



OVH.com

Trisotech Inc

OVH

Service Organization Controls (SOCSM) 3 Report-Type II
On OVH's Description of its Private Cloud System on the Suitability of the
Design and Operating Effectiveness of its Controls Relevant to Security.

Period from **December 1st, 2015 to November 30th, 2016**

Table of contents

SECTION I	Independent Service Auditor's Report provided by KPMG	4
SECTION II	Description of controls provided by OVH.....	6
1.	Management Assertion	7
2.	Company overview.....	8
3.	Definition of Services covered in the report	10
4.	Dependency on sub service organizations' controls.....	11
5.	Relevant aspects to System description and control environment ..	11
6.	Complementary User-Entity Controls	14

Trisotech Inc

-Intentionally left blank-

Trisotech Inc

SECTION I

**Independent Service Auditor's Report
provided by KPMG**



Trisotech Inc



Independent Service Auditor's Report

To the Board of Directors of

OVH Groupe SAS, Roubaix, France
-hereinafter also referred to as „OVH“ or „Company“-

We have examined management's assertion that during the period December 1st, 2015 to November 30th, 2016, OVH Group SAS ("Service Entity") maintained effective controls over the Private Cloud Services System to provide reasonable assurance on the suitability of the design and operating effectiveness of controls to meet the criteria for the security principle set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* issued by the American Institute of Certified Public Accountants and the Chartered Professional Accountants of Canada (applicable trust services criteria) (applicable trust services criteria).

OVH's management is responsible for this assertion. Our responsibility is to express an opinion based on our examination. Management's description of the aspects of the OVH Private Cloud Services System covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, CPA Canada and, accordingly, included

- (1) Obtaining an understanding of OVH's relevant controls over the security of the Private Cloud Services System;
- (2) Testing and evaluating the operating effectiveness of the controls; and
- (3) Performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, OVH's ability to meet the aforementioned criteria maybe affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on the AICPA and CPA Canada trust services security criteria.

Montreal, December 21st, 2016

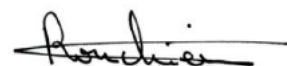
KPMG Canada LLP.



Paris, December 21st, 2016

KPMG France SA.

Renaud Ronchieri,
Partner, IT Advisory



SECTION II

Description of controls provided by OVH

Trisotech Inc

1. Management Assertion



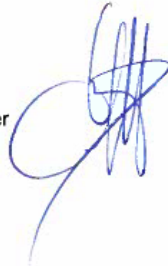
December 21st, 2016

The management of OVH Groupe SAS ("OVH") makes the following assertion pertaining to the Private Cloud Services:

OVH maintained effective controls over the Private Cloud Services system, during the period December 1st, 2015 to November 30th, 2016, in Montreal and France Data Centers delivering the service, based on the AICPA and CPA Canada Trust Services security, criteria set forth in TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids) to provide reasonable assurance on the suitability of the design and operating effectiveness of controls. The attached description of the Private Cloud Services System identifies those aspects of the system covered by our assertion.

OVH Groupe SAS
Laurent Allard
Chief Executive Officer

December 21st, 2016



Trisotech Inc

2. Company overview

2.1. Historical background and international expansion

The origins of OVH.com date back to 1999 when Octave Klaba, then a recent IT graduate from a leading French engineering school (ICAM Lille) acquired his first Server to host his own personal website. He quickly noticed the lack of any affordable webhosting solution for individuals and small businesses. By word of mouth, he received a growing demand from friends and other individuals to host their websites, so he decided to purchase additional units to meet this demand.

Octave and his family, all engineers, quickly understood the huge potential behind the idea and joined forces to develop the business. In 2003, the family embarked upon the design, assembly and commercialization of their own Servers and established first a Datacenter in Paris. At that time OVH.com engineered a unique and groundbreaking Watercooling system for Servers, now a proprietary technology providing OVH.com, with a distinct competitive advantage over its competitors, in terms of energy consumption and costs, a major expense for Datacenter operators.

The savings gained from vertical integration of Server production and the many innovations including Watercooling allowed OVH.com to offer a competitive value proposition for hosting solutions (little more than half the price of competitors at the time) combined with reliability and performance.

OVH.com development milestones



Source: Company information

With leading technology and an attractive value for money offer on a fast growing market, OVH.com was well positioned for the rapid growth that ensued.

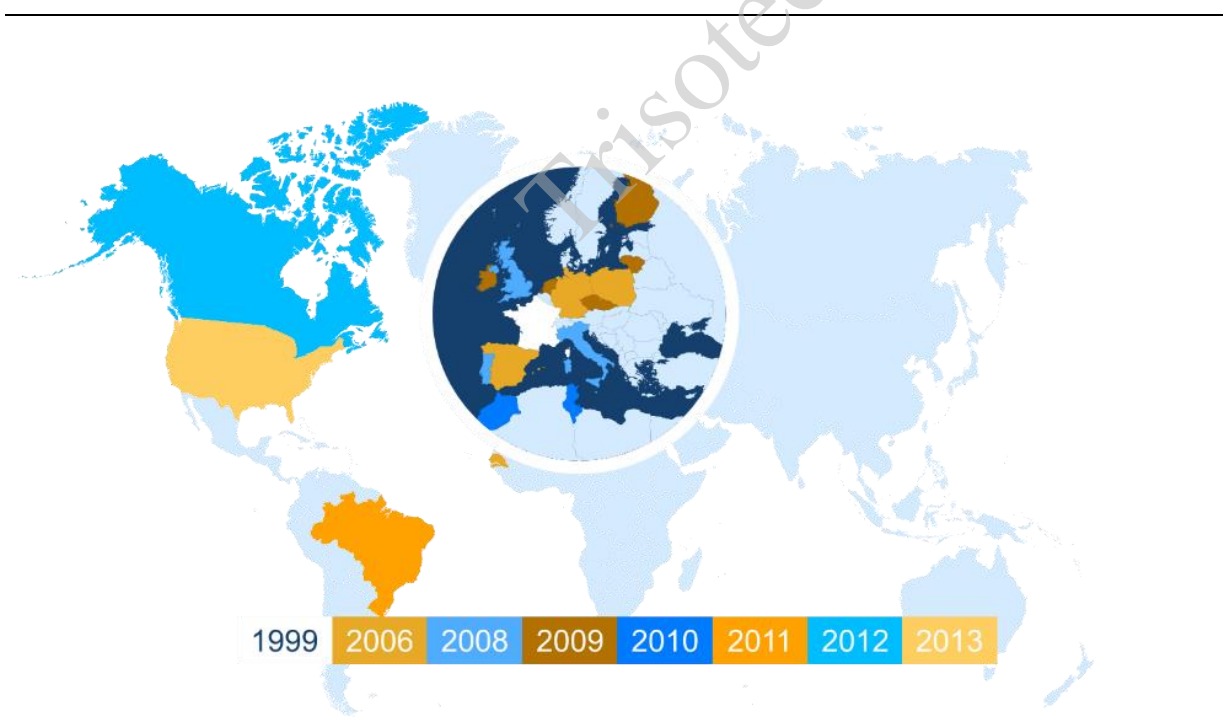


In 2005, the company began to feel constrained by the relatively small Paris Datacenter that hosted its Servers and decided to move its headquarters to Roubaix where it built its first self-designed Datacenter (RBX 1). The Roubaix site continued to expand year after year to accompany OVH.com’s growth. Roubaix now features six modern Datacenters built with incremental technologies driven by the group’s large investment in R&D over the years. The Roubaix 4 and 5 Datacenters were built in 2011 and 2012 using a cutting edge proprietary eco-room technology which allows the sites to operate in optimal condition with no recourse to any kind of active air conditioning. Together, Roubaix’s six Datacenters currently host close to 140,000 Servers along with their backups, infrastructure and the necessary systems to ensure the reliability, security and “redundancy” of Data stored, as well as best in class transmission speeds.



From 2005 to 2010 OVH.com also opened a new chapter of its history by starting its international expansion, opening Sales offices in 14 other countries across Europe and Africa.

International expansion and presence



Source: Company information

As well as the above strategic investments, OVH.com continued to reinforce its core business in Europe:

- In 2012, in addition to RBX 5, OVH.com opened a new Datacenter in Strasbourg (SBG 1).
- In 2013, OVH.com also continued its expansion in Strasbourg with Strasbourg 4 (SBG 4) and developed the largest data center in Europe in Gravelines (GRA 1 near Dunkerque) on more than 20,000 sqm.
- Further additions were being made to the OVH.com Datacenter base in 2014 with the launch of SBG 3, BHS 2 and RBX 6.

These investments are part of OVH.com Management's strategy aimed at driving long term growth by focusing investment in new generation technologies with very high growth potential, as well as increasing its footprint in key growth markets...

3. Definition of Services covered in the report

This report concerns the Private Cloud Services provided by OVH to its final customers. The Private Cloud Services are "Infrastructure As A Service" services. These services are delivered and operated from the Data Centers of Paris, Roubaix and Strasbourg for France and Beauharnois for Canada.

Private Cloud Services consist of machines (hosts, datastores) or resources (RAM, CPU) offered to customers on totally dedicated high availability infrastructures. Driven by VMware and Microsoft solutions in "as a Service" mode, clients build their Cloud by adding on demand physical resources to meet their needs and achieve business growth.

Virtual machines (VMs) are hosted in a virtual environment. Clients get the features of a physical server without having the actual hardware. Any OS can be installed on a VM and Clients can create as many VMs as they need on their Private Cloud.

Once the VM has been installed as per the model, Clients can customize as they want (CPU, RAM, storage, software...), to obtain a final version which matches the initial requirement.

The hosts and datastores are interconnected via a high availability lossless network. The 100% guarantee also applies between the internet and the virtual machines.

Private Cloud responds to numerous outsourcing requirements, as well as those of secure critical infrastructure construction. Total isolation and High Availability SLAs are guaranteed for the customers.

4. Dependency on sub service organizations' controls

As part of OVH Groupe SAS's activities, some Data Center maintenance activities are subcontracted to a set of third party providers. The control objectives and related controls executed by subcontractors are included in OVH Groupe SAS's description of its controls and are included within the scope of this report as the controls are the responsibility of OVH.

5. Relevant aspects to System description and control environment

5.1. Organisation, People and Processes

The control environment sets the tone of an organisation, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, management's operating style, delegation of authority systems, as well as the processes for managing and developing people in the organization.

The teams, especially the one working on the Private Cloud perimeter comprises only a small number of employees, and meetings are held, on demand, with the managers of the departments. Employees working on the Private Cloud have a confidentiality clause in their contract, and they are aware that a breach of confidentiality is a cause for immediate dismissal. Every employee has several review meetings with his operational manager, and at least every two years with his hierarchical superior. The management has developed a revamping and completion of procedures, which mostly address the functioning or development of controls. Management also organises the distribution of roles and responsibilities to combine at best the competences and experience of key staff between system and software development and maintenance skills. Private Cloud junior operators are supervised and trained by senior operators, who have mostly been trained and promoted in-house on the Private Cloud Solutions. Turnover of staff is considered particularly low for this business. Periodical, temporary, or permanent changes of distribution of roles and responsibilities between technical staff and management are also part of the company policy to optimize the rotation of experiences and add to the quality control.

Definition of controls and possibility to implement, with due consideration to the cost versus importance of risk is the responsibility of the Board, who is assisted for technical issues by internal and external Technical Experts / Consultants.

Procedures are defined by the technical staff and approved by Quality and Internal Control and Top Management, with the participation of relevant managers when needed.

Monitoring of procedures is the responsibility of the Quality and Internal Control Manager and the Board. Regular external audits are performed by external auditors for the operational tasks and compliance with ISO 27001 security requirements.

For the Private Cloud, Management periodically reviews with the managers the respect of procedures and results controls.

6.1.1 Risk Assessment processes

Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives and thus risk assessment is the identification and analysis of relevant risks to achievement of assigned objectives. Risk assessment is a prerequisite for determining how the risks should be managed.

Any decision, whether related to acquisition of software, change in the hardware infrastructure, development of new functionality for the Private Cloud Infrastructure management portal, implementation of protective measures and controls, or other, is made **by** the Board after sharing between the managers and collective evaluation of risks as far as possible.

A structured and formalized risk assessment approach was initiated by OVH in 2013, aiming to identify the major risks on the core business processes and finance, legal, HR, purchasing and sales processes.

This process is rolled out once a year to adjust risk assessment regarding business changes and notably is a basis for decision regarding new business investments.

Operational and technical risk assessment for the Private Cloud Solution was initiated in 2012 during the Information Security Management System (ISMS) implementation and is reviewed yearly prior to the ISO 27001 certification. Risks are identified at a detailed level and action plans are defined, implemented and monitored in order to mitigate those risks.

A process dealing with security breaches and incidents has been implemented within the ISMS in order to anticipate and handle properly, with the minimal impact on operations, the security incidents.

6.1.2 Information and Communication processes

Pertinent information must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. 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.

Effective communication also must occur in a broader sense, flowing down, across and up the OVH organization. All personnel receive a clear message from top management that control responsibilities must be taken seriously. They understand their own role in the internal control system, as well as how individual activities relate to the work of others. They have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators and shareholders.

For any new procedure release or modification, all members of staff are informed by Email and have access to such procedure in the collaborative internal web site.

The CEO also communicates by Email to all members of staff for important subjects related to the company, evolution of new contracts, start of new projects, introduction of new applications, etc.

In the case of new projects with new infrastructure or software, a special project team is formed and trained and a supervision program is established.

Technical and operational processes of the Private Cloud Infrastructure are formalized and controlled by the Quality and Internal Control Manager, with many consistency and accuracy controls which have been designed over time, since the ISMS implementation in 2012 and the 1st ISO 27001 Certification.

6.1.3 Monitoring processes

Internal control systems are monitored by a process that assesses the quality of the system's performance over time. It is accomplished through both ongoing monitoring activities as well as periodic, separate evaluations. Monitoring controls operate at the entity level as well as at the process level.

Supervision of controls for the technical Private Cloud infrastructure (hardware and software), is performed directly by the Quality and Internal Control Manager and the Board. The Quality and Internal Control Manager reviews the respect of SLAs for technical processes, and is directly supervising the running and maintenance of the infrastructure on a day to day basis.

Data Center Managers are in charge of supervision of controls related to security and protection of premises, as well as direction and supervision of the providers in charge of administration of environmental controls.

Technical incidents and problems (breakdown, disruption of service, slow down, bugs, etc.) are subject to analysis and review in management meetings based on the event. Having in mind the transparency culture of the company towards its operations, these incidents are communicated in real time to final clients through a dedicated internet portal, access is not restricted.

The small number of incidents since the launch of the Private Cloud Solution, as well as the results of SLA Compliance and technical partners' audits, is the best reward and motivation for this dedication.

6.2 Infrastructure, Software and Data

Private Cloud Computing (“PCC”): OVH.com’s Private Cloud offers the most secured Cloud Solution with guaranteed resources and the best cost-effectiveness on the market. With this service, the physical computing resources (the Servers) used for a given customer’s web data are ring-fenced and isolated from other Servers: they will serve only for the customer’s data, however the load from several customer services will be automatically balanced across the customer’s private Cloud, allowing for optimal performance without the need to use different physical machines for each service.

Services will instead be attributed one or more virtual machines to run on and more or less resources / hosts will be allocated to each service depending on the overall load. In order to offer the very best in Private Cloud virtualization, OVH.com has developed a strong partnership with VMware aiming to deliver complete Virtual Machines and Hypervisor platforms ready to run on OVH.com’s Servers. This historical partnership is a strong entry barrier on the market for new entrants who would need to negotiate their own system configurations in order to offer customers turnkey solutions as integrated and easy to use as OVH.com’s.

6. Complementary User-Entity Controls

OVH’s system was designed with the assumption that certain policies, procedures and controls would be in existence or implemented by user entities. These controls should be in operation at the user entities to complement OVH’s controls to achieve the customer’s security or business requirements in regard to the use of the System.

Trisotech Inc

Trisotech Inc



OVH.com