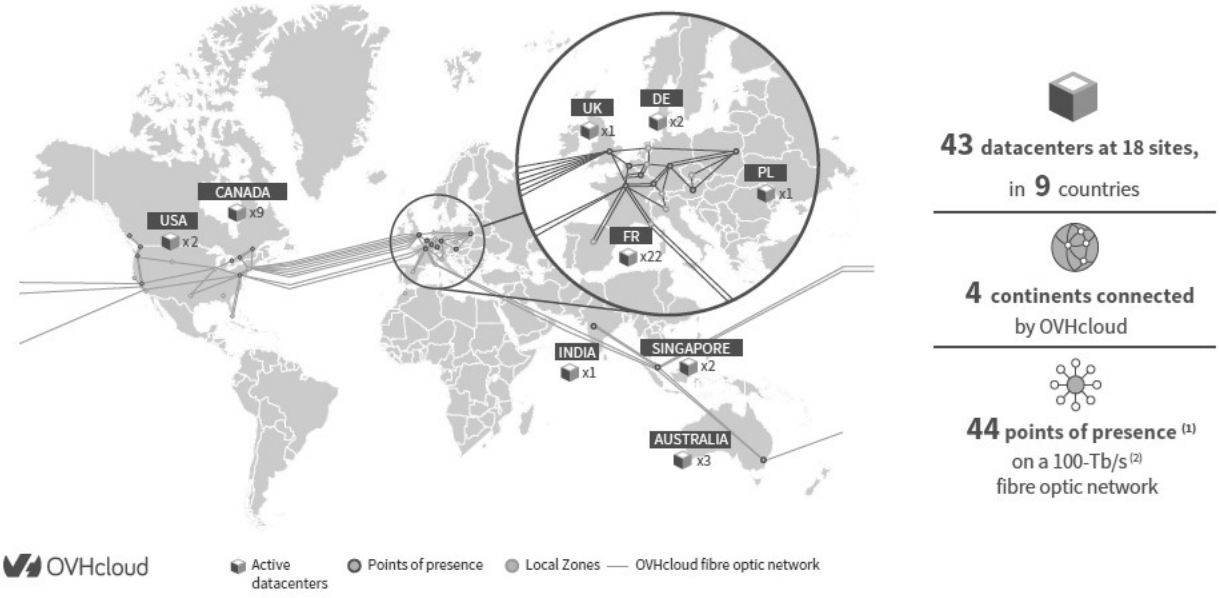
— **Data:** transaction streams, files, databases, tables, and output used or processed by the system.

These components are described in further detail below.

2.1. Infrastructure

OVHcloud has multiple clouds around the world, each operating from a Point of Delivery (POD). A POD is a standardized design of equipment and software that provides the in-scope cloud services. A POD consists of servers, storage and network devices and may vary in size, but the design architecture is similar from site to site.

OVHcloud operates 43 datacenters in 18 locations in Europe, North America, and Asia-Pacific. OVHcloud manufactures its servers in-house and is not dependent on a third-party manufacturer, except for DC tape datacenters and Cold Archive service.



Source: At 31 August 2024, Company.

(1) A point of presence is a point at which the network establishes a connection with the internet.

(2) Tera bits per second.

Figure 10: OVHcloud geographical representation

For Public Cloud products, the following datacenters are used to deliver the service:

Geographical Area	City	Code	Address	Type
France	Roubaix	RBX	2 rue Kellermann 59100 ROUBAIX	OVH DC
	Gravelines	GRA	ZI des Huttes - Route de la ferme Masson 59820 GRAVELINES	OVH DC
	Strasbourg	SBG	9 rue du Bassin de l'Industrie 67000 STRASBOURG	OVH DC
	DC tape Croix	CRX03	155 avenue Georges Hannart 59170 CROIX	OVH DC
	DC tape Bordeaux	VDO01	Bordeaux	Shell & Core
	DC tape Grenoble	EYN01	Grenoble	Shell & Core
	DC tape Saint-Pierre-des-Corps	SDP01	Saint-Pierre-des-Corps	OVH DC
	3-AZ Paris / Marcoussis	MR901	15 rue Marin Angiboust, 91460 Marcoussis	Colocation SOC report managed by suppliers
	3-AZ Paris / Ferrières-en-Brie	IEB01	16 Av. Joseph Froelicher, 77600 Ferrières-en-Brie	Colocation SOC report managed by suppliers
	3-AZ Paris / Clichy	CCH01	7-9 Rue Petit 92582, Clichy	Colocation
Canada	Beauharnois	BHS	50, rue de l'Aluminerie, Beauharnois QC J6N OC2	OVH DC
United Kingdom	Erith	ERI	Viking Way 14, Belvedere Link Industrial Estate - ERITH DA8 1EW	OVH DC

Germany	Limburg	LIM	LIMBURG: Limburger Straße 45, 65555 Limburg-Offheim Germany	OVH DC
Poland	Ozarow	WAW	UL. KAZIMIERZA KAMINSKIEGO 6 – 05-850 OZAROW MAZOWIECKI - POLSKA	OVH DC
Australia	Sydney	SYD1	Data Centre SYDNEY - 639 Gardeners Road, MASCOT NSW 2020	Colocation SOC report managed by suppliers
		SYD2	Next DC 6-8 Giffnock Avenue, Macquarie Park NSW 2113	Colocation SOC report managed by suppliers
India	Mumbai	MUM	Yotta Datacenter Park - Panvel Hiranandani Fortune City. Survey No. 30, MH SH 76, Panvel, Navi Mumbai, Maharashtra 410206, India	Colocation SOC report managed by suppliers
Singapore	Singapore	SGP1	ALTIMAT Data Center Singapore Pte Ltd - 110 Paya Lebar Road - SINGAPORE 409009	Colocation
		SGP2	23 Tai Seng Drive #06-00, Singapore 535224	Colocation

2.2. Software

	System				Application	Monitoring and Auditing
	Management tools	*Virtualization and management tools*	*Server operating systems*	*Backup systems*		
Public Cloud-Compute	Puppet Terraform Deployment-as-a-Service (DaaS) MariaDB RabbitMQ	Openstack Nova Qemu (KVM) Kubernetes Docker	Ubuntu	Swift S3	Octavia (HAProxy)	OVH Logs Data Platform Prometheus / Thanos
Public Cloud-Block Storage	Admin servers Puppet	VMs on OVH Private Cloud (PCC - vSphere)	Multiple admins deployed in geographically independent locations with the same accesses so no failover needed Multiple puppet hosts in geographically independent locations. VM disk on PCC datastores which are redundant by design	Code is hosted on stash.ovh.net, database backups hosted on PCS (Swift)	N/A	Icinga2 Opsgenie OVH Logs Data Platform
Public Cloud-Object Storage	Internally developed orchestrators (Mozg) to manage overall infrastructure puppet prefect	VMs on OVH Private Cloud (PCC - vSphere)	Ubuntu Debian	MySQL dump stored in Swift in another DC VM Managed Backup service provided by PCC	N/A	Icinga2, Opsgenie, OVH Logs Data Platform Prometheus, Grafana, Mimir Tenable, Sonarqube, REVmon

	admin servers					
Data	Ansible MongoDB OpsManager Terraform Aiven (Aiven is a supplier that provides managed services for databases. SOC controls for this provider are covered by its own SOC2 report)	N/A	Ubuntu running Kubernetes clusters and debian	MongoDump for MongoDB sercices block storage disk snapshot etcd is backuped upon each deployment on a given region, backup is sent to PCS swift	Postgresql, MySQL, MongoDB,Redis, OpenSearch, Apache Kafka, apache MirrorMaker 2, Kafka Connect, Grafana, Cassandra, M3DB, M3 Aggregator AI products (models training jobs, VSCode/Jupyter notebooks, Inference APIs deployments) Apache Spark / Jupiyter	Prometheus and Mimir internal offer for metrics LDP for logs Revmon, Jfrog Xray, CVEmon, Tenable for CVE, sentry
Kubernetes	Ansible Terraform	Openstack Docker Kubernetes	Debian	Etcdctl-backup Internal CriticalDB backup management	N/A	Warp10 Mimir OpsGenie LDP Sentry

2.3. People

OVHcloud's mission and core values are carried out by OVHcloud people with respect to integrity, ethical values, management's operating style, delegation of authorities, as well as overall the organization processes set by the Governance.

All personnel are provided with the legally binding Code of Ethics and IT Charter before following onboarding and awareness training. OVHcloud made available an Ethics and Compliance hotline for personnel to anonymously report on possible violations or misconduct. All contracts include non-disclosure requirements and personnel are made aware that any confidentiality breach, violation or misconduct may lead to a disciplinary action which might cause an immediate dismissal. Throughout the hiring process, a staff screening is performed ensuring new hires would fit their role based on knowledge and experience proportionally to the position they would take at OVH-cloud. Staff screening also includes background checks in line with local laws and regulations.

Management distributes roles and responsibilities based on the skillset appropriateness to best combine the skills and experiences of key staff between management, system and software development and maintenance skills. As part of their onboarding, new personnel are trained on OVH-cloud security and control measures that have been defined by management. Regular management and one-to-one meetings are held ensuring continuous feedback and team development in order to support OVHcloud objectives and security measures.

2.3.1. Organizational Structure

The following organization chart illustrates OVHcloud's organizational structure:

- The BU Commerce is responsible for selling OVHcloud solutions to customers, providing them support, animating an ecosystem of offers and partners.
- The BU Product is responsible for developing, automating and operating the cloud infrastructures and platform, relying on industrial standards and based on customer and market feedback.
- The BU Industry is the infrastructure architect and operator of OVHcloud from engineering to server manufacturing, from infrastructure design to data centre management ensuring the level of quality and availability of the infrastructures adapted to the services expected by OVHcloud customers.
- The BU Ops is responsible for coordinating and ensuring that the company's resources are aligned with its objectives by streamlining the organization, providing information systems, automating processes via lean management, and facilitating cooperation between the BUs.
- The BU Corporate consists of the Finance, HR and Legal management functions.

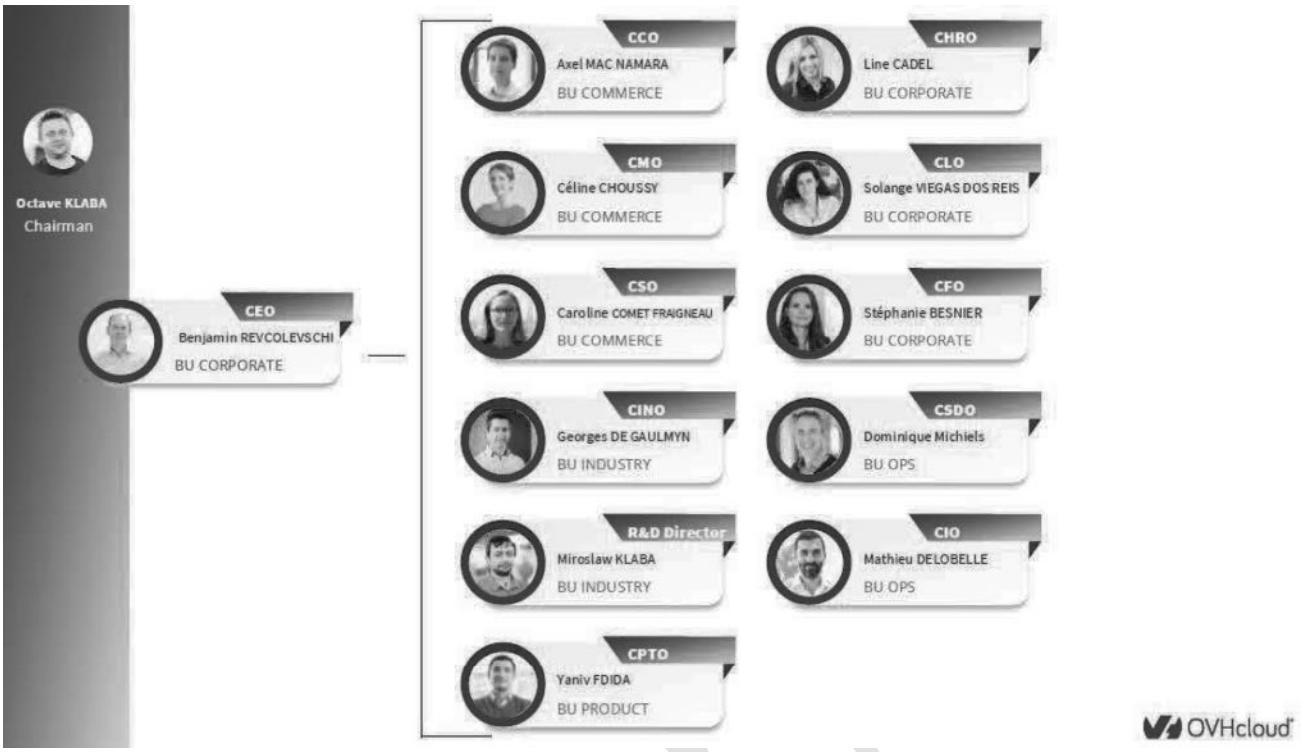


Figure 11: OVHcloud organizational structure

2.3.2. Governance

Governance sets the tone at the top as a foundation of OVHcloud's mission and core values. OVHcloud operates under the management of an Executive Committee committed to the Group's mission to provide customers around the world with secure, trusted, open, sustainable cloud solutions. In addition, the Group is overseen by a Board of Directors composed of independent *administrators*. An overview of the members can be found here: https://corporate.ovhcloud.com/en-ie/company/governance/.

OVHcloud corporate governance has established, maintains and monitors standards for integrity, ethical values, management's operating style, delegation of authorities, as well as overall organizational processes. For that purpose, OVHcloud governance has distributed appropriate roles and responsibilities within the organization:

- The Chief Information Security Officer (CISO) to oversee the information security program and who is supplemented by a security team responsible for centralizing the global coordination of information security within OVHcloud including:
    - Dedicated Security Managers responsible for determining, implementing, maintaining and monitoring appropriate and relevant state-of-the-art security measures;
    - A Risk Manager who coordinates the management of security risks and the associated action plans;
- The Data Protection Officer to oversee all topics related to privacy;

- A network of Security and Privacy referents within the different BUs responsible for security and privacy topics within their scope; they ensure the link between the security and privacy teams with the Product and IT teams;
- An Ethics and Compliance team to oversee the ethics and compliance topics.

2.4. Procedures

2.4.1. Policies and Procedures

OVHcloud has developed and maintains its Information Systems Security Policy made publicly available on OVHcloud website: https://docs.ovh.com/gb/en/security/issp/. The ISSP provides the security reference framework to which OVHcloud management is committed towards all OVHcloud stakeholders.

Beyond the main policy setting the security concepts and approach, OVHcloud is organized by security themes adapted to OVHcloud organization and operations with dedicated security procedures and controls:

During the year 2023, the 28 security themes were redesigned:

1	Define and maintain security governance (Security governance)
2	Maintain consistent security principles and documentation (Security model)
3	Provide to customer appropriate security features to manage their risks (Customer Security Features)
4	Implement appropriate data protection for any data managed or hosted (Data Protection)
5	Demonstrate compliance with OVHcloud commitments (Security compliance)
6	Promote risk-based decisions (Security risks management)
7	Build, develop and maintain relationship with security ecosystem (Security ecosystem)
8	Protect customer's cloud usage (Security Protection for Customer)
9	Protect OVHcloud technical reputation (External technical reputation)
10	Assess security and implement continuous improvement (Audits and controls)
11	Assets management
12	Ensure alignment of resources with security objectives and develop a security culture (Human resources, Awareness and Training)
13	Identity, Authentication and Access Management
14	Protect end-user information system (End user information system)
15	Supply Chain and Service Provider Management
16	Support IT and product developments (Project management)
17	Manage security in IS evolution (Change management)
18	Secure continuous delivery

19	Use strong Cryptography (Cryptography)
20	Deploy and maintain secure configuration and hardening (Configuration and hardening)
21	Ensure Network security (Network security)
22	Operations and Maintenance in Security Conditions
23	Logging, security monitoring and detection
24	Vulnerability and patch management
25	Security incident management
26	Datacenter security
27	Office security
28	Resilience

In a fast-moving world where change is the only constant, security practices must constantly evolve to remain relevant and adapted to its environment. As a result, OVHcloud security policies, procedures and controls are subject to a constant evolution to maintain state-of-the-art security practices.

2.4.1.1. Automated Procedures

The automated procedures consist of programmatic controls developed and incorporated into the system, as well as network, infrastructure, server and system software support and monitoring tools. The key automated processes and tools include:

- User authentication and access controls
- Scheduled system and infrastructure backup processes
- Automated system monitoring and logging
- Automatic alerting (for security and availability)

2.4.1.2. Manual Procedures

Manual processes (supported by policies, procedures, and guidelines) for operating and maintaining the system, including processes for:

- User administration processes
- Security and vulnerability management processes
- Service desk processes
- Client delivery, onboarding and system configuration processes
- Client decommissioning processes
- Change management processes
- Security Monitoring
- Patch updates and change control processes

- Physical security processes
- Technical configuration baselines
- Incident and problem management processes
- HR procedures, including background checks and performance reviews
- Business Continuity and Disaster Recovery procedures

2.5. Data

The key types of data collected, processed, and stored by the Public Cloud Services System include:

- Server and network configurations
- Custom parameters for client configurations
- Client information specific to access control, including usernames
- Client personal data specific to support and billing
- Logs of all infrastructures, including customers infrastructures

This data is collected, processed and stored to guarantee the provision, connectivity and maintenance in operating condition.

Attachment 2 - Principal Service Commitments and System Requirements

OVHcloud establishes policies and procedures for the Public Cloud Service System to meet its objectives for providing cloud and data services. Those objectives are based on: (i) principal service commitments and requirements made to user entities; (ii) laws and regulations governing the provision of such services; and (iii) other financial, operational, and compliance requirements that OVHcloud has established for these services.

The principal service commitments and system requirements for the Public Cloud Services System include but are not necessarily limited to:

- Security practices within the design, implementation and operation of the Public Cloud Services System are adopted to secure data from unwanted access through access control, technical infrastructure control, encryption, monitoring, and policies and procedures.
- Availability practices within the design, implementation and operation of the Public Cloud Services System are adopted to reduce the likelihood and impact of system inaccessibility through capacity management, backup strategies, and business continuity planning.
- Confidentiality practices within the design, implementation, and operation of the Public Cloud Services System are adopted to identify confidential information classified according to the TLP protocol and apply protection against unauthorized disclosure, through policies and procedures, data classification, security controls, and data destruction.
- Privacy practices within the design, implementation and operation of the Public Cloud Services System are adopted to put in place protection controls to protect Personally Identifiable Information (PII) as a cloud PII processor considering 3 main sources of requirements:
    - Legal, statutory, regulatory and contractual requirements;
    - Risks;
    - Corporate policies.

OVHcloud establishes operational requirements that support the achievement of its security and availability commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in the company's policies and procedures, design documentation, and contracts with customers. Information security and availability policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Storage Services System.

Attachment 3 - OVH Groupe S.A.'s Complementary User Entity Controls

OVHcloud services were designed with the assumption that certain policies, procedures and controls are implemented by its customers in a principle of shared responsibility between OVHcloud and its customers. While OVHcloud achieves the objectives described in Section III, the overall achievement of the control objectives also depends on the policies, procedures and controls implemented by user organizations. As such, user organizations are responsible for the design, implementation and operation of their OVHcloud environment according to the level of service they have chosen. Therefore, user organizations are responsible for evaluating their own internal control to determine whether the identified Complementary User Entity Controls have been appropriately designed and operating effectively, where applicable.

The list of Complementary User Entity Controls presented below does not represent all control considerations required by user organizations as other controls may be required in line with the user organization's characteristics.

	Complementary User Entity Control Considerations	Associated Criteria
	General	
1	User organizations should maintain formal policies that provide guidance for information security within the user organization and the supporting IT environment.	CC1.5, CC5.3
2	User organizations are responsible for identifying and establishing adequate controls in line with responsibilities defined as per the contractual agreement and the Data Protection Agreement signed with OVHcloud.	CC1.1, CC1.3, CC1.5
3	User organizations should assess whether the security control objectives applied by OVHcloud are relevant to the risks associated with the way they use their OVHcloud infrastructure. Therefore, user organizations are responsible for identifying the risk and corresponding controls to be implemented to address those risks when using OVHcloud services, software and implementing OVHcloud operational controls.	CC3.1, CC3.2, CC3.3
	Access	
4	User organizations are responsible for establishing appropriate controls and measures allowing relevant access to the environment provided by OVHcloud.	CC6.1, CC6.2, CC6.3, CC6.4, CC6.5,

		CC6.6, CC6.7
5	User organizations are responsible for using strong authentication methods to their OVHcloud environments such as multi-factor authentication or strong passwords.	CC6.6
6	User organizations are responsible for establishing appropriate access controls over the use of their OVHcloud environments such as security groups, Identity Access Management and/or Access Controls Lists and Segregation of Duties.	CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7
7	User organizations are responsible for reviewing the access rights and logs associated with their OVHcloud accounts.	CC6.1, CC6.3
8	User organizations are responsible for granting and disabling access to their OVHcloud services when necessary.	CC6.3, CC6.5
9	User organizations are responsible for ensuring the supervision, management and control for access to key systems hosted in the OVHcloud environment.	CC6.1, CC6.3, CC7.2
10	User organizations must ensure that their workstations and mobile equipment are secure to enable the administration tasks of their OVHcloud service and related systems in line with the criticality of their environment.	CC6.1, CC6.6, CC6.8
	Security events, backup and patching	
11	User organizations are responsible for monitoring security related events and logging appropriate diagnostic information of their systems in their OVHcloud environment.	CC7.1, CC7.2, CC7.3
12	User organizations are responsible for identifying and patching vulnerabilities as well as ensuring periodic maintenance on their OVHcloud environment in line with responsibilities defined as per the contractual agreement.	CC7.1, CC7.2

13	User organizations are responsible for establishing their own backup and restoration processes in the event of loss or damage to their OVHcloud environment. User organizations may subscribe to OVHcloud additional services for this purpose.	A1.2, A1.3
14	User organizations are responsible for implementing their own Disaster Recovery and Business Continuity Plans that address the inability to access or utilize their OVHcloud environment. User organizations may subscribe to OVHcloud additional services for this purpose.	CC9.1, A1.2, A1.3
15	User organizations are responsible for ensuring that their OVHcloud resources have the appropriate levels of redundancy and isolation; redundancy can be achieved using multiple locations.	CC9.1, A1.1, A1.2
16	User organizations are responsible for implementing appropriate incident response processes.	CC7.4, CC7.5
	Change management	
17	User organizations are responsible for following appropriate security practices during development and deployment of their systems in the OVHcloud environment.	CC8.1
18	User organizations are responsible for appropriately testing and approving changes on their systems before being deployed in their OVHcloud environments.	CC8.1
	Data and Privacy	
19	User organizations are responsible for managing compliance with applicable laws and regulations (including the General Data Protection Regulation).	P1.1, P2.1, P4.2, P6.6
20	User organizations are responsible for the integrity and the content of the data stored in their OVHcloud environment and the data transfers from their OVHcloud environment to an external environment. User organization should establish adequate controls for ensuring data integrity and compliance with applicable regulatory requirements.	CC6.7
21	User organizations are recommended to use encrypted (TLS/SSL) connections for all their interactions with OVHcloud. User organizations are responsible for determining, implementing and managing encryption requirements in their	CC6.7, CC6.8

	OVHcloud environment when it is not enabled by default and / or can be controlled by user organizations.		
22	User organizations are responsible for managing IP resources in an appropriate and sufficient manner to ensure the proper functioning of the OVHcloud services they subscribed to.		CC6.7, CC6.8
	Public Cloud specifics		
23	Compute	User organizations are responsible for installing and managing operating systems and applications on their instances.	CC6.1, CC5.1
24		User organizations are responsible for their use of the Service, in particular allocated processing capability and storage resources: User organizations are responsible for ensuring that instances have sufficient resources to function correctly.	A1.1, A1.3
25		User organizations are responsible for allocating appropriate storage assets to their instances, managing data lifecycle, including backups and encryption.	A1.2, A1.3, CC6.7, CC6.8
26	Block Storage	User organizations are responsible for allocating appropriate storage assets to their instances, managing data lifecycle, including backups and encryption.	A1.2, A1.3, CC6.7, CC6.8
27	Object Storage	User organizations are responsible for allocating appropriate storage assets to their instances, managing data lifecycle, including backups and encryption.	A1.2, A1.3, CC6.7, CC6.8
28	Managed Kubernetes	User organizations are responsible for their use of the Service, in particular allocated processing capability and storage resources: User organizations are responsible for ensuring that instances have sufficient resources to function correctly.	A1.1, A1.3
29		User organizations are responsible for not altering the pre-configured systems that operate the Kubernetes cluster.	CC5.1, CC5.2, CC6.1

30	Private Registry	User organizations are responsible for the lifecycle of the images stored in their private registry; user organizations are responsible for ensuring their images are devoid of security vulnerabilities or malware.	CC5.1, CC6.6, CC7.2
31	Data	User organizations are responsible for their use of the Service, managing data lifecycle and encryption.	CC6.7