2

RISK FACTORS AND INTERNAL CONTROL

2.1 RISK FACTORS /AFR/

2.1.1 Mapping and summary table of the main risks

Risk category	Description of the risk
Risks related to OVHcloud's strategy and market	Non-realisation of the anticipated benefits of its acquisition strategy (*)
	Difficulties in the development of new products or services in an increasingly competitive market
	Risks related to the international expansion of OVHcloud
	OVHcloud's growth depends on increased IT spending and cloud usage by businesses
	Risks related to the implications of climate change
Risks related to OVHcloud's business	Supply chain risks (*)
	Risks related to a major interruption of OVHcloud services (*)
	Risks related to an incident on OVHcloud's physical infrastructures- (*)
	Risks related to the commercial development of OVHcloud
	Risks related to the launch of new projects
Human resources risks	Risks related to difficulties in recruiting and integrating new recruits
	Risks related to the development and retention of key people
	Risks related to occupational, physical or mental accidents
Financial and accounting risks	Tax risks
	Liquidity risks
	Risks related to currency exchange rates and interest rates
	Risks related to fraud
	Inflation-related risks
Legal and compliance risks	Risks related to non-compliance with certain laws and regulations
	Risks related to regulatory changes
	OVHcloud may not be able to protect its intellectual property rights.
Systems security risks	Risks related to the interruption of an internal IT system or tool
	Risks related to cybersecurity
	Risks related to data protection, loss or theft
Other risks	OVHcloud has entered into, and may continue to enter into, certain related-party transactions.

Risk management is closely monitored by Group management. The main mission of risk management is to identify, evaluate and prioritise (based on potential impact and probability of occurrence) risks, as well as to assist Group management in choosing the most appropriate risk management strategy and, in order to limit the remaining significant risks, to define and monitor the related action plans.

CSR risks are covered in Appendix II "Statement of Non-Financial Performance" ("*Déclaration de Performance Extra-Financière*" of this Universal Registration Document.

Risk mapping

The Group has developed a risk map in order to prevent the major risks relating to its activity, with the support of an external consultant specialising in these subjects. The risk mapping process, which was initiated in 2020, has made it possible to identify the main risks to which the Group is exposed and to assess their potential impact, taking into account their criticality, *i.e.* their potential severity and probability of occurrence.

The process of risk mapping involves the management of all Group activities and functions to a large extent, enabling the targets and challenges of all stakeholders to be taken into account. The exercise consists in particular of identifying the most significant risks for the Group, grouped into different families (strategy and markets, operational, human resources, financial, regulatory and legal, information systems). A description of the risks and their causes is provided, and for each of these risks, the probability of occurrence, their potential impact on the Group, and their current level of control are assessed. Following the assessment of the control of these risks, action plans are defined.

Progress in implementing the action plans is the responsibility of the Company's Executive Committee, which reviews them every two months. Risk mapping and action plans are presented to the Company's Audit Committee twice a year.

2.1.2 Main risks identified and system for managing these risks

The risk factors described below are, as of the date of this Universal Registration Document, those which the Company considers are likely to have a material adverse effect on OVHcloud, its business, financial position, results or outlook. The list of risks presented in this chapter is not exhaustive; other risks that are unknown or that OVHcloud does not consider to be significant at the date of this Universal Registration Document could have such an adverse effect.

In accordance with Article 16 of Regulation (EU) 2017/1129 of the European Parliament and of the Council, as amended, this chapter presents the risks identified as part of OVHcloud's significant risk mapping, which assesses their materiality (*i.e.* their potential impact and likelihood of occurrence), after taking into account the plans to mitigate these risks.

Within each risk category listed below, the risks that OVHcloud considers to be the most significant at the date of this Universal Registration Document are listed first and marked with an asterisk (*).

2.1.2.1 Risks related to the OVHcloud strategy and market

Non-realisation of the anticipated benefits of its acquisition strategy (*)

Description of the risk

OVHcloud expects to make acquisitions in order to expand its service offering portfolio (particularly in the area of software platform services) and geographic footprint. Acquisitions and other similar transactions and arrangements involve significant challenges and risks.

In general, when OVHcloud makes acquisitions, it is exposed to the risk that they will not contribute to the implementation of OVHcloud's strategy, that OVHcloud will receive an unsatisfactory return on its investment or that it pays too high a price, including due to liabilities or conditions that were not identified during the due diligence process prior to the acquisition. There is also the risk that OVHcloud will have difficulty integrating and retaining new employees, new business systems and new technologies, or that the acquisition distracts management from other OVHcloud activities. It may take longer than expected to realise the full benefits from these transactions and arrangements, such as increased revenue or enhanced efficiencies, or the benefits may ultimately be smaller than OVHcloud expected. These events could adversely affect OVHcloud's business, financial position and operating results.

Management of the risk

Within OVHcloud, the strengthening of the financial teams dedicated to acquisitions makes it possible to improve the sourcing of potential acquisitions and to have a regular link with the banks and the Company's ecosystem, to ensure the proper monitoring of changes in the market.

Dedicated teams from several departments are involved throughout the acquisition process in order to anticipate and monitor project developments. A systematic and comprehensive approach to the various teams is carried out during the acquisition process. A regular review is maintained during the integration phase to ensure the smooth running of the integration process. OVHcloud has made several acquisitions in recent years, which has strengthened the processes while improving the expertise of OVHcloud teams to select and integrate the acquired companies and assets. For instance, the successful integration of ForePaaS, acquired in April 2022, translates by the departure of any of the 23 employees present at the time of the acquisition, allowing ForePaaS and OVHcloud to deliver as planned the product development.

The success of these transactions and arrangements will depend in part on OVHcloud's ability to leverage them to enhance its existing cloud offerings or develop compelling new ones.

Difficulties in the development of new products or services in an increasingly competitive market

Description of the risk

The markets in which OVHcloud operates are rapidly evolving and highly competitive. In order to be competitive in these markets, OVHcloud must continually innovate and adapt its offers to changing customer needs. A significant part of the anticipated growth of the cloud market depends on innovations in areas such as graphic processing units, containerisation, hyper-convergence and edge computing. OVHcloud's ability to grow and win customer business will depend to a significant extent on its capabilities in these and other developing areas, in which many of OVHcloud's competitors have (and are likely to continue to have) leading offerings. OVHcloud believes the pace of innovation in cloud products and services is likely to continue to accelerate as customers increasingly base their purchases of cloud offerings on their needs for new and upgraded features that are expected to drive a significant share of future market growth. The future success of OVHcloud depends on its ability to continue to innovate in response to these demands (which means continuing to invest in technologies, services and partnerships) and increasing customer adoption of its cloud offerings.

Additionally, as the markets in which OVHcloud operates continue to mature and new technologies and competitors enter such markets, competition might intensify. Many of OVHcloud's competitors are much larger, well-known international cloud companies, including the so-called "Hyperscalers" (Amazon Web Services, Google Cloud Platform and Microsoft Azure), as well as other established cloud providers such as IBM Cloud and, in Asia, Alibaba Cloud. In Europe, OVHcloud also competes against cloud specialists such as Hetzner, Leaseweb and iomart, and many emerging cloud providers. As OVHcloud expands its offering of software platforms, it will also compete to a greater degree with other companies in these markets, such as Salesforce, Oracle, IBM and SAP. New competitors are likely to continue to enter the market as it evolves. For example, Microsoft, Orange and Capgemini announced the formation of the partnership (Bleu), which aims to offer sovereign data cloud solutions that could compete with those of OVHcloud.

Many of OVHcloud's competitors, particularly outside Europe and in the public cloud space, have greater brand awareness, larger customer bases, extremely aggressive business practices and greater financial, human or technical resources, than OVHcloud. These same competitors are likely to be able to respond more quickly than OVHcloud to new markets and developments in terms of opportunities, technologies, standards, customer requirements and purchasing practices. The Hyperscalers, in particular, are among the largest and best known information technology companies in the world, with established relationships on a global, regional and local scale, and brand recognition that OVHcloud is unlikely to be able to achieve. The Public Cloud market, which is dominated by the Hyperscalers, is expected to be the fastest growing segment of the cloud market. If OVHcloud is unable to compete effectively against the Hyperscalers, its growth prospects could be adversely affected.

If OVHcloud is unable to enhance its cloud offerings to keep pace with market evolutions, or if competitors emerge that are able to deliver competitive offerings at lower prices, more efficiently, more conveniently or more securely than OVHcloud's cloud services, OVHcloud's business, financial position and operating results could be adversely affected.

Management of the risk

OVHcloud positions itself against its competitors on the basis of various factors, including: price, performance, multi-cloud and hybrid cloud trends, customer support, scalability, reliability, data sovereignty, security, sustainable development, energy efficiency and compatibility with existing standards.

In order to continue to offer new solutions and maintain its positioning, OVHcloud has an open development strategy. For example, the Company can build on open source software and acquire new technological bricks by integrating companies such as ForePaaS, acquired in 2022. OVHcloud also has internal teams to develop its product roadmap and the Company can forge partnerships with recognised players in their fields, such as MongoDB or Nutanix, if it considers that the products are standards expected by its customers. During its fiscal year 2022, OVHcloud invested 92.2 million euros in research and development, as detailed in note 4.10 of chapter 5 of the this Universal Registration Document.OVHcloud also has an integrated industrial production tool and dedicated research and development teams that enable it to quickly adapt its manufacturing and supply needs to support product changes.

Risks related to the international expansion of OVHcloud

Description of the risk

As part of its growth strategy, OVHcloud is seeking to expand its income from other regions, including in Continental Europe (outside France), Northern Europe and the United States.

OVHcloud may face significant challenges in its efforts to expand its international income. Outside its home market of France, OVHcloud has lesser brand recognition and does not benefit from the historical web hosting market leadership that it enjoys in France, reducing opportunities for cross-selling. Market dynamics and customer preferences in international markets are likely to be different from those of OVHcloud's traditional markets and local policies of economic patriotism can make it difficult to access new territories. Certain markets that OVHcloud targets (such as the United States market) are dominated by hyperscalers, and the expansion of OVHcloud in these markets will depend on its ability to market its products to customer segments that it believes are users of this type of service, such as smaller companies ("level 2") and systems integrators. Even if OVHcloud is able to expand internationally, managing international operations requires a more structured organisation and greater resources than managing operations in OVHcloud's home market, which will increase OVHcloud's overhead expenses even if there is a not a corresponding increase in income generated from these new markets.

OVHcloud could be faced with geopolitical tensions in certain countries or regions that would limit its ability to develop its commercial offering locally. OVHcloud could also suffer a nationalisation of its assets or abusive legal attacks. Accordingly, OVHcloud might not meet its international expansion targets, and even if it does, there can be no assurance that the profitability of its expanded international activities will be satisfactory.

Management of the risk

OVHcloud has developed several programmes and initiatives to limit the risks associated with its international expansion. The creation of commercial clusters allows OVHcloud to have local teams, experts in their regions with knowledge of local specificities, in order to define the commercial or product offers that are most in line with the expectations of local customers. This organisation also makes it possible to control and anticipate any changes in the markets, both by the end customer and by local public authorities.

The Company has also set up a programme dedicated to assessing and monitoring projects to open new data centres ("GEOS programme"). This programme involves all the teams concerned by a project to open a data centre and makes it possible to anticipate potential obstacles.

Situation in Ukraine

With regard to the current geopolitical situation between Russia and Ukraine, the Group is constantly monitoring its domestic customers in Russia, Belarus and Ukraine. As of the date of this Universal Registration Document, the Group states that it strictly complies with the regulations in force. Furthermore:

- revenue generated in Russia, Belarus and Ukraine represents approximately 1.5% of the Group's revenue as at 31 August 2022;
- the Group does not have any employees in Ukraine, Russia or Belarus;
- the Group has no service providers (individuals) based in Ukraine;
- it has no infrastructure in these three countries;
- there is no material risk of recovery of receivables due at 31 August 2022.

OVHcloud's growth depends on increased IT spending and cloud usage by businesses

Description of the risk

OVHcloud expects that a significant portion of its growth will result from the rapid growth of the cloud market segments in which it operates. Continued market growth depends on businesses continuing to increase their spending on outsourced IT infrastructure, and devoting a greater share of their IT spending to the cloud.

While cloud spending has increased significantly in recent years, there can be no assurance this trend will continue in the future. The rate of growth in spending will depend on a number of factors that are beyond OVHcloud's control, including overall business spending and investment levels, decisions relating to the allocation of such spending to cloud projects, the level of confidence of businesses in cloud services (which could be adversely impacted by any service incidents in the market), the development of new cloud-based services, regulatory developments, sustainability concerns (given the significant use of electricity and water in data centres) and other factors.

Even if the cloud market continues to grow as a general matter, the rate of growth could be lower in the product and geographic segments that generate most of OVHcloud's income. In FY2022, 62% of OVHcloud's income was realised in the Private Cloud market, which has grown, and is expected to continue to grow, at a less robust pace than the Public Cloud market. In addition, 78% of OVHcloud's revenue for the 2022 financial year was generated in France and elsewhere in Europe, which is a significantly smaller cloud market than the United States. Businesses in Europe have been slower to adopt cloud solutions than in other markets (such as the United States). If they do not increase their cloud spending, the growth of the market in Europe could turn out to be lower than expected.

OVHcloud's revenue growth will also depend on the growth rate of the Web Cloud market, which includes website hosting, domain name registration, telephony and other services. The Web Cloud market is more mature than the cloud market generally, and is expected to grow at a slower rate than the cloud market in the coming years.

As a consequence, OVHcloud's overall revenue growth could be lower than that of the cloud market generally, and lower than that of other cloud market participants. Slower revenue growth could negatively impact OVHcloud's profitability and financial position, as well as the market price of its shares.

Management of the risk

OVHcloud reduces these risks by diversifying its geographical presence, its offerings and the profile of its customers. OVHcloud is the European cloud leader and has a global footprint with a commercial presence in 140 countries. In 2022, OVHcloud generated 49% of its revenue in France, 29% in Europe (excluding France) and 22% in the rest of the world. In addition, OVHcloud offers its customers a varied range of products and services that meet different needs and are not exposed to the same economic dynamics. Lastly, the growth strategy focused on key account customers enables OVHcloud to strengthen its diversification with customers with greater financial strength and significant development prospects in the cloud.

Risks related to the implications of climate change

Description of the risk

Due to the geographical scope of its operations and sites, the Group could be exposed through various causes to:

- Occurrence of extreme natural disasters such as floods, earthquakes, extreme droughts, "giant" fires, landslides, cyclones or tsunamis;
- Tightening of regulations on energy management (electricity), water use and building construction standards;
- Occurrence of occasional or permanent shortages (water, electricity, etc.).

This risk is exacerbated by climate change, which has a direct impact on the frequency and severity of these events. Large-scale or repetitive natural disasters can also lead to exceptional situations of disruption of the external physical infrastructures and means of communication on which OVHcloud depends to carry out its activity, and cause damage to the infrastructures for which it is responsible. OVHcloud may thus temporarily be unable to implement its services according to the conditions defined by the contracts. The Group may have to compensate for unavailability by means of costs that exceed forecasts. For example, the multiplication of heat wave events could increase the operating cost of the Group's cooling systems.

Management of the risk

The implementation of OVHcloud services requires constant vigilance and anticipation. In addition to regulatory requirements, OVHcloud offers solutions to actively manage risks related to natural disasters, in particular with its hyper resilience plan, through:

- The CSR function integrated into the Group Strategy Department and represented on the Group Management Committee;
- The integration of environmental innovation into R&D projects (reduction of energy consumption or reduction of the need for natural resources such as water);
- Diversification of energy supplies including low-carbon energy;
- Deployment of a comprehensive risk management process:
  - identification and assessment of the exposure of sites to natural disasters;

- risk mitigation through the implementation of corrective and preventive actions;
- duplication of production and operating resources through the redundancy of equipment, facilities and services;
- analysis with customers of the vulnerabilities of the deployed infrastructures and support and advice on optimisation;
- acquisition and development of new solutions focused on business continuity recovery.

The risk related to natural disasters is reduced thanks to: (i) the choice of site locations in order to limit their exposure, (ii) the analyses of the various scenarios allowing the implementation of adapted prevention plans, as well as (iii) the development of business continuity plans. Site audits and insurance systems supplement the measures for managing this type of risk.

2.1.2.2 Risks related to OVHcloud's business

Supply chain risks (*)

Description of the risk

OVHcloud could be exposed to the failure of a key supplier or to difficulties in sourcing key components. OVHcloud servers use components from major global manufacturers such as Intel and AMD for microprocessor chips, Micron Technology and Samsung for memories, Arista and Cisco for network equipment and Seagate and Toshiba for hard drives. The global market for components is currently experiencing shortages and delays, as a result of increased demand arising from greater use of information technology during the Covid-19 crisis.

The Company could experience disruptions in its supply chains, for example related to the continuation or worsening of the Covid-19 pandemic or to geopolitical tensions, which would impact server production and data centre operations. There are a limited number of suppliers of electronic components worldwide, and certain of them are located in markets in East Asia that are subject to potential disruption for geopolitical reasons. Despite regular, high-level contacts, the size of OVHcloud on the global market limits its ability to sign generalised delivery agreements.

If OVHcloud is unable to obtain a sufficient number of electronic components, it may dismantle existing servers and reuse electronic components to manufacture new servers. The re-utilised electronic components may have lower performance features, and may experience more disruptions, than new processors. This may lead to impaired service quality or service disruptions, which could increase the risk of customer churn and reputational harm, and cause a negative impact on OVHcloud's business, financial position and operating results, and it could specifically bring OVHcloud to increase its stock or the production costs of its servers.

Management of the risk

Thanks to its vertically integrated model, OVHcloud can control the entire value chain. OVHcloud builds precautionary inventories, in order to be able to withstand temporary disruptions, and has a well-organised purchasing organisation.

OVHcloud's model also allows it to plan and anticipate certain orders and guarantees flexibility. Finally, the purchasing teams continue to develop commercial relationships with OVHcloud suppliers in order to negotiate supply contracts at the global level.

In addition, OVHcloud has a recycling policy based on a logistics chain allowing the reuse of components and equipment. In this context, OVHcloud recovers the components from equipment considered to be at the end of its life, subjects them to tests and then reuses those it believes could be used inside new equipment.

Risks related to a major interruption of OVHcloud services (*)

Description of the risk

OVHcloud relies on access to sufficient and reliable electric power, internet, telecommunications and fibre optic networks to successfully operate its business. In addition, OVHcloud's proprietary water-cooling system for its servers requires OVHcloud to have access to substantial volumes of water at its data centres. Any interruption in these services could result in OVHcloud not being able to provide customers with its cloud offerings at adequate performance levels, or at all. For example, in 2017, the electric power supply was interrupted at one of OVHcloud's Strasbourg data centres, and the backup power supply did not function properly, resulting in a service outage for approximately three hours. In addition, in the context of an energy shortage, OVHcloud is exposed in certain countries to a risk of electricity shedding that could lead to a temporary interruption of its services. Any interruption in these services could result in OVHcloud not being able to provide customers with its cloud offerings at adequate performance levels, or at all.

OVHcloud's solutions rely on third-party software and open-source software maintained by organisations of which OVHcloud is only one of many members. For example, OVHcloud's Hosted Private Cloud solutions rely on virtualisation software provided by VMWare, and its Public Cloud solutions rely on the OpenStack and Kubernetes platforms. In addition, OVHcloud depends on the availability of licenses for software used by its business customers, such as Office365. If there are vulnerabilities, bugs or corruptions in this underlying software, or if the software ceases to be available, or if competing software gains greater market acceptance, OVHcloud may suffer disruptions or other performance and quality problems. If the software upon which OVHcloud depends experiences these or other deficiencies, or if licenses are unavailable or contain restrictions, OVHcloud's competitive position may decline and customer churn may increase, either of which would have an adverse impact on OVHcloud's reputation and profitability.

In its service contracts, OVHcloud typically commits to its customers that its platform will maintain a minimum level of availability, through service-level agreements (SLAs). For example, OVHcloud undertakes to maintain a service level of 99.9% availability for the Premier offers in the Hosted Private Cloud segment. In OVHcloud's Public Cloud offerings, OVHcloud commits to maximum recovery times in case of outages. If these outages are caused by a problem outside of OVHcloud's control, it could be difficult for OVHcloud to meet its SLA commitments.

Although OVHcloud considers that it has put in place adequate safeguard measures depending on the services subscribed, these may prove insufficient to prevent an interruption of service. Additionally, OVHcloud may face costs associated with repairing such service disruption. All of the above consequences could have a negative impact on OVHcloud's business, financial position and operating results.

Management of the risk

Thanks in particular to its water-cooling model, OVHcloud is constantly trying to reduce its electricity and water consumption. The effectiveness of this model can be found in the PUE (Power Usage Effectiveness) ratio, which reached 1.28 in 2022, as detailed in Chapter 3 of this Universal Registration Document. In the same way, since water-cooling is carried out in a closed circuit, OVHcloud consumes much less water for the operation of its data centres compared to a traditional data centre cooled by an air conditioning air-cooling system. This performance is reflected in the WUE (Water Usage Effectiveness) ratio, which reached 0.26 l/kWh.

OVHcloud also provides for several redundancy measures in the event of power outages, for example with the implementation of several electricity delivery points in its data centres or with the presence of a diesel generator on site that can be activated in the event of an outage.

In order to be able to intervene as quickly as possible in the event of a breakdown, OVHcloud has organised its technical support to be available 24 hours a day, seven days a week, in a "follow the sun" organisation. An NOC (Network Operating Centre) team is always present to ensure the availability of the internet network and intervene if necessary.

Lastly, OVHcloud develops its software in Open Source, which it considers to be a significant advantage in ensuring the quality and availability of the software developed. The number of independent developers or other companies working together on this software is a guarantee for the robustness and quality of the code. All of this work is generally public, which also allows for auditability and transparency in the code.

Risks related to an incident on OVHcloud's physical infrastructures (*)

Description of the risk

Many of OVHcloud's data centres and server manufacturing facilities are housed in former industrial buildings. Depending on the age of these buildings, the industry of the former occupant and the industries of neighbouring facilities, certain of OVHcloud's facilities may have existing structural and environmental defects that may present safety and compliance risks or require OVHcloud to spend significant amounts on remediation.

Some of OVHcloud's data centres and manufacturing sites engage in activities that are classified as presenting environmental or other risks under applicable French legislation. In many such cases, OVHcloud is required to obtain permits from competent governmental authorities before commencing operations. The application process is costly and time consuming, and OVHcloud could be required to remedy defects and risks as a condition to obtaining the necessary authorisations. In this respect, the application for authorisation for the Roubaix site submitted in 2019 was the subject of additional requests from the authorities during its investigation, and authorisation was granted in 2021, a few months after the additional information requested was provided. With respect to the other sites, the Company is not aware of any refusals by the administration, has not been forced to close any data centres, and has not been subject to any sanctions. While all required applications have been submitted or are in process with a view to OVHcloud obtaining such authorisations, it cannot be certain that such authorisations will be granted. The administration's requests may require investments in compliance to reduce the potential impact of claims related to classified activities (for example: fires or water pollution). If it operates activities in sites that are subject to administrative authorisations, until these authorisations are formally granted, OVHcloud could be subject to administrative sanctions or be obliged to suspend its classified activities on the sites concerned, which could lead to a loss of customer service and impact OVHcloud's income and reputation.

Additionally, OVHcloud may incur liability based on various building conditions. For example, some of OVHcloud's facilities may contain, or may have contained, hazardous substances, or may not be in compliance with current health and safety standards or building codes.

Lastly, OVHcloud has been, and may be in the future, subject to litigation in relation to the state of its facilities or nuisances (such as noise and heat) generated from such facilities. It is currently subject to claims of this nature with respect to its data centre in the nineteenth *arrondissement* of Paris, and while the financial impact of these claims is not expected to be significant, OVHcloud may need to modify its operations to resolve them. If any of this litigation cannot be resolved in a timely and cost-effective manner, OVHcloud's business, financial position and operating results may be harmed.

OVHcloud's Paris data centre hosts applications that are essential to the OVH Groupe's internal operations. If an incident were to affect this site, the consequences could be significant for the Company. Thus, OVHCloud has begun the migration of all the services it contains on other sites. This migration, which is currently underway, should be completed during the first quarter of 2023 and will strengthen the applications concerned.

OVHcloud's data centres could be affected by destructive natural events that would impact the Company's activities.

Management of the risk

While OVHcloud commissions environmental and safety audits before acquiring sites for data centres, it cannot be certain that these audits will reveal all defects and risks, or that the cost of remedying any such defects and risks will be consistent with the amounts budgeted by OVHcloud for such purpose.

Although OVHcloud's policy is to seek to remedy any risks that are identified, doing so could be costly and time-consuming, and failure to make necessary repairs and to complete any other required work could damage OVHcloud's reputation, subject it to liability and disrupt its business.

More generally, OVHcloud carries out reviews of facilities with its insurers in order to prevent potential risks in advance.

Following the Strasbourg fire, OVHcloud is implementing a "hyper resilience" plan in order, among other things, to take security standards in its data centres beyond the regulatory standards and insurers' recommendations.

The data centres have 24/7 physical security, a highly regulated and controlled access policy, and have dedicated anti-intrusion systems.

Strasbourg incident

During the night of 9-10 March 2021, a major fire broke out at one of OVHcloud's four data centres in Strasbourg, France. A judicial appraisal was conducted by the Court of Justice of Strasbourg by order on 27 April 2021 following an interim summary issued by the Company and its insurer AXA to determine the origin of the fire and the possible aggravating factors. Based on the information currently available, it appears that the fire started in an energy room housing electrical equipment. To date, the forensic appraisal is still ongoing, the mission of the forensic appraisers having been extended until 30 August 2023.

As a result of the fire, OVHcloud was required to cut off electricity at the entire site, closing all four Strasbourg data centres. The data centre at which the fire occurred was destroyed, and a second data centre was partially damaged. While OVHcloud transferred as many customers as possible to other data centres, many customers lost service for a significant time period. In addition, because data backup services are optional, paid services for most customers, some of OVHcloud's customers did not have them, and those that had not carried out their own backups experienced a permanent loss of data.

The fire and its consequences had a significant financial impact on OVHcloud and could have additional consequences that may impact the financial statements for future periods. At 31 August 2022, the balance of the provision amounted to €24.5 million. The provision was determined in conjunction with the Company's advisors, after studying customer claims by exposure category, even though not all the claims received have yet been settled or adjudicated.

OVHcloud has declared to its insurers, as part of its property damage and civil liability insurance policies, the incident related to the Strasbourg fire and its consequences, including losses from customer claims. In September 2021, OVHcloud's insurers paid it a single lump-sum indemnity of €58 million for direct damage caused by the fire.

Legal proceedings related to the Strasbourg incident

OVHcloud has become, and may continue to become, the subject of legal actions initiated by customers that have suffered alleged losses as a result of the fire, including actions for damages for loss of service and loss of data. While OVHcloud's customer contracts contain clauses limiting OVHcloud's liability, customers may argue that their losses are not covered by these clauses, or that the clauses are unenforceable.

At 31 August 2022, OVHcloud had received a limited number of complaints and requests for information from customers alleging to be affected by the Strasbourg incident, a significant portion of which were received in the first three months following the fire. Customers, located primarily in France and to a lesser extent in other European countries, are requesting information about the data stored on the OVHcloud servers, recovery of any lost data and, in some cases, monetary compensation. The requests for compensation are generally for small individual amounts, or are not quantified.

OVHcloud believes that, in a significant proportion of cases, customer claims are unfounded, and that in most other cases the commercial gestures already spontaneously granted to customers largely compensate for any prejudice suffered by them. OVHcloud has endeavoured to find an amicable agreement to settle customer claims whenever possible.

OVHcloud may be required to pay certain amounts as part of settlement agreements, or as a result of definitive legal decisions. In addition, OVHcloud incurs certain costs related to the management of this litigation and these agreements. In this respect, OVHcloud does not consider that the total cost of appraisal costs, procedural costs and customer claims has changed since 31 August 2021. At 31 August 2022, the balance of the provision amounted to €24.5 million. The provision was determined in conjunction with the Company's advisors, after studying customer claims by exposure category, even though not all the claims received have yet been settled or adjudicated.

Risks related to the commercial development of OVHcloud

Description of the risk

The majority of OVHcloud's customer contracts are short-term and can generally be cancelled by the customers with little or no prior notice. In the Public Cloud segment, OVHcloud's income is generated through usage fees, and customers are not required to maintain any minimum level of usage. In the Private Cloud segment, OVHcloud's customers generally subscribe on a monthly basis, and can cancel their subscriptions at any time (subject in certain cases to minimum engagement durations). Accordingly, OVHcloud bears the risk of customer churn, which could occur or accelerate at any time. If OVHcloud's customers cancel their contracts or reduce their use of OVHcloud's services, OVHcloud's income and profitability will be adversely impacted.

OVHcloud markets its service offerings in part through third parties such as system integrators and other IT consultants, as well as through web agencies, which propose OVHcloud's services to their own customers. OVHcloud's income growth plans depend in part on its ability to successfully expand income generated through this marketing channel. It cannot be certain that it will be able to achieve its target. When OVHcloud markets its services through third parties, it gives up a measure of control over the process, and it depends on the third party's relationship with its customers in order to attract those customers. OVHcloud's relationships with its third party marketing partners are not exclusive, and the partners might decide to promote the offerings of competitors over those of OVHcloud, in which case OVHcloud would lose income generation opportunities. If a marketing partner includes OVHcloud's services in a package that includes other IT services, a problem in the delivery of those other services, or the negligence or malfeasance by such marketing partner, could lead customers to reduce their use of the entire package, including OVHcloud's services. Moreover, any event that impacts the reputation of a reseller could indirectly impact OVHcloud's reputation. Such incidents, if they were to occur, could negatively impact OVHcloud's income and market position.

Management of the risk

OVHcloud continually improves its customer service and puts customer satisfaction at the heart of its policy. This strategy has shown results and enabled OVHcloud to post a net retention rate of 114% in 2022, an improvement compared to 2021. In addition, OVHcloud increasingly offers its customers the option to subscribe to its services and products with commitments over several months, in return for a reduction on public prices. This option allows OVHcloud to ensure increased visibility on the evolution of its existing revenue.

Finally, the revenue generated by OVHcloud's partners reached double-digit growth in 2022. This performance illustrates the success of the growth strategy with third parties. Thanks to its significant price/performance ratio and its positioning across all cloud businesses, OVHcloud offers its partners the possibility of proposing extremely competitive offerings that meet a wide range of their needs to their own customers. This momentum is maintained by OVHcloud with, in particular, training sessions for resellers and integrators to ensure that their internal teams are aware of OVHcloud's offerings and are able to sell and make the best use of the services and products sold by the Company.

Risks related to the launch of new projects

Description of the risk

As part of its activity, OVHcloud regularly develops and launches new services and products. These launches may represent significant marketing and commercial expenses and may not find the success expected by the Company. Several factors can negatively influence this type of launch, whether it is an erroneous analysis of the market and customer expectations or a too early or poorly targeted "go-to-market". Failure to launch new projects could prevent OVHcloud from achieving its income growth targets, which would have an adverse impact on its profitability.

Management of the risk

OVHcloud has implemented strict decision-making processes for new project launches with mandatory steps. These processes make it possible to involve the various teams mobilised on these projects and ensure optimal development, in-depth market studies and a structured launch. A team is dedicated to managing these new projects and monitoring processes. This team is also responsible for the monitoring and continuous improvement of recently launched projects.

2.1.2.3 Human resources risks

Risks related to difficulties in recruiting and integrating new recruits

Description of the risk

It is important to OVHcloud's business to attract and retain highly-skilled and international personnel, particularly engineers with expertise in software development, coding and other highly specialised information technology functions. The marketplace is highly competitive, and qualified IT personnel are in high demand, which may make OVHcloud's recruiting and retention efforts challenging.

If OVHcloud's company culture changes or is perceived negatively, or if OVHcloud is unable to develop its employer brand on par with competitors, it may experience difficulties attracting and retaining personnel. OVHcloud may not be able to achieve its commercial targets, and its business, income and finance results may suffer.

Management of the risk

OVHcloud, through its positioning as a European cloud leader, defender of European sovereignty and its growth profile, offers a unique value proposition for many recruits. In addition, the Company's continuous international development enables it to broaden the pool of talent likely to join it.

OVHcloud has set up an onboarding process lasting a full week, with the intervention of several members of the Executive Committee and a broad presentation of the Company, its businesses and its organisation. This week makes it possible to create links between new recruits from their first days at OVHcloud and to engage new recruits in the culture of OVHcloud.

Risks related to the development and retention of key people

Description of the risk

The Company employed around 2,800 people at the end of August 2022, with many employees dedicated to technical development or specialised IT topics. These professions are particularly under pressure and many companies, regardless of their sector of activity, are looking for similar profiles. Thus, OVHcloud may be faced with the departure of key people for its organisation. In addition, as the skills required in IT evolve rapidly and constantly, OVHcloud must be vigilant in providing its employees with continuous training on new issues that may arise, in particular technical issues.

Management of the risk

OVHcloud is particularly vigilant about adapting working conditions, employee loyalty and the training offered. Human resources processes are in place to support people within the Company, with monitoring of employee engagement, career development and continuous training programmes. Several loyalty drivers are in place at OVHcloud, including measures for improved living conditions at work (access to a crèche, a doctor, a gym).

For the skills most at risk, a mapping of human resources tensions is in place and makes it possible to closely monitor the development of key people.

Risks related to occupational, physical or mental accidents

Description of the risk

OVHcloud could be sued for accidents at work, physical accidents, during maintenance operations or in data centres, or mental accidents, for example following an excessive workload or a particularly stressful situation.

Management of the risk

The Company has created a "Quality, Environmental, Health and Safety Policy" ("QEHS") team dedicated to these topics. In addition to offering personal protection equipment in its data centres, the Company undergoes certification processes in order to constantly improve its security methods and standards for its teams. In order to limit mental risks, the Company has implemented several measures such as a psychosocial audit, a mental risk mapping and the existence of an alert tool. Employee surveys are carried out regularly to work on any weak signals.

2.1.2.4 Financial and accounting risks

Tax risks

Description of the risk

OVHcloud determines the amount of taxes it is required to pay based on its interpretation of applicable treaties, laws and regulations in the jurisdictions in which it operates. The tax and social security regimes applied to OVHcloud's business activities and past or future reorganisations involving Group companies, shareholders, employees and/or managers are or may be interpreted by relevant French or foreign authorities in a manner that is different from the assumptions used by OVHcloud in structuring such activities and transactions. Based on its international activity and its expansion, OVHcloud is subject to complex and evolving tax legislation which may be subject to different interpretation in the various countries in which it operates (in particular with respect to transfer pricing, sales taxes, VAT and similar taxes). OVHcloud therefore cannot guarantee that the relevant tax authorities will agree with its interpretation of the applicable legislation in their jurisdictions. Furthermore, tax laws and regulations or other compulsory levies and their interpretation and application by the jurisdictions or administrations involved may change, in particular in the context of joint initiatives taken at international or EU level, which could increase the tax burden on the Group.

Moreover, several countries have implemented a tax on digital services, demonstrating a global trend of rapid and unpredictable changes in tax legislation (or a broader interpretation of existing legislation) applicable to certain activities of the Group. Because the scope of application of these taxes differs between countries, OVHcloud is not affected by all of these taxes. New or revised regulations may subject the Group or its customers to additional sales, income and other taxes. OVHcloud cannot predict the effect of such initiatives. New or revised taxes could increase the cost of doing business online and OVHcloud's internal costs, which could impact both OVHcloud and its customers.

Any of the abovementioned events could adversely affect OVHcloud's business, operating results, prospects and/or financial position.

Management of the risk

OVHcloud and its legal tax teams ensure that they comply with the tax laws in which the Company operates. OVHcloud can be supported by an external consulting firm when necessary.

Tax policy

The OVHcloud Group's tax policy provides that the Group undertakes to apply the laws, regulations and tax treaties in force in all countries in which it operates.

The Group's values and ethical principles as well as its requirements in terms of social responsibility lead it to:

- conduct its operations in accordance with their economic reality;
- refuse any aggressive tax planning and the use of artificial structures located in "tax havens";
- cooperate with local tax authorities during tax audits.

None of the transactions carried out by the OVHcloud Group aims to evade the payment of tax. The Group is in the process of compiling all of these actions and provisions into a formal tax policy.

Liquidity risks

Description of the risk

Liquidity risk is the risk that OVHcloud does not have the necessary funds to meet its commitments when they fall due. In a situation of stress on the credit market, the Company may not be able to obtain the financing or refinancing necessary to implement its growth plan and this could have a negative effect on the activities and OVHcloud's operating results, outlook and/or financial position.

Management of the risk

Following its successful IPO in October 2021, with a capital increase of €350 million, and the signature in September 2021 of a new unsecured senior loan agreement for a total principal amount of €920 million, OVHcloud has strengthened its financial structure. In addition, in October 2021, the Company repaid all of its previous syndicated loan, as well as the bonds that had been issued as part of a Euro Private Placement, for a total amount of €705.2 million. At 31 August 2022, the undrawn portion of the new RCF amounted to €360 million.

Thus, after these transactions and at the end of its 2022 financial year, OVHcloud's net debt leverage reached 1.7x its adjusted EBITDA. This level remains lower than its target of remaining below a debt gearing ratio of 3x its adjusted EBITDA.

Risks related to currency exchange rates and interest rates

Description of the risk

OVHcloud's financial statements are presented in euros, while a portion of its income, expenses, assets and liabilities are denominated in other currencies, exposing OVHcloud's operating results and financial position to foreign exchange risk. In 2022, approximately 25% of OVHcloud's revenue was generated in currencies other than the euro, primarily by entities with functional currencies in Canadian dollars and US dollars, with smaller amounts realised in pounds sterling and Polish zloty. While a portion of OVHcloud's costs are denominated in these currencies, unfavourable movements in exchange rates would nonetheless adversely impact OVHcloud's operating income. An adverse change of 10% in exchange rates would have a negative impact of approximately €15 million on OVHcloud's revenue. In addition, a significant portion of OVHcloud's capital expenditure (mainly for server components) is incurred in US dollars.

If OVHcloud is not able to successfully hedge against the risks associated with currency fluctuations, its operating results could be harmed. In addition, adverse movements in exchange rates would reduce the value in euros of OVHcloud's assets denominated in foreign currencies, which would not be fully offset by changes in the value of liabilities, and would thus negatively impact OVHcloud's shareholders' equity.

The loans taken out by the Company bear interest at a variable rate equal to a reference rate plus a margin, which exposes OVHcloud to interest rate risk. If the interest rate increases, OVHcloud may be obligated to pay a greater amount of interest than currently anticipated. If OVHcloud is not able to successfully hedge against the risks associated with currency fluctuations, its operating results could be harmed.

All of the foregoing could adversely affect OVHcloud's financial position, operating results and cash flow.

Management of the risk

In order to limit the risks posed by currency and interest rate fluctuations and their potential impacts, OVHcloud uses simple and unstructured hedging instruments. Forward purchases of US dollars are regularly made to cover future expenses in this currency over the next 12 months.

In addition, as of 31 August 2022, two interest rate swaps were set up for a total amount of €375 million to fix part of the interest rates on the Company's debt.

Risks related to fraud

Description of the risk

OVHcloud could be the victim of external or internal fraud that could have a negative impact on the Company's finance results. This potential fraud could be a willful act, inappropriate use of the Company's assets or non-compliance with laws or regulations, by an employee or an external party.

Management of the risk

OVHcloud has implemented internal control procedures, which are reviewed by external auditors. Dedicated validation flows have been set up to control and monitor the issuance of credit notes and a team is responsible for monitoring and anticipating potential payment fraud.

In addition, OVHcloud has set up an internal reporting procedure that allows any Group employee to report, anonymously if they wish, any inappropriate or illegal behaviour, including behaviour constituting fraud or attempted fraud.

Inflation-related risks

Description of the risk

In an economic context of sharply increasing inflation, OVHcloud could suffer direct negative effects on its financial profile and deteriorate its margins. OVHcloud is particularly exposed to the increase in electricity costs, which are expected to increase for the 2023 financial year. The Company may not be able to pass sufficiently significant price increases to its customers to cover the widespread increase in its cost base.

Management of the risk

Thanks to its vertically integrated model, which limits the number of suppliers, OVHcloud has the ability to directly control some of the costs related to the production of servers and data centre management. In addition, the Company continues to improve its purchasing policy and logistics strategy in order to compensate for potential increases.

OVHcloud has an active strategy of hedging its electricity costs. As of the date of this Universal Registration Document, the Group knows the cost of nearly 90% of its electricity consumption for the 2023 financial year. Despite this hedge, electricity costs are expected to increase for the 2023 financial year. The Company expects them to be between 5% and 10% of its revenue (mid to high-single digit) for the 2023 financial year.

The Group has announced gradual price increases, in line with cloud industry-wide rises, which will enable OVHcloud to maintain its 2023 adjusted EBITDA margin in line with 2022.

All of the foregoing could adversely affect OVHcloud's financial position, operating results and cash flow. In addition, any further deterioration in the economic environment may have an impact on the Company and its financial position.

2.1.2.5 Legal and compliance risks

Risks related to non-compliance with certain laws and regulations

Description of the risk

Laws and regulations governing data privacy and protection and data sovereignty requirements are rapidly evolving, extensive, complex and include inconsistencies and uncertainties. As an example, the following is a non-exhaustive list of European and international texts whose provisions are likely to have an impact on OVHcloud's organisation and activities:

- the European directive on measures intended to ensure a high common level of security for networks and information systems in the European Union (the "**EU**") (directive EU/2016/1148), transposed into French law on the 26 February 2018, and imposing significant cybersecurity protection requirements on digital service providers such as OVHcloud;
- the General Data Protection Regulation ("**GDPR**") (EU) 2016/679 of 27 April 2016, which entered into force in May 2018 establishing requirements for the processing of personal data of EU residents, which impacts the activities of OVHcloud and its customers; and the violation of which may result in administrative fines of up to €20 million or 4% of the overall annual revenue of the data controller for the previous year;
- the regulation on an internal market for digital services (commonly known as the "**Digital Service Act**" or DSA), adopted on 4 October 2022, reinforces OVHcloud's obligations in terms of the treatment of illegal or potentially dangerous content;
- The European regulation, commonly known as the "**Digital Market Act**" (DMA), was definitively adopted on 14 September 2022 and develops a binding framework in favour of European innovation, in particular through competition and interoperability rules for the major platforms considered to be gate keepers; OVH is not such a gate keeper and would not be directly impacted at first, but could be in the future. OVHcloud will monitor changes to this regulation in order to comply with any obligations that may be imposed on it in the future;
- The European regulation known as the "**Data Governance Act**" (or DGA) adopted in July 2022 and which provides a framework for the reuse of data held by public administrations and whose operational implementation is expected in September 2023. As these administrations are customers of OVHcloud, the latter may be subject to indirect effects;
- The draft European **Data Act** regulation, which aims to complete the European systems in terms of the single data market and data protection, and which would provide, in particular, the possibility of changing cloud services free of charge;
- The draft CSAM Regulation (for "Child sexual abuse material"), which aims to better combat child abuse, particularly on electronic communication networks, and could consequently subject OVHcloud to new or strengthened obligations in this area, it being specified that since 2004, OVHcloud is already subject to specific obligations under the French law on confidence in the digital economy;
- The draft regulation on Digital Operational Resilience for the Financial Sector, proposed by the European Commission on 24 September 2020, which would if adopted impose a number of requirements on cloud outsourcing arrangements in the financial sector, including subjecting OVHcloud to audits, inspections and other supervision by financial regulators, and potentially to significant fines in case of non-compliance with its obligations; and
- The United States Clarifying Lawful Overseas Use of Data Act (the "**Cloud Act**"), which was signed into law in March 2018, which (i) allows US law enforcement to access electronic information held by cloud companies subject to US jurisdiction, even if that information is located outside of the United States; and (ii) enables the US government to enter into agreements with foreign states that would allow the participant states to request information held by cloud companies subject to the partner country's jurisdiction.

OVHcloud also monitors developments concerning the legislative or regulatory frameworks relating to the transfer of personal data outside the EU, in particular following the cancellation of the Privacy Shield, by the European Court of Justice on 16 July 2020. This cancellation has the effect of making the transfer of personal data from Europe to the United States more restrictive, as this country cannot guarantee a level of protection of personal data equivalent to that offered by the GDPR. This circumstance has a direct impact on the data sovereignty issues defended by OVHcloud.

On 25 March 2022, the European Commission and the United States announced the signature of an agreement in principle to adopt a new regulation governing the transfers of personal data to the United States. Such an agreement would have the effect of easing the legal constraints surrounding these transfers and facilitating the use of American entities by European companies, particularly in terms of hosting, thus impacting OVHcloud's activity. A decree implementing this agreement has already been adopted by the President of the United States in October 2022, but this decree will probably be submitted to the European Court of Justice for analysis. In addition, the European application texts remain to be adopted.

In addition to these specific laws, OVHcloud must ensure compliance with the legal rules applicable to all companies (rules of the French Commercial Code, Sapin 2 law, etc.).

Management of the risk

OVHcloud has an internal organisation that makes it possible to anticipate and mitigate the risks related to changes in, or even non-compliance with, the applicable legislation. This organisation relies in particular on the Legal Department, the Data Protection Officer (DPO) and the teams in charge of legal compliance. In addition, the Company commissions external audits to ensure compliance.

The Company also complies with the latest important regulations such as GDPR and Sapin 2.

In order to ensure compliance with the applicable legislation on personal data protection, OVHcloud has adopted various procedures.

Thus, for example, following the opening of its American subsidiary, OVHcloud has drawn up procedures to prevent the transfer to this subsidiary of data stored on OVHcloud's European servers, and contractual provisions stipulating that OVHcloud's customers are primarily responsible for most regulatory compliance. However, OVHcloud cannot be certain that its procedures or contractual protections will be fully effective, with the result that it may inadvertently breach certain of these regulations. Potential monetary penalties for violations are significant, and if applied to OVHcloud could have a significant impact on its financial position. In addition, any actual or reported violation of data protection or privacy regulations could impact OVHcloud's reputation and its business and income.

Risks related to regulatory changes

Description of the risk

OVHcloud believes that one of its competitive advantages, as a European cloud service provider, is that it can offer European customers assurances that they can limit their own data protection and privacy compliance risk by using OVHcloud's services, rather than those of competitors located in other territories or subject to legislation that does not offer the same protections as European data protection regulations. In particular, OVHcloud believes that data stored on its servers (other than those of its US subsidiary) are not subject to subpoenas or warrants issued by US authorities under the Cloud Act, in contrast to data stored on servers controlled by competitors that are subject to US jurisdiction.

It is not certain that OVHcloud's customers will perceive OVHcloud's data sovereignty advantage as a significant factor in their choice of cloud service provider. Surveys realised by OVHcloud have shown that data sovereignty is becoming more significant for decision-makers at its customers, but that it remains less of a priority than other factors such as performance and price. Moreover, Group competitors may structure their operations so as to be able to provide assurances regarding protection of data from subpoena under the Cloud Act and other relevant issues, in which case OVHcloud's competitive advantage may be less significant than anticipated. For example, Microsoft and Orange have announced a new partnership, which intends to propose a data sovereign cloud solution that, if successful, could increase competitive pressure on OVHcloud.

Moreover, OVHcloud's clients may also become subject to burdensome new tax obligations. If OVHcloud's customers are unable to comply with such regulations or if they determine that compliance or the payment of any applicable tax is too costly, their businesses and financial position might be adversely affected, and they may choose to reduce or to eliminate activities that rely on OVHcloud's services.

Management of the risk

In order to limit the risk related to the Cloud Act, OVHcloud has strictly separated its American activities from the rest of the Group, with differentiated legal and technical organisations. For example, US employees do not have access to customer data located outside the data centres based in the United States.

In addition, the legal and public affairs teams actively monitor regulatory change projects in order to anticipate potential changes.

Despite the measures put in place, the Company cannot guarantee that new laws or regulations would not put its operations at risk.

OVHcloud may not be able to protect its intellectual property rights

Description of the risk

To be successful, OVHcloud must protect its technology and brand in France and other jurisdictions through trademarks, domain names, trade secrets, patents, copyrights, service marks, invention assignments, contractual restrictions and other intellectual property rights and confidentiality procedures. Despite OVHcloud's efforts to implement these protections, they may not protect OVHcloud's business or provide it with a competitive advantage for a variety of reasons, including:

- the failure of OVHcloud to obtain patents and other intellectual property rights for important innovations or to maintain appropriate confidentiality and other protective measures to establish and maintain its trade secrets;
- uncertainty in, and evolution of, legal standards relating to the validity, enforceability and scope of protection of intellectual property rights;
- potential invalidation of OVHcloud's intellectual property rights through administrative processes or litigation;
- third-party commercial strategies consisting of triggering unfounded but very costly litigation in the United States in order to bring about an out-of-court settlement that is less onerous than legal fees alone ("patent trolls" phenomenon);
- any inability by OVHcloud to detect infringement or other misappropriation of its intellectual property rights by third parties; and
- other practical, resource or business limitations on its ability to enforce its rights.

Further, the laws of certain countries may not provide the same level of protection of corporate proprietary information and assets, such as intellectual property, trademarks, trade secrets, know-how and records, as the laws of France. As a result, OVHcloud may encounter significant problems in protecting and defending its intellectual property or proprietary rights abroad. Additionally, OVHcloud may also be exposed to material risks of theft or unauthorised reverse engineering of its proprietary information and other intellectual property, including technical data, data sets or other sensitive information. OVHcloud's efforts to enforce its intellectual property rights may be insufficient to enable it to derive a significant commercial advantage from the intellectual property it develops. Moreover, if OVHcloud is unable to prevent the disclosure of its trade secrets to third parties, or if its competitors independently develop any of its trade secrets, it may not be able to establish or maintain a competitive advantage in the market, which could seriously harm its business.

Litigation may be necessary to enforce OVHcloud's intellectual property or proprietary rights, protect its trade secrets or determine the validity and scope of proprietary rights claimed by others. Any litigation, whether or not resolved in OVHcloud's favour, could result in significant expense to OVHcloud, divert the efforts of its technical and management personnel and result in counterclaims with respect to infringement of intellectual property rights by OVHcloud. If OVHcloud is unable to prevent third parties from infringing on or misappropriating its intellectual property or are required to incur substantial expenses defending its intellectual property rights, its business, financial position and operating results may be materially adversely affected.

Management of the risk

OVHcloud has an internal organisation that mitigates the risks related to the protection of its intellectual property rights or the infringement of these rights.

In this context, it has a legal team dedicated to the protection of its intangible assets, which relies on specialised law firms around the world. In addition, OVHcloud has implemented an ambitious patent filing strategy at the Group level and in several territories, and holds 137 patent families as of August 31, 2022. OVHcloud uses service providers and tools to detect unauthorised use of its distinctive signs (brands, domain names) and its patents in several countries. In addition, OVHcloud bases most of its IT developments on open source licenses in order to limit third-party claims.

2.1.2.6 Systems security risks

Risks related to the interruption of an internal IT system or tool

Description of the risk

Despite ongoing testing of OVHcloud's software and platforms, its cloud offerings could contain coding or configuration errors that can impact the function, performance and security of its solutions and result in negative consequences. Detecting and correcting any errors can be time consuming and costly. Mistakes are likely to affect their ability to function appropriately, integrate or operate correctly. They are also likely to generate internal security breaches in OVHcloud's software or platforms and are likely to adversely affect the market penetration of its cloud offerings.

In addition, OVHcloud may be faced with various causes of interruption of its services such as a malicious act, an obsolete infrastructure problem, an insufficient level of security or the loss of connection to the network. For example, on 13 October 2021, following a human intervention on computer equipment, the OVHcloud network, and therefore the Company's customers, were disconnected from the internet for several minutes.

If OVHcloud experiences errors or delays in releasing its cloud offerings, customers may cease using its offerings and its income could decline. Enterprise customers rely on OVHcloud's cloud offerings and related services to run their businesses, and errors could expose OVHcloud to performance and warranty claims as well as significant harm to OVHcloud's brand and reputation, which could impact its future income and profitability.

Management of the risk

OVHcloud has set up a regular review of its code and its infrastructures by a team of IT auditors, which carries out access and penetration tests of its systems. With regard to OVHcloud's internal IT systems, the Company has set up redundancy of its systems between two data centres, a Business Continuity Plan and a Business Recovery Plan, in order to limit the potential risks of interruption.

OVHcloud has network redundancy and performs regular backups.

Although OVHcloud considers that it has implemented risk management measures, these may prove insufficient to prevent an interruption of services.

Risks related to cybersecurity

Description of the risk

By its very nature, OVHcloud's business depends on providing third parties, most of whom are unknown to OVHcloud, with access to OVHcloud's servers for purposes of storing data and performing processing operations, through systems that can be accessed over the internet. The occurrence of a large-scale cybersecurity incident could significantly disrupt OVHcloud's servers and interrupt its cloud services, as well as lead to a security breach or loss of customer data.

Computer hackers and others may be able to develop and deploy IT-related viruses, worms and other malicious software programmes that could attack OVHcloud's systems, create system disruption and cause shutdowns or denials of service, exploiting potential security vulnerabilities. OVHcloud's servers may also be accessed or modified improperly as a result of customer, partner, employee or supplier malfeasance, and third parties may attempt to fraudulently induce customers, partners, employees or suppliers into disclosing sensitive information such as user names, passwords or other information in order to gain access to OVHcloud's services or control panel, and the data or systems of its customers, suppliers or partners. These risks will increase as OVHcloud continues to expand its business and store and process increasingly large amounts of data and host or manage more of its customers' IT operations in cloud-based environments. The risks are particularly acute in customer segments involving sensitive data, such as financial information and healthcare data.

Because the techniques used to obtain unauthorised access to, or sabotage, IT systems change frequently, grow more complex over time and often are not recognised until launched against a target, OVHcloud may be unable to anticipate or implement adequate measures to prevent such techniques. OVHcloud might not discover any security breach and loss of information for a significant period of time after it occurs. Following discovery, OVHcloud might need to shut down systems and limit customer access to its services, which could adversely impact income or cause OVHcloud to breach its service level agreements (SLAs), in which case OVHcloud could be required to grant service credits to, as well as compensate for the damages sustained by, the affected customers. Security vulnerabilities are from time to time identified by third-party security researchers, who may publish their findings before alerting the system operator. The time between when a security researcher publicly announces a security vulnerability and when the mitigation technique is fully deployed allows for a window for exploitation by those seeking to employ the vulnerability to gain access to OVHcloud IT systems.

OVHcloud could suffer significant damage to its brand and reputation if a cyber attack or other security incident were to allow unauthorised access to, or modification of, its customers' data, other external data or its own data or IT systems, or if the services it provides to its customers were disrupted, or if OVHcloud's servers were reported to have, or perceived as having, security vulnerabilities. Customers could lose confidence in the security and reliability of OVHcloud's servers and perceive that they are not secure, causing a loss of income.

Further, OVHcloud does not directly control the content that its customers store, use or access in its cloud offerings. If its customers or users use OVHcloud's products for the transmission or storage of personally identifiable information and its security measures are or are believed to have been breached as a result of third party action, employee error, malfeasance or otherwise, its reputation could be damaged, its business may suffer, and it could incur significant liability as a result of administrative, criminal or other proceedings. In addition, the costs OVHcloud would incur to address and fix these security incidents would increase its expenses. As a consequence, the occurrence of a significant cybersecurity incident or the perception of an increased cybersecurity risk could materially and adversely impact OVHcloud's operating results and financial position.

OVHcloud uses software (such as antivirus and monitoring and detection tools) licensed from third parties to protect its servers and IT systems from cyber attacks and system breaches. It also relies on third-party virtualisation technology (which allows individual machines to operate multiple "virtual servers") and open source solutions to regulate access to data and processing operations of different customers or of differing levels of sensitivity. Because of its dependence on third party solutions, OVHcloud does not fully control the mechanisms used to maintain the security of its systems. Additionally, if a third party were to cease providing this technology, or if it were to change or increase the price of its offerings, OVHcloud would need to quickly either find another third party provider or develop this technology internally, either of which could increase costs or cause operational interruptions.

As cybersecurity threats and responses evolve, OVHcloud might be required to pay third party providers for updates and enhancements in order to maintain adequate levels of security protection. It might be difficult for OVHcloud to change providers, leaving it with few or no alternatives to paying the fees demanded by its existing third party providers. If the fees payable to third party providers were to increase significantly, OVHcloud's costs could increase, adversely affecting its profitability.

If security systems provided by a third party were to fail to protect OVHcloud's systems or the data or systems of its customers adequately, OVHcloud could suffer cyber attacks or privacy breaches that would impact its income and business reputation, as discussed above. Moreover, OVHcloud might not be in a position to remedy any such failure without assistance from the third party provider, which could result in delays and impact the availability of OVHcloud's systems to serve customer needs. In addition, if a different customer of a third party security solution provider were to experience a cybersecurity incident, even if it is unrelated to OVHcloud's operations, the confidence of OVHcloud's customers could be adversely affected, causing a loss of income.

Management of the risk

OVHcloud has implemented several measures to limit cybersecurity risks, resulting in several certifications such as ISO 27001, SEC 1, SEC 2 or PCI DSS. In addition, the Company has regular contact with the ANSSI (French National Cybersecurity Agency) in order to anticipate new attacks or improve its existing processes. OVHcloud regularly maps its IT risks and carries out cyber attack simulations campaigns for its employees. The results of these tests are detailed in Chapter 3 of this Universal Registration Document.

OVHcloud's architecture and processes are designed to limit the exposure in term of systems and time, but several factors could limit OVHcloud's capacity to sufficiently reduce the risk and a significant impact could occur. OVHcloud's systems continue to evolve, and it is often an early adopter of new technologies; however, its business policies and internal security controls may not keep pace with these changes as new threats emerge.

While OVHcloud seeks to take precautions to guard against cybersecurity incidents, those precautions might prove to be ineffective or fail to prevent significant security breaches. In addition, OVHcloud may be vulnerable to new security breaches that have not yet been identified.

In any event, OVHcloud has also taken out a cyber insurance policy with a leading insurer to cover the effects of a possible cybersecurity incident. The implementation of this insurance was subject to compliance by OVHcloud with binding specifications imposed by the insurer.

Risks related to data protection, loss or theft

Description of the risk

Many data protection and privacy regulations impose stringent requirements on OVHcloud's customers, who must ensure the protection of the information of their own customers, including information stored on OVHcloud's cloud servers. Moreover, ever more stringent regulations are being proposed that could have a significant impact on the technology companies that represent a significant portion of OVHcloud's customer base. If so, OVHcloud could lose income from these customers, and its business and financial position could be adversely impacted.

Management of the risk

OVHcloud regularly organises fake email tests to measure the response of its employees. The results of these tests are available in Chapter 3 of this Universal Registration Document. The Company has classified its data by level of risk in order to determine the access and measures necessary to limit the loss or theft of this data. Lastly, OVHcloud has an organisation, processes and teams dedicated to cybersecurity.

2.1.2.7 Other risks

OVHcloud has entered into, and may continue to enter into, certain related-party transactions

OVHcloud has entered into various agreements with companies controlled by Mr. Octave Klaba, founder of the Company and current Chairman of its Board of Directors, and members of Mr. Octave Klaba's family, who are direct or indirect shareholders of the Company. The Klaba family currently controls the Company.

OVHcloud obtains metal components for the manufacturing of its servers from AixMétal, which is controlled by members of the Klaba family. The premises of OVHcloud's server manufacturing facility, data centre and headquarters located in Roubaix, France, are owned by companies controlled by the Klaba family and leased to OVHcloud.

Although OVHcloud believes that all such arrangements have been negotiated on an arms' length basis and use commercially reasonable terms, it has not obtained proposals for these arrangements from unrelated parties. In addition, OVHcloud's operational flexibility to modify or implement changes with respect to the description or pricing of services provided by related parties may be limited: if an agreement with a related party is terminated, there could be disruptions upon transition, and there can be no assurance that OVHcloud will be able to obtain the same products at the same or lower cost. In particular, if OVHcloud experiences difficulties with the metal components supplied by AixMétal, it may take a significant amount of time to find an alternative supplier able to produce similar components, and there may be an impact on OVHcloud's ability to manufacture and deploy new servers as rapidly as it has historically been able to do so, potentially affecting OVHcloud's ability to serve customer capacity requirements.

In addition, OVHcloud is the main cloud service provider for Shadow, which is controlled by members of the Klaba family. The revenue from contracts signed with Shadow is significant for OVHcloud (representing approximately 2.1% of OVHcloud's income in 2022), and as for all of its customers, OVHcloud cannot guarantee that this revenue is acquired on a permanent basis beyond the contractual commitments in force. Similarly, the capital expenditure generated by these contracts is significant, and their premature interruption would affect the expected return on investment.

OVHcloud may enter into other related-party agreements in the future. These agreements will be subject to the rules of approval provided for by the applicable French law as well as to the internal rules of validation of OVHcloud (in particular approval by the Executive Committee and, where applicable, by the Board of Directors), but it cannot be assured that, individually or as a whole, they would be concluded under conditions similar to those that OVHcloud could obtain from unrelated parties.

2.2 INSURANCE AND RISK COVERAGE

Insurance policies are generally taken out by the Company, on its own behalf and on behalf of its subsidiaries, through a broker mandated to negotiate with the main insurance companies to set up or renew the most appropriate guarantees for risk coverage requirements. Insurance companies are selected on the basis of criteria such as the amount of premiums, the scope of coverage offered, the ability to set up integrated programmes such as master policies, the duration of the commitment, their availability to insure the risks in question in the light of all their other commitments in the segment and market in question, and the ability to offer qualitative support in order to better understand risk management.

OVHcloud adapts its insurance coverage according to the evolution of risks related to its usual activities.

Coverage is normally renewed annually, except for certain one-time contracts taken out for one-time projects covering a specific period. The insurance contracts expiring on 6 and 15 October 2021 and 1 January 2022 have been renewed. The insurance contracts maturing at the end of August/beginning of September 2022 have been extended to cover identical guarantees or reassessed as necessary, until 31 December 2022 in order to harmonise the maturities of all insurance contracts. At the time of publication of this document, OVHcloud has obtained an agreement in principle on the renewal of the insurance policies that expire on 31 December 2022.

Below is a summary of the main insurance policies taken out by OVHcloud. OVHcloud prefers to take out “master” policies in order to pool coverage within the Group. For regulatory or factual reasons, such as the size of a subsidiary, OVHcloud also uses local or “standalone” policies taken out directly by its subsidiaries.

The Group also has insurance policies covering the liability of executives (“D&O” policy), risks relating to office facilities, its car fleet, and the travel of its employees using their own vehicle for business and occasional trips, professional assignments, construction work, installation of equipment or fittings in its data centres or offices or the transport of goods (mainly technological and IT equipment). The Group has numerous comprehensive home insurance policies covering rented homes made available to staff during occasional business trips to the head office, as well as the medical office of doctors also working on behalf of OVHcloud. Through its subsidiaries, the Group also has a number of insurance policies covering property damage, civil and employer’s liability and compensation for employees, offices and international data centres.

2.2.1 Property damage

OVHcloud’s property and casualty insurance policy is based on the principle of “all risks except” covering all non-excluded material damages. The Company has taken out this policy which applies to certain subsidiaries in France, Germany, Belgium and the United Kingdom.

This contract was renewed on 1 September 2021 with AXA, as leading insurer with 35% of the risk shares and seven co-insurers sharing 65% of the remaining risk and according to the conditions of a prevention plan established and extended under the same guarantees until 31 December 2022.At the time of publication of this document, OVHcloud has obtained an agreement in principle on the renewal of the insurance policies that expire on 31 December 2022.

This insurance policy covers, in particular, direct material damage to insured property of accidental origin, including buildings, furniture, equipment and/or rental risks, miscellaneous costs and losses resulting from the covered material damage, financial consequences of civil liability following a fire, an explosion, water damage, attacks and acts of terrorism in France as well as the costs of resumption of activity following the material damage covered and the experts' fees following material damage.

The maximum compensation due for all losses covered (including direct damage, business recovery costs, all coverages, including costs and losses and liabilities) amounts to €140 million per claim. Coverage limits and sub-limits are applicable depending on the nature of the damage suffered or the category of property insured. The deductible for all damages amounts to €3 million. In the absence of the installation of automatic protection in accordance with AXA’s recommendations, this deductible is increased to €15 million for the Roubaix, Gravelines and Strasbourg sites, €6 million for the Croix site and an additional €10 million deductible for the Erith (United Kingdom) and Limburg (Germany) sites, taking the deductible to €13 million, as well as €3 million for the Paris 19th site taking the deductible to €6 million. These deductibles will be reduced to €3 million on completion of an investment programme agreed with the insurers and according to their recommendations, the amount of which is already included in the capital budget for the coming years (see Section 1.4.5 “*Medium-term targets*” of this Universal Registration Document). In addition, at the Roubaix, Gravelines, Strasbourg and Croix sites, the Company must maintain in place three specific complementary fire prevention measures (security guards, fire permits and means of intervention in charge on the premises), failing which the deductible would increase by 100% in the event of a claim. An additional contractual provision to terminate the insurance policy was given to the insurer at the renewal on 1 September 2021. The right of cancellation is conditional on the failure to implement a number of personnel and organisational recommendations or the placing of orders relating to the implementation of complete protection on the Roubaix, Strasbourg, Gravelines, Croix, Erith and Limburg sites, in accordance with the insurer’s recommendations and according to a procedure including the insurer for validating these projects, prior to 31 December 2021. All human and organisational recommendations were carried out successively on 31 December 2021 and 30 April 2022. On 30 April 2022, AXA confirmed that OVHcloud had fulfilled its contractual obligations in terms of risk prevention in accordance with its recommendations, and the early termination option was therefore cancelled.

The exclusions are in line with market standards and include, in particular, late payment penalties, fines, penalties and other criminal sanctions, loss of business and customers, operating losses and damage resulting from epidemics, pandemics or epizootics, as well as costs and losses, operating losses and damage resulting from administrative measures, sanitary measures, total or partial closure or withdrawal of administrative authorisation, impossibility, restriction or difficulty of access.

The amount of the insurance contract premium for the insurance period from 1 September 2022 to 31 December 2022 will be prorated and subject to the increase in insured capital due to the integration of new data centres in the policy.

2.2.2 Civil and cyber liability

"Information technology and communication civil liability and cyber risk management" coverage covers the financial consequences of operational, product, professional and cyber liability for technologies, due to damage caused to third parties (including customers), as a result of, during or at the time of the activities covered by the contracts as well as the financial consequences related to cyber risks. In particular, all sales, services and work concerning the digital industry and internet hosting are insured, such as, among others, the hosting of websites, servers, dedicated servers, shared server leasing, the registration of domain names, data hosting (including health and banking data), the design of software or the manufacture of servers. The combined cyber guarantee includes protection against any breach of its automated data processing systems, its own confidential data and information, as well as the personal and confidential data of third parties, contained and processed in its information systems or in those its subcontractors and external service providers, along with the financial consequences related to a cyber incident and/or an incident disrupting operations, including incident response costs, operating losses, and the costs of restoring the IT system or ransoms and cyber-extortion costs.

This master programme is broken down into three insurance contracts called "lines" in order to obtain sufficient guarantees in terms of "civil liability and cyber corporate risk management" coverage. The second and third lines will be applied in addition to and after the total exhaustion of the underlying lines, by one or more claims during the insurance period, of the cumulative amount of coverage under these contracts.

This insurance policy covers the Company and its subsidiaries, excluding subsidiaries or permanent facilities located in the United States. The Group's US subsidiaries benefit from their own insurance policies. A combined first-line "civil liability and cyber-company" policy has been taken out with Chubb with effect from 1 January 2022 for a one-year period subject to tacit renewal. The maximum amount of compensation for the main risks, all damages combined, under this insurance policy is €10 million per claim for operating civil liability, €5 million per insurance period for professional civil liability and civil liability due to products and €5 million per insurance period and per claim for losses due to cyber risk.

Exclusions are in line with market standards and include, but are not limited to, notification fees, e-threat fees and fees for assistance in the event of an investigation by the data protection authority, fines, penalties and other criminal sanctions, various environmental impairments, or damages resulting from the unlawful collection, retention or use of personal data.

Exclusions are in line with market standards and include, among others, intentional misconduct (except by agents), property damage, failure to comply with specific recommendations of a legally constituted authority, and war and terrorism (cyber-terrorism is covered).

A combined second-line "civil liability and cyber-company" policy was taken out with CNA with effect from 1 January 2022 for a one-year period subject to tacit renewal. The maximum amount of compensation for the main risks, all damages combined, under this insurance policy is €10 million per claim for operating civil liability, €5 million per insurance period for professional civil liability and civil liability due to products and €5 million per insurance period and per claim for losses due to cyber risk.

A third-line "professional civil liability" policy was taken out with Ergo with effect from 1 January 2022 for a one-year period subject to tacit renewal. The maximum amount of compensation for the main risks, all damages combined, under this insurance policy is €5 million per insurance period for operating civil liability, after delivery, works or acceptance and for professional civil liability, all risks combined.

Several deductibles are applicable, including €50 thousand for property damage and immaterial damage and €250 thousand for non-bodily injury, professional liability and civil product liability due to property damage, immaterial damage and bodily injury, including financial guarantees related to cyber risks.

The amount of all premiums for the "civil liability and cyber-corporate" master programme for the insurance period from 1 January 2022 to 31 December 2022 amounts to €838 thousand including tax.

2.2.3 Executives liability and initial public offering

The Company has put in place a specific hedge in order to protect itself against the liability that it and its executives could incur in connection with its business as well as the listing of the Company's shares on the regulated market of Euronext Paris.

The Group has entered into a first-line contract with AXA-XL with effect from 15 October 2021 for a period of one year. The second, third, fourth and fifth line contracts were signed with AIG Europe, BHSI, Beazley and Zurich. The guarantee ceiling under each of these contracts is €10 million.

This contract was renewed on 15 October 2022 for one year, under normal market conditions but will no longer include the guarantee relating to stock market claims related to the IPO, which was only put in place for one year.

2.3 INTERNAL CONTROL AND RISK MANAGEMENT

2.3.1 Organisational framework for risk management

Operational risk management is the responsibility of the Ethics and Compliance and Data Protection Departments, which report to the Legal Department, as well as the Quality, Health, Environment and Information Systems Security Departments, which report to the Operations Department.

Ethics and Compliance

The Group pays strict attention to the compliance of its procedures and employee practices with applicable regulations. The Group has thus deployed ethics and anti-corruption codes with associated training. In addition, the Group raises awareness among its employees of whistleblowing issues, in particular as part of the measures put in place in accordance with the law of 9 December 2016 on transparency, the fight against corruption and influence peddling and the modernisation of economic life (the so-called "Sapin II" law). A platform accessible at all times has been set up on which employees can declare any observed act violating the Group's ethical code: "ROGER" (Respect OVHcloud Guidelines and Ethical Rules).

Data Protection

Under the supervision of its Data Protection Officer (DPO), the Group implements a rigorous personal data protection policy. A policy for the use of personal data has been established which describes precisely the processing that OVHcloud may be required to carry out on data concerning customers, suppliers and partners, as well as the conditions of their implementation.

In the context of the processing operations covered by the personal data use policy, OVHcloud complies, in its capacity as data controller, with the regulations in force, in particular with the GDPR, as well as with any regulations of the Member States of the European Union that may apply to said processing operations, in particular French law No.78-17 of 6 January 1978 relating to data processing, files and freedoms, as amended.

In this respect, OVHcloud undertakes in particular to:

- only collect personal data that are necessary for the above-mentioned purposes;
- implement processes to ensure the accuracy and updating of data used in the context of the said processing, as well as their deletion when they are no longer useful for the purposes pursued;
- not to process personal data in its possession for purposes other than those mentioned in this policy, unless it obtains the consent of the data subjects, or informs them in advance about processing on legal grounds other than consent;
- document the processing operations carried out in a register and carry out all the necessary impact analyses prior to their implementation;
- implement an incident and data breach management process, and in the event of a breach, notify the protection authority under the conditions of Article 33 of the GDPR, and inform the data subjects, in accordance with Article 34 of the GDPR when the breach is likely to result in a high risk to rights and freedoms; as well as
- implement technical and organisational measures to protect personal data against security risks, as defined in OVHcloud's information systems security policy.

Information Systems Security

Information security is the subject of a programme and commitments developed within the OVHcloud Information Systems Security Policy ("ISSP"). This policy puts forward the following principles of application:

- deployment a large-scale, industrial approach to security;
- positioning OVHcloud as a trusted player in the ecosystem;
- operating a secure cloud for all;
- implementation of security management systems (ISMS) and privacy management systems (PIMS);
- risk-based approach to safety;
- demonstration of security through certification, internal control and external audit;
- unified response to security incidents and personal data breaches;
- integration of security and privacy issues into product development; and
- safety assessment and implementation of continuous improvement.

The Information Systems Security Policy ("**ISSP**"), under the responsibility of the Chief Information Systems Officer ("**CISO**"), is reviewed by the Executive Committee, which verifies that its content is consistent with the Group's strategic targets. It is revised once a year. The ISSP applies to all Group companies, employees, suppliers, service providers, subcontractors and users of the information system, regardless of their status.

Under the responsibility of the Chief Information Systems Officer ("**CISO**"), the OVHcloud security team is itself composed of three teams:

- Tool security, in charge of developing and operating the tools supporting the security policy;
- Operations security, responsible for ensuring the implementation of good security practices within operations and the implementation of formal security management processes, supporting the integration of security tools and the alignment of security arrangements within the Company; and
- Security.cert, in charge of monitoring threat sources, identifying cyber attack tools and methods to anticipate them, and managing security incidents.

OVHcloud ensures that employees are aware of the challenges of IT security and, more specifically, of cybersecurity. To this end, the Group regularly conducts cyber attack simulation campaigns (phishing) designed on the basis of sophisticated scenarios. The latest campaigns have shown very good results with a 91% success rate.

Quality, Health, Environment

Through its Health and Safety policy, OVHcloud oversees the implementation of measures to offer safe and healthy workspaces for all its employees and stakeholders, its sites and its products. The Group's industrial risk management policy is based on two axes: (i) prevention through audits carried out by external bodies at each of the sites, which result in reports with both human and material recommendations, and (ii) protection through the development of risk reduction plans, incorporating short- and medium-term investments as well as organisational or management actions.

Finally, the Company's Audit Committee plays a role in risk management and internal control. It ensures the relevance, reliability and implementation of the Company's internal control, identification, hedging and risk management procedures relating to its activities and financial and non-financial accounting information. The Group's risk mapping and the action plans implemented are reported twice a year by the Group's Chief Financial Officer.

2.3.2 Internal control

This Universal Registration document, which includes the management report of the Company's Board of Directors to the General Meeting, includes information on the internal control and risk management procedures implemented within the Company, pursuant to the provisions of Articles L. 22-10-35 of the French Commercial Code, and on how the Company takes into account the social and environmental consequences of its business, as well as its social commitments to sustainability, diversity and anti-discrimination, pursuant to the provisions of Articles L. 225-102-1 and L. 22-10-36 of the French Commercial Code.

2.3.2.1 Definition and targets of internal control

In order to address the risks identified and presented in the previous section, OVHcloud has adopted a governance, rules, policies and procedures constituting its internal control and risk management system.

Internal control system

In accordance with the AMF reference framework, under the responsibility of the Group Chief Executive Officer, the internal control system in force within the Group is based on a set of appropriate resources, policies, behaviours, procedures and actions, to ensure that the necessary measures are taken to control:

- compliance with applicable laws and regulations;
- the application of instructions, guidelines and rules set by management;
- the proper functioning of the Company's internal processes, in particular those contributing to the protection of its assets;
- the quality and reliability of financial and accounting information.

Risk management system

The risk management system aims to identify, analyse and manage the Company's main risks.

More generally, the Group's internal control and risk management system contributes to the control of its activities, the effectiveness of its operations and the efficient use of its resources. This system is updated regularly, according to a continuous improvement process, in order to better measure the level of risk to which the Group is exposed, as well as the effectiveness of the action plans put in place to address it.

The internal control and risk management system cannot, however, provide an absolute guarantee that targets will be achieved and the total elimination of risks, in particular:

- cases of deliberate collusion between several people that evade the control system in place;
- cases of deliberate management fraud;
- in the event that the implementation or even the maintenance of a control would be more costly than the risk it is supposed to mitigate;
- in addition, in the pursuit of the aforementioned targets, it goes without saying that companies are confronted with events and uncertainties that are beyond their control (unforeseen changes in markets and competition, unforeseen changes in the geopolitical situation, etc.).

2.3.2.2 General organisation and internal control procedures

The internal control environment is based in particular on the values governing the behaviour and ethics of the Group's employees and third parties. In order to disseminate these values, the Group has implemented the following charters and code of conduct:

- Code of ethics and anti-corruption governing the rules of behaviour of employees and also of partners/suppliers;
- Reporting platform that makes it possible to report any behaviour contrary to the ethics framework and any serious situation or fact observed in the company or at our partners/suppliers in all confidence and confidentiality;
- OVHcloud's values shared by all employees, including the obligation to act responsibly and ethically. These founding values contribute to the dissemination of a respectful corporate culture;
- IT and communication and security charters including all rules and best practices in terms of physical and logical security of the Group's IT resources by users;
- Stock market ethics charter, implemented in 2021, in accordance with the AMF instructions, defines the obligations of persons holding inside information.

In addition, the organisation of internal control relies on various players throughout the decision-making and responsibility chain, in particular employees, the Executive Committee along with supervisory bodies such as the Board of Directors and the committees. The Company's Audit Committee plays a role in risk management and internal control. It ensures the relevance, reliability and implementation of the Company's internal control, identification, hedging and risk management procedures relating to its activities and financial and non-financial accounting information.

Internal control is based in particular on:

- The Group Legal Department advises and assists the operational departments and subsidiaries on significant legal matters;
- The Group Tax Department advises and assists the operational departments and subsidiaries on significant tax matters;
- The Group Financial Operations Department ensures the implementation and compliance with the reporting and preparation procedures of the consolidated financial statements;
- The Group Human Resources Department advises and ensures that internal practices comply with laws and regulations relating to employment law;
- The Group Operations Department carries out specific risk analyses and proposes action plans in terms of security, safety and business continuity.

Finally, the statutory auditors are informed of the internal control system and the risks identified by the Group in the assessment.

2.3.2.3 Internal control procedures relating to the preparation and processing of financial and accounting information

OVHcloud's accounting and financial function is managed by the Group's Finance Department, which reports directly to Senior Management.

The Group Finance Department's responsibilities mainly cover the preparation of financial statements, management control, taxation, financing and cash management, and participation in financial communication and purchases.

The IFRS accounting rules and methods in force within the Group are presented in the notes to the consolidated financial statements in this document. At each accounting close, the Audit Committee ensures that they are kept with the Finance Department and the statutory auditors.

Each half-year, after review by the Audit Committee, the Board of Directors approves the half-yearly and annual financial statements which the statutory auditors are asked to approve.

Information systems

The purpose of the accounting and financial information systems deployed within the Group is to meet the requirements of compliance, security, reliability, availability and traceability of information.

OVHcloud is gradually rolling out SAP as the only information and management system for financial management and accounting data. During the 2022 financial year, the Group rolled out SAP in its main subsidiaries in France, Canada and the United States. The roll-out in other regions will continue during the 2023 financial year. The use of a single tool ensures consistency in the processing, comparison and control of accounting and financial information. In addition, OVHcloud uses ViaReport for consolidation data.

In order to strengthen the internal control of the systems, the Organisation and Information Systems Department has strengthened the segregation of duties system and improved access rights controls, through a formal annual review across the entire Group scope.

Financial communication

The Financial Communication and Investor Relations Department, under the supervision of the Chief Financial Officer, manages the Group's financial communication.

The Group disseminates financial information by various means, in particular:

- press releases;
- the Universal Registration Document;
- the presentation of the half-year and annual results.

The Group's website has a dedicated Investors section which includes the aforementioned items as well as other regulatory or informational items.

The statutory auditors

As part of their mission to certify the financial statements, the statutory auditors make comments. At the time they deem appropriate, the statutory auditors communicate to management, at the appropriate level of responsibility, the internal control weaknesses identified during the audit that they deem of sufficient importance to merit its attention, except if they consider this approach inappropriate in the circumstances. They make this communication in writing when it concerns weaknesses that they consider to be significant. The statutory auditors communicate any significant weaknesses in internal control to the bodies mentioned in Article L. 823-16 of the French Commercial Code, at the time they deem appropriate, in writing.

As part of their ongoing mission, the statutory auditors audit the annual and half-yearly financial statements and statements of consolidated entities. The Group's annual consolidated financial statements are prepared by the Financial Operations Department under the responsibility of the Group's Chief Financial Officer. The Group's Chief Executive Officer and Chief Financial Officer certify the regularity, sincerity and fair presentation of the consolidated financial statements by signing a confirmation letter sent to the statutory auditors.


DREAM
INTO THE
CLOUD