



Sustainability **Report 2022**

Environmental, Social and Governance Report

Contents

Message from the Chief Executive Officer	01	6 Ethics, fair practices, compliance and security	58
Foreword	01	6.1 Compliance governance and organisation	58
1 Business model	02	6.2 Ethics, prevention and anti-corruption	59
1.1 Our business model	02	6.3 Cybersecurity governance and organisation	63
1.2 Our human values	04	6.4 Information system protection	64
2 Risks and opportunities	05	6.5 Data protection	66
Introduction	05	6.6 Transparency and the fight against tax avoidance	67
2.1 Risk factors	07	6.7 Export control	67
2.2 Internal control and risk management	20	7 Other regulatory issues	69
2.3 Materiality analysis of sustainability issues	26	7.1 Respect for human rights	69
3 Our key performance indicators and results	29	7.2 Collective agreements	70
4 Attracting and retaining talent	30	7.3 Societal commitments to the circular economy	70
4.1 Cybersecurity – a sector with a severe skills shortage	30	7.4 Food, food waste and food insecurity; animal welfare	71
4.2 Human Resources mission and organisation	31	7.5 Physical and sports activities	71
4.3 Employee commitment	33	8 Methodology note	72
4.4 Performance and talent programme	34	8.1 Scope of consolidation	72
4.5 Training and skills development	35	8.2 Methodological information on indicators	76
4.6 Exclusive Academy: tomorrow's skills	36	8.3 Extra-financial performance statement/ GRI/SDG cross-reference table	78
4.7 Diversity, inclusion, equity and equal opportunities	36	9 Opinion of the independent notified body	83
4.8 Health and safety	39		
4.9 #WeAreExclusive	40		
5 Environmental footprint	43		
5.1 Energy consumption	43		
5.2 Carbon footprint	44		
5.3 Other environmental indicators	50		
5.4 Green Taxonomy	51		

Message from the Chief Executive Officer

Our vision of a totally trusted digital world is our ambition, guiding us daily in our activities and actions. This ambition comes together with responsibility and commitments to becoming a sustainable, socially conscious and responsible company, for the benefit of our business partners, employees and the communities where we operate, and with respect for the environment.

As a global cybersecurity company, helping to protect the digital infrastructures that power many of today's businesses, economies, and societies, we have a sharp perspective on the interconnected nature of the world we live in. Cyber threats can have direct impacts on the activities of companies, the operations of public entities, and as a result, on citizens. Protecting against them requires vigilance, robust technical solutions, action and integrity.

So, we understand the importance of environmental, social, and governance (ESG) factors in building a sustainable business. ESG considerations are critical in not only mitigating risk, but also driving innovation, improving performance, and creating long-term value for all stakeholders.

No company can achieve its business ambitions and ESG challenges alone. We operate within a complex ecosystem and value chain and use our energy and influence to provide solutions to bring about positive impact.

That's why we are committed to collaborating with all our stakeholders to drive systemic change. We are proud to be part of a growing community of like-minded organizations, that place ESG considerations at the heart of their business, and work in partnership to contribute to a sustainable future. The Exclusive Academy, a tangible and concrete step towards addressing the skills gap in the cybersecurity sector, is a good example of the initiatives and impact we want to make.

We know that this is just the start of a long journey and there is much to do. Therefore, we'll continue to make ESG a key focus and priority. There are many challenges ahead, and we are ready to meet them alongside business partners and employees, who share our commitment to ESG principles. Together, we work together to move toward a totally trusted, digital, and sustainable future for all.

Jesper Trolle

Foreword

Following its Initial Public Offering on 23 September 2021, the Exclusive Networks Group is publishing in its Universal Registration Document, in addition to its management reports, its second Sustainability Report

or Extra-Financial Performance Statement, which aims to report on how it addresses the social, societal and environmental consequences of its activities.

Business model

Our business model

1 Business model

1.1 Our business model



Vision

We believe that everyone is entitled to live in a digital world made safer by the most innovative technology.



Resources

Experienced, highly qualified employees from a wide range of backgrounds

2,411 employees

43% of employees are women

1:2 ratio one technical engineer for every two sales people

Best-in-class vendor portfolio

> 260 vendors

Exclusive Networks vendors are recognised by Gartner as market leaders in key sub-sectors

Ability to identify, attract and develop the leaders of tomorrow: 50 companies analysed each year and 10 welcomed on board

Global and local presence

Offices in 47 countries

Over 170 countries covered

Access to a large and diverse network of partners: > 25,000

Several system integrators, including the 20 largest in the world

Proven industry consolidation platform

18 acquisitions during the last decade to support and accelerate the growth strategy

Strong track record of profitable growth

Gross sales: +33% CAGR

116% net customer retention rate over the last three years

37% EBITA margin

Asset-light model: > 90% average cash conversion over the last three years

Unique

Best-in-class product portfolio and services

Five strategic pillars



Take advantage of the underlying growth enjoyed by our vendors and the cybersecurity market in general within existing geographical areas of operation



Enable new vendors to set up in our regions
Increase our potential



market by adding new geographical areas and consolidating under-represented areas by way of mergers and acquisitions



Mission

Thanks to our global platform, our commercial nous and the technical expertise of our teams, we accelerate adoption of the most innovative cybersecurity technologies by putting security companies in touch with thousands of organisations all around the world.

We allocate time and resources to raising awareness of inherent cyberspace risks, and we invest in training the security experts of tomorrow.

positioning

A local perspective backed by a global organisation



Develop our range of services so that we can diversify all along the value chain and enhance customer retention



Adopt the transition towards the cloud by:

- a. Partnering with the main vendors of cloud security software.
- b. Deploying the appropriate commercial proposition and suitable tools/platforms.

Value creation

Societal impact

Launch of **Exclusive Academy** in October 2022, 20 participants, three-year programme: a response to the severe shortage of skills and talent in the cybersecurity sector

Economic impact

Make businesses more **competitive** by reducing the risk of cyberattacks

Facilitate the **digital transformation**

Track-record of accelerating acquired companies' growth: **achieving synergies** by sharing technical and commercial expertise

Partners

Provide partners with **new revenue streams** in a constantly evolving technological environment

Offer **high-quality** training for partners and end-customers: vendor technology training

Over 11,000 professionals trained in 2022

Vendors

Ability to accelerate their **international expansion**

Extensive range of services enabling them to optimise their marketing costs and processes

76 vendors added over the last five years

Employees

Engagement rate of **72%** as per the employee engagement survey of 21 April

Financial performance

- **Gross sales** above €5,150 million
- **Net margin** in the range of €450 million to €465 million
- **Adjusted EBIT** in the range of €172 million to €178 million
- **Operating FCF, adjusted** above 80% of adjusted EBITDA

1.2 Our human values

Our human values are described in our Code of Conduct, which we distribute to all our employees when they join.

Our People Values People focused

We care for our people :

- Do things to help other people without expecting any reward for yourself
- Identify times when someone else needs your support and provide it

Experts

We grow our own experts

- Create your own development plan and carry out planned activities
- Support others' development activities
- Help others identify development opportunities
- Encourage your team members / direct reports to apply for suitable internal opportunities

Fun

We build fun into what we do

- Look for ways to make work fun
- Arrange events that are fun for others
- Join in with social events that others plan
- Encourage others to join in with social events

Trust

Our relationships are built on trust

- Positively challenge to understand a situation more clearly but believe the information that your colleague is telling you
- Keep your promise to a colleague to complete the task you said that you would
- Trust colleagues or reportees to do what they promise they will do
- Delegate tasks appropriately to colleagues or reportees and trust that they will do it

Responsive

We are responsive to the needs of others

- Respond quickly to requests from others for information or support to get their work done

2 Risks and opportunities

Introduction

The Group conducts its activities in an international economic and political environment that was notably marked in 2022 by a tense geopolitical context, an acceleration of inflation and the tightening of monetary policy by central banks. The evolution of the Covid-19 pandemic and its uncertainties (intensity, governmental measures taken in this regard – lockdown, curfew etc.), as well as conflicts and economic crises could have a significant impact on the Group's activities, results, financial situation, reputation or prospects.

Risk analysis and management are an integral part of the Group's various decision-making processes. They are structured around four main stages: risk identification, prioritisation, management and monitoring.

As part of its risk management system, the Executive Committee periodically reviews the main risks, which are reported by the various operational departments (see below, section 2.2 "Internal control and risk management").

Pursuant to the Prospectus Regulation, the risks presented below are identified as the most significant and specific to the Group that could have a material impact on its business, financial condition, reputation, results of operations or growth prospects as at the date of the 2022 Universal Registration Document.

These risks were submitted to the Executive Committee and the Audit Committee, which, after consultation and based on their impact, agreed on the main risks. These risks were then validated by the Board of Directors on the recommendation of the Audit Committee.

The selected risks are presented in a limited number of categories by type. Within each category, the most significant risks are presented first. Risk assessments are conducted while taking into account the probability of occurrence and the expected magnitude of their negative impact.

As a result of the last update of the risk map in 2022, action plans for each risk have been implemented and/or updated. The update of the risk map in 2023 will make it possible to assess the results of the risk management measures and to present the net risk in the future.

The main risks described in section 2.1 "Risk factors" below include social, environmental, societal and governance risks, identified with a pictogram [ESG](#).

Although climate change does not appear among the major risks described in this section, the Exclusive Networks Group is fully aware of its wider responsibility within its ecosystem. The Group's greenhouse gas assessment clearly reflects this situation, with a very high proportion of the Group's emissions falling under Scope 3, both upstream and downstream in its value chain. The Group is committed to playing its full part in addressing climate change.





Investors should note that the list of risks presented below is not exhaustive and that other risks of which the Group is currently unaware or which have not been identified as significant as at the date of the 2022 Universal Registration Document may exist, and if they were to materialise could have a significant impact on the Group, its activities, its financial situation, its results, its ability to achieve its objectives or its reputation. It should be noted that no new critical risks were identified during the 2022 financial year.

Risks and opportunities

Introduction

The most important risks, specific to Exclusive Networks, are presented below, by category and in descending order of criticality level (based on a combination of the probability of occurrence and the expected magnitude

of their negative impact). The table below presents the result of this assessment on a scale of three criticality levels: high, average or low.

Category	Risks	Criticality
 Strategic and market risks	Risk related to macroeconomic and political conditions	■ ■ ■
	Risk related to the supply of products and solutions distributed by the Group	■ ■ ■
	Risk related to acquisitions & integrations	■ ■ ■
	Risk related to the Group's ability to maintain a portfolio of products and services tailored to demand	■ ■ ■
	Reputational risk	■ ■ ■
 Risks related to operations	Risk related the attractiveness and/or loss of talent and executives ESG	■ ■ ■
	Risk of cyber-attacks, systems security, data protection ESG	■ ■ ■
	Risk related to vendor concentration	■ ■ ■
 Financial risks	Foreign exchange risk	■ ■ ■
	Interest rate risk	■ ■ ■
	Liquidity risk	■ ■ ■
 Legal and regulatory risks	Risk related to export control regulations and sanctions regimes and embargoes relating to economic sanctions on dual-use products ESG	■ ■ ■
	Risk related to corruption (business ethics) ESG	■ ■ ■
	Tax risk	■ ■ ■
	Risk related to litigation and disputes	■ ■ ■
	Risk related to personal data breach ESG	■ ■ ■

Criticality: ■ Low ■ Medium ■ High

2.1 Risk factors

2.1.1 Strategic and market risks

Risk related to macroeconomic and political conditions

Criticality level: 

Risk description

Due to its global footprint, the Group is exposed to the risks of global macroeconomic instabilities and political tensions.

International tensions (e.g. China-Taiwan relations, China-US tensions, and the Russian-Ukrainian conflict) may lead to a deterioration in the business climate and could result in increased trade barriers or international sanctions. This was the case in the trade war between the US and China on the one hand and the EU on the other. The sanctions adopted by the West against Russia could be broadened.

Continued economic uncertainty in many countries, as well as instability in the emerging markets in which the Group operates, continue to fuel a tense global economic environment. In particular, the Group is impacted by freight costs downstream and upstream of the products it distributes.

At the time of publication of the 2022 Universal Registration Document, the direct impact on the Group's business of the conflict between Russia and Ukraine, and the related European, American and British sanctions, remains limited. The Group is not present in Russia, Belarus or Ukraine and has no significant revenue nor margin from those countries. Furthermore, none of its major vendors or partners are expecting a significant business disruption due to the conflict. The main area of concern for the Group remains the impact of the conflict on the economies of the Eastern European countries where the Group operates, in particular Poland, Romania and Hungary.

The Group is nevertheless suffering from the backlash of a war situation and the inherent costs (inflationary pressure fuelled by soaring energy (about +7% to 9% over one year in the euro zone) and raw materials prices, higher cost of solutions offered to customers).

These conditions may lead to adverse consequences for the Group such as reduced demand for cybersecurity solutions and services in general, increased competition, lower prices, loss of vendor rebates, extension of customer payment terms, increased bad debts, limited access to liquidity, increased currency volatility making hedging more expensive and difficult to obtain).

Risk management

These critical or tense situations are the subject of action plans that are used to support decision-making with regard to the Group's development.

In this respect, to mitigate the impact of an unfavourable change in the economic or political situation of a country in which the Group operates, the Group has put in place the following measures:

- the review by the Executive Committee of developments in the most exposed countries where the Group, its customers and vendors are present (see below, "Risk related to the supply of products and solutions distributed by the Group");
- monitoring at Executive Committee and operational level of existing tensions between China and the United States over Taiwan, in particular the additional restrictive measures taken by the United States with regard to China and the newly targeted entities and persons (see section 2.1.4 "Risks relating to export control regulations, sanctions regimes and embargoes concerning economic sanctions applicable to Dual-use products") of this Chapter 2.

 Risk related to the supply of products and solutions distributed by the Group

Criticality level: 

Risk description

The Group depends on the sourcing strategy of its vendors of the products it distributes.

Since 2020, the supply chains of IT industries (including those of the Group's partner hardware manufacturers) have been heavily impacted by the shortage of electronic components needed for the solutions distributed by the Group. These solutions are often manufactured in Taiwan and imported from China. For example, Fortinet's hardware sales (sourcing from Taiwan) represent 15% of the Group's total 2022 revenue.

The shortage of electronic components affected the Group's supply capacity and caused significant delays in its ability to distribute cybersecurity products and solutions.

Additionally, as described in section 2.1.1 which describes the risks related to macroeconomic and political conditions, the increase in inflationary pressure has resulted in a significant increase in freight costs due to the rise in energy costs.

Risk management

The Group has implemented a number of measures to mitigate this risk:

- adjustment of its logistics infrastructure and strengthening of inventory management in conjunction with key vendors, including:
 - the development of regional inventories for key vendors to improve product availability and cut delivery times,
 - the safeguarding of transport capacity and service levels and related costs (strengthening of partnerships with carriers with their own aircraft fleet),
 - strengthening collaboration with vendors in sharing *forecast* and sales pipeline data to secure product availability;
- currency hedging: see below, "Foreign exchange risk" described in section 2.1.3 "Financial risks" of this Chapter 2.

Risk related to acquisitions & integrations

Criticality level: 

Description

As part of its development strategy, the Group has made 18 acquisitions since its inception, including two in 2021. These acquisitions are one of the Group's strategic pillars that have enabled it to strengthen its strategy towards emerging vendors and its geographical presence. For example, the acquisition of Ignition Technology has enabled the Group to offer a targeted proposition to emerging security vendors while the acquisitions of Veracomp in 2020 and Networks Unlimited in 2021 have enabled the Group to expand into Central and Eastern Europe and Sub-Saharan Africa.

The main risks associated with these acquisitions relate to:

- *due diligence* that is sometimes incomplete due to difficulties in gathering certain targeted information and/or the unavailability of such information. Furthermore, the Group cannot guarantee that the documents and information examined during these audits are complete, appropriate or accurate. In particular, it is difficult to guarantee that this due diligence has made it possible to identify all the risks related to possible litigation of the acquired companies, or to possible breaches of applicable anti-corruption regulations;
- over- or under-estimated financial valuations of certain assets, which lead to the recognition of accounting discrepancies. Despite an in-depth analysis of each target, their valuation and the assumptions concerning them were sometimes found to be inaccurate and their actual performance different from the results initially expected;
- human risks related to the integration of employees of acquired companies and their adaptation to the human resources policy and working environment of a large group;

Risk management

The Group has a dedicated M&A department which is responsible for (i) analysing opportunities in terms of strategic rationale, value creation and risks for the Group; (ii) fulfilling the opportunities approved by the respective management bodies (Executive Committee and Board of Directors); and (iii) coordinating the integration within the Group.

The Group has a formal and centralised process for its acquisitions and integrations. This process is spearheaded by Executive Management, with contributions mainly from the M&A, Finance, Legal and Human Resources Departments. This process includes in particular:

- preliminary audits of each target in as many areas as possible depending on the target, carried out by a multidisciplinary internal team (experts in the area audited) and external advisers who review all the elements provided to them by the target. Management sessions with the target's management are also organised to ensure that the target's business and identified risks are properly understood;
- the creation of dedicated committees with the corresponding contacts by level and department at a frequency adapted to the phase of the acquisition project;
- the usual legal protections in acquisition contracts, in particular asset and liability guarantees;
- the Executive Committee examines all acquisition opportunities (rationale, business plan, value creation, risks etc.). These opportunities are regularly presented to the Board of Directors;

.../...

Risk related to acquisitions & integrations

Criticality level: 

Description

.../...

- operational risks due to the need for a high level of team involvement to successfully integrate the acquired companies, which may have a negative impact given the additional workload this generates and the ability of these teams to carry out their daily activities.

Risk management

- the implementation of an integration process and methodology coordinated by the team in charge of integrations covering all operational, financial, social and legal aspects. They include, among others:

- on the financial side (i) the implementation of a business plan validated by the managers, the chief operating officer and the chief financial officer concerned in the Group, (ii) an integration manual detailing the necessary actions to be implemented in terms of reporting and financial monitoring with the support of the Group's Finance Department and (iii) an integration plan relating to internal control. The integration plan is supervised by a specific committee including the Group chief financial officer, the Group Human Resources Director and the operational manager for the area.

In accordance with IFRS, the Group Finance Department assesses the value and measures any impairment of goodwill each year. The net book value of goodwill amounts to €295 million. Impairment tests are carried out and monitored by the Group's Finance Department and presented in Note 7.2 – Impairment Tests to the 2022 consolidated financial statements in Chapter 5 of the Universal Registration Document,

- on the personnel front, the Human Resources Department and HR managers are responsible for applying a progressive policy of adapting the targets' employees to the Group's policies and procedures in terms of training, compensation and integration,
- legal integration and risks & compliance.

Risk related to the Group's ability to maintain a portfolio of products and services tailored to demand

Criticality level: 

Risk description

As part of its mission, the Group must constantly offer the most relevant solutions that meet the requirements of the market and the needs of its customers. In this respect, the Group depends on the ability of vendors to (i) keep ahead of technological changes, (ii) introduce and improve their products and services, and (iv) adapt to industry standards.

New violations of IT system infrastructures are occurring with ever-increasing regularity, as cyber-criminals become more and more adept at exploiting new "techniques", breaching vulnerabilities and devising other methods of attack.

Vendors of cybersecurity consequently make every effort to anticipate and counter these attempts with equally ingenious solutions. The deployment of such solutions can nevertheless be extremely time-consuming, and a hundred or more new start-ups appear in the cybersecurity business every year.

The approach developed by Exclusive Networks is not only to understand the market but also to anticipate the needs of its partners and their users. To this end the Group has set up a Technology Watch Committee (see opposite).

Any inability of a vendor to anticipate industry trends and/or adapt to market needs could have a material adverse effect on the Group's business.

Risk management

The Group has implemented a process for identifying and managing its vendors which includes:

- the creation of a Technology Watch Committee which reviews *the quality* of the technological value propositions of potential new vendors. The role of this Technology Watch Committee is to propose the best market access for Exclusive Networks and its vendors.

The Technology Watch Committee includes technical members from the major countries and/or regions, the chief strategy officers of Nuaware and Ignition, and the Vice-President Global Alliances and Ecosystem, who is a member of the Executive Committee;

- the creation of a Technology Committee, which reviews the quality of the solutions sold;
- a process of integration of new vendors which ensures the roll-out of solutions to the Group's partners/clients;
- a strategy for analysing the situation of existing vendors, which makes it possible to closely monitor their performance with the Group's clients and which can be accompanied by internal improvement plans if necessary.

Reputational risk

Criticality level: 

Risk description

The Group sources cybersecurity solutions exclusively from international vendors. The quality of Exclusive Networks' offering is therefore intrinsically linked to the performance of its vendors.

A failure in a product resold by the Group could therefore have a negative impact on its brand image. Such failures could either result from the products themselves or from their parameters (coding or design defects or other failures or errors that could hinder the customer's operations or cause malfunctions).

Furthermore, the cybersecurity solutions distributed by the Group are often critical to the conduct of end-users' operations, so any defects could also affect their own operations, thereby indirectly placing the Group at risk for damage to the end-user's operations.

Lastly, if the Group were itself the victim of a cyber-attack, this could affect its brand image and its credibility with its customers.

Risk management

As part of its activities and in order to mitigate reputational risk, the Group:

- has a Security Operations Centre (SoC) to share best practices and protect against potential attacks (see below, 2.1.2 "Risk of cyber-attacks, systems security, data protection");
- monitors incidents and ensures that all vendors inform the Group of alerts on detected failures regarding new threats from cyber criminals;
- ensures that vendors:
 - guarantee that end users will receive solutions that work to their specifications through an end-user licence agreement, and/or
 - offer a support contract to end-usersinsofar as the legal agreements between the Group and vendors do not always cover the risks related to potential failures;
- has third party liability insurance to cover claims under the dedicated policy.

2.1.2 Risk related to operations

Risk related to attractiveness and/or loss of talent and executives ESG

Criticality level:

Risk description

The Group's success depends, to a large extent, on its ability to identify and recruit the key skills of tomorrow, retain its talent and train the next generation of cyber experts to reduce its exposure to talent shortages.

This search for expertise, combined with a particularly competitive environment due to the scarcity of candidates, may lead to difficulties in recruiting such profiles.

At the same time, the departure of experienced employees and key executives could have an impact on the governance and/or operational management of strategic projects.

Risk management

The Group pays great attention to internal communication, diversity, equal opportunities, working conditions, the quality of its human resources management and the commitment of its employees.

The Group has deployed an annual monitoring of employee commitment at the global level, which gives rise to global and local action plans with the aim of strengthening this commitment.

Wherever possible, the Group allows employees to work from home in order to achieve a better work-life balance.

In addition, the Group's personnel management information system, deployed worldwide by the Human Resources Department, ensures the global management of all processes relating to talent management, enabling a harmonised approach to performance monitoring.

The main actions implemented in 2022 include:

- the implementation of succession plans at global and local levels for key roles in the company (including Executive Committee members, key executives). The succession plan is reviewed by the Nomination and Compensation Committee and presented to the Board of Directors;
- the launch of a global Top Talent programme allowing a specific focus on the development, recognition and retention of the Group's top talents and the creation of a Talent Community to prepare the future and anticipate the next generation of internal leaders;
- the launch of a global salary policy at both head office and country level including cross-functional and other categories.

In 2022, the Group also reinforced:

- its Human Resources Department with the recruitment of a Talent Acquisition Director, thus enabling better management and quality of internal recruitment processes (better anticipation, creation of a pool of candidates);
- its proximity to specialised schools or universities (particularly in France with the launch of Exclusive Academy with CalPoli and in collaboration with Guardia and Oteria Cyber School based in Paris) to integrate trainees, train and instil the challenges and skills needed in cybersecurity in the new generation.

(See Chapter 4 "Attracting and retaining talent" for more information on social matters, specifically, the organisation, policies and key achievements, and related indicators).

 Risk of cyber-attacks, systems security, data protection ESG

Criticality level:

Risk description

The Group’s IT systems could be subject to malicious intrusion, cyber-attack, phishing, social engineering, attempts to overload the servers or data privacy breaches.

Any such breach could result in the disclosure of sensitive or personal data, significant legal and financial exposure, damage to the Group’s reputation, loss of competitive advantage and a loss of confidence in the security of the Group’s IT systems.

For example, in December 2020 the Group detected a cyberattack and breach of its systems in the UAE, US, France, UK and Singapore. Although the breach resulted in unauthorised access to data, the cyberattack did not impact the Group’s day-to-day operations. Following this breach, the Group inspected and upgraded its global systems and processes to strengthen their integrity and efficacy (see opposite).

The sophistication and constant evolution of cyber-attacks make it difficult for the Group to anticipate this risk. Furthermore, third parties, such as solution providers that host the Group’s IT systems, could themselves be subject to such attacks resulting in a failure of their own systems and security infrastructure.

Any actual or perceived breach or inappropriate use, disclosure or access to such data could damage the Group’s reputation as a trusted brand and/or result in significant business losses or disruptions (see “Reputational risk” above).

Risk management

Over the last two years, Exclusive Networks has significantly strengthened its cyber-attack management and prevention programme along three main lines:

- the implementation of a Security Operation Centre (SOC) in all countries, monitoring infrastructures in real time and reporting any suspicions of abnormal behaviour or potential risks. The SOC has implemented the most innovative solutions proposed by the Group’s vendors. A project has been launched for the certification of the SOC by the International Organisation for Standardisation (ISO) and other global organisations. The SOC is connected to the NATO security systems in order to benefit from their information on possible risks related to the Russia/Ukraine conflict;
- the strengthening of the cybersecurity team with the recruitment of highly experienced profiles and the creation of a Cyber Defence Committee chaired by the Head of the SOC, who reports directly to the Chief Information Officer, a member of the Executive Committee;
- the implementation of a programme to raise awareness among all employees to the risks of cyber-attacks, through training modules and real-life phishing campaigns.

(See Chapter 6, section 6.4 “Information system protection” for more information on data protection in terms of its organisation, policies and key achievements and related indicators.)

 Risk related to vendor concentration

Criticality level:

Risk description

The Group distributes the products of approximately 290 established and disruptive vendors, covering the key segments of cybersecurity and the related segments. The Group’s sales are concentrated within a small number of these vendors with which it has long-standing relationships. Indeed, Exclusive Networks’ top 20 vendors accounted for 87% of sales in 2022 and its top five vendors for 65%.

The main vendors experienced strong growth in 2022 such that their respective weight in the Group’s revenue remained stable in 2022.

The termination of the contractual relationship with one of the key vendors could result in a significant decrease in the Group’s activity and its turnover.

Risk management

The Group’s efforts to diversify its offering resulted in two new cybersecurity segments in 2022: Cloud Security and OT/IoT Security.

In 2022, it succeeded in this diversification by signing contracts with 13 new software vendors and 14 contract extensions to ensure the expansion of Exclusive Networks’ distribution rights in new countries and/or on new product and service lines.

In its commercial relationships, the Group maintains strong relationships with its vendors and has set up a dedicated “Vendor Management” team (it organises quarterly reviews with vendor managers) and implements internal performance acceleration and improvement plans when necessary.

2.1.3 Legal and regulatory risks

Risk related to export control regulations and sanctions regimes and embargoes relating to economic sanctions on Dual-use products ESG

Criticality level:

Risk description

The Group directly or indirectly purchases and distributes products and solutions considered Dual-use, i.e. classified as Dual-use items (likely to have both civilian and military use) where they incorporate encryption technology. Their export or re-export may thus be subject to the obtaining of an export licence granted by the authorities of the exporting countries or an exemption.

The development of the Group's activities and locations thus increases its exposure to political and economic risks specific to certain countries that could affect its activities and results. The Group's ability to market new products and enter new markets may depend on obtaining government certifications and approvals.

Despite the Group's efforts to comply with all such laws and regulations, unintended violations or failure to comply could result in the suspension of export privileges.

This is because these rules are based on international, national and regional security strategies, national independence and global geopolitical developments.

In the event of non-compliance with applicable laws and regulations, the Group could be exposed to significant fines and other administrative and criminal sanctions that could have a material adverse effect on its financial condition, business and reputation.

Risk management

The Group has taken all appropriate and necessary measures to comply with all international and national trade regulations applicable to its activities. It has set up a specific internal plan dedicated to these export control and embargo compliance regulations.

This plan includes:

- adapted procedures and IT tools, such as the one used to ensure the final destination of products;
- employee awareness programmes;
- a regular internal audit plan;
- a system for monitoring legislative and regulatory developments and restrictions applicable to the Group's activities;
- a system for screening vendors, resellers, end customers and other partners;
- Group businesses and entities are provided with specific assistance and advice by the community of export control experts, country and Group champions.

In 2022, the Group strengthened its organisation by creating the position of Group Export Control Manager, whose main missions are to update procedures to supervise the community of country Export Control Managers appointed in each Group company. Group companies report to the Group Export Control Manager any disputes or potential non-compliance with regulations, inform the relevant authorities of any non-compliance found and take all necessary steps to prevent any problems that may arise.

(See Chapter 6, section 6.7 "Export control").

 Risk related to corruption (business ethics) ESG

Criticality level:

Risk description

Exclusive Networks operates in a complex and evolving legal and regulatory environment.

The Group is subject to various national legislations, as well as to international standards. This is the case, in particular, for anti-corruption and money laundering regulations.

In this respect, Exclusive Networks has identified two main corruption risks due to its geographical location and its relationships with partners and stakeholders:

- the expansion of its activities in countries where the corruption perception index is high according to the ranking established by Transparency International, particularly in Asia and Africa;
- the Group’s model, which is based on a network of partners made up of resellers and distributors, represents an additional risk for the Group, because it is responsible for the activities carried out on its behalf.

Non-compliance with the law, as well as unethical behaviour, could expose Exclusive Networks Group and/or its employees to investigations, administrative or judicial proceedings, criminal or civil sanctions and additional penalties (such as exclusion from government contracts).

These investigations or possible convictions could also have financial, reputational, operational and/or legal consequences for the Group.

Risk management

In accordance with the requirements of the Law on the Prevention of Corruption and the Transparency of Economic Life and Public Procedures (known as the “Sapin 2” Law), Risks & compliance has set up a compliance programme and has a dedicated team, made up of specialised lawyers and local advisers (brought together in a network of *Ethic Champions*).

The following are the main actions carried out in 2022:

- update of anti-corruption procedures and reinforcement of the Group’s commitments: updated in 2022, the Code of Conduct defines and illustrates the types of behaviours to be adopted and prohibited in terms of preventing and fighting corruption and influence peddling. In this respect, the Group is committed to zero tolerance of corruption and influence peddling;
- launch of the update of the corruption risk assessment legal entities of the Group and the corresponding definition of specific corrective plans;
- launch of a third party onboarding tool integrity review system with a gradual roll-out planned until the end of 2023 (“My TrustedPartner”);
- continuation of the employee training and awareness-raising programme to ensure that employees are familiar with the procedures, particularly in the functions most exposed to this risk;
- an internal and external alert system, available to employees and stakeholders, also helps to counter this risk. Appropriate disciplinary measures are taken in consultation with the Human Resources Department and Executive Management when necessary;
- a regular internal audit plan. The Internal Audit department is responsible for the evaluation of the measures implemented. This department ensures that compliance related incidents are identified and addressed.

For more information on the Group’s preventive measures regarding corruption, see sections 6.1 “Governance and organisation” and 6.2 “Ethics, prevention and anti-corruption” in Chapter 6.

Risk related to litigation and disputes

Risk description

The Group may become involved in legal proceedings, including government investigations, that arise out of the ordinary conduct of its business, including matters involving intellectual property rights, commercial matters, merger-related matters, domestic and/or international regulations, product liability and other actions.

The Group is currently not involved in any claims, litigation or lawsuits. Although the Group may not always win its case, the risk is not expected to have a material adverse effect on its consolidated financial position, results of operations or cash flows. The Group can also not predict the outcome of litigation or other investigations in which it may be involved at any time.

As at the date of the 2022 Universal Registration Document, there are no pending or potential legal or arbitration proceedings, including any proceedings of which the Group is aware, that are likely to have or have had in the last twelve months a material effect on the Group's financial position or profitability, other than those reflected in the financial statements or disclosed in the notes to the financial statements.

Criticality level: 

Risk management

The Group closely monitors the status of ongoing litigation and disputes and has implemented reporting rules to enable the Group's Legal Department to be informed as soon as possible of the occurrence of a significant dispute and to optimise its handling and understanding of related risks and possible consequences.

A provision is made in the financial statements for any litigation that may arise.

The Group relies on a network of lawyers and advisers specialised in their field and selected by the Group's Legal Department to manage and monitor the main disputes and litigation.

The Group considers that customer satisfaction and respect for good commercial and ethical practices are key to limiting the number of disputes to which the Group could be exposed. It therefore pays particular attention to customer satisfaction and the implementation of good practices on a daily basis.

Tax risk

Risk description

Due to the global and cross-border nature of its distribution business, and given the complex international tax environment, the Group faces tax risks and uncertainties inherent to its business.

This is due to the number and complexity of tax regulations, both local and international (including transfer pricing rules and principles governing the application of withholding taxes), and their interpretation in each country. In particular, in many jurisdictions, there is substantial uncertainty as to the classification of cybersecurity solution licence proceeds as business profits or royalties.

In this global environment, the Group aims to comply with all applicable tax rules and regulations in the countries in which it operates, ensuring that the correct amount of tax is paid in the jurisdictions where it generates profits and value. The Exclusive Networks Group is committed to upholding local and international rules, including the principles laid down by the OECD.

Criticality level: 

Risk management

The Exclusive Networks Group handles tax issues with integrity and does not engage in any artificial tax schemes.

The Group's tax department is organised around a central tax team that reports to the Group Finance Department and locally to the local Finance Directors. The Group also uses external advisers to ensure that risks are identified and assessed and that measures to control them are put in place.

Any tax disputes give rise to provisions that are duly recorded in the accounts.

For more information on tax policy and tax avoidance, see section 6.6 "Transparency and the fight against tax avoidance" in Chapter 6.

Risk related to personal data breach

Criticality level: ■ ■ ■

Risk description

In conducting its business, the Group collects and processes personal data from customers, end-users and prospects.

Global privacy policies have developed considerably creating a complex compliance environment governed by legislation such as the European Union's General Data Protection Regulation (GDPR) in force since 25 May 2018, in addition to the e-privacy Directive 2002/58/EC and national legislation.

These regulations establish a legal framework for the protection of personal data, with enhanced rights for citizens and new obligations for businesses in this area.

Any real or perceived breaches or improper use of, disclosure of, or access to such data could harm the Group's reputation as a trusted brand and could have a material adverse effect on the Group's business, results of operations or profitability.

Should there be a breach of the General Data Protection Regulation (GDPR), the Commission Nationale Informatique et Libertés (French data protection authority – CNIL) may issue the following sanctions in France once the right to reply has been exercised:

- a reprimand;
- an injunction to comply. This may be accompanied by a penalty of up to €100,000 for every day of delay;
- a temporary or definitive restriction on processing, a ban or withdrawal of an authorisation;
- the withdrawal of a certification;
- the suspension of data flows intended for a recipient located in a third country or for an international organisation;
- a partial or whole suspension of the decision to approve binding corporate rules (BCR);
- an administrative fine of up to €10 million or 2% of the company's annual sales worldwide. For more serious breaches, this amount may be increased to €20 million or 4% of annual sales worldwide;
- the publishing of its decision, as determined by the CNIL's restricted committee.

Risk management

In order to mitigate the impact of this risk, the Group is focusing on the following actions:

- monitoring and strengthening the compliance system with the support of the relevant departments in each country;
- the continuous improvement of the systems in each country by the data protection officers (DPO);
- training and awareness-raising of employees on the protection of personal data (with the development of e-learning to ensure continuity of training);
- the conduct of multi-level controls.

For more information, see Chapter 6, sections 6.4 "Information system protection" and 6.5 "Data protection".

.../...

Risk description

.../...

It may also order the infringing parties to pay for the decision to be published in any publications and other forms of media it determines.

- There is a simplified sanctions procedure for less complicated instances or minor infringements: sanctions in these cases cannot be published and are restricted to a reprimand, a fine of up to €20,000 or an injunction accompanied by a penalty capped at €100 for every day of delay.

Any insurance coverage for protecting against loss from cybersecurity and privacy risks may not be sufficient to cover all possible claims, and the Group may suffer losses that could have a material adverse effect on its business.

While the Group has not experienced any significant data breach (breach of data confidentiality, data integrity or data availability), or any material financial losses related to cybersecurity attacks, the Group's systems, those of its vendors and customers, and those of the Group's third party service providers are under constant threat. The Group has suffered cybersecurity attacks, informed its customers and taken the appropriate corrective measures. The impact of the risk is therefore both reputational and financial.

Risk management

2.2 Internal control and risk management

This section describes the internal control and risk management system applied within the Group in accordance with the AMF reference framework published in July 2010, which is based on national and European

legislative and regulatory provisions and international best practices and benchmarks for internal control and risk management, in particular ISO 31000.

2.2.1 Objectives of internal control and risk management

The purpose of the internal control and risk management system is to identify and analyse the Group's main risks. Risks that fall outside the acceptable limits set by the Group are dealt with and, where necessary, addressed through action plans. These action plans may include the transfer of financial consequences (insurance mechanism or equivalent), an adaptation of the organisation, or the implementation of policies, procedures or controls by the Internal Control or Risks & Compliance department. To this end, the Group has implemented an internal control system, based on the risk management system, to identify the main risks to be controlled and to ensure in particular:

- compliance of the Group's management actions with laws and regulations;

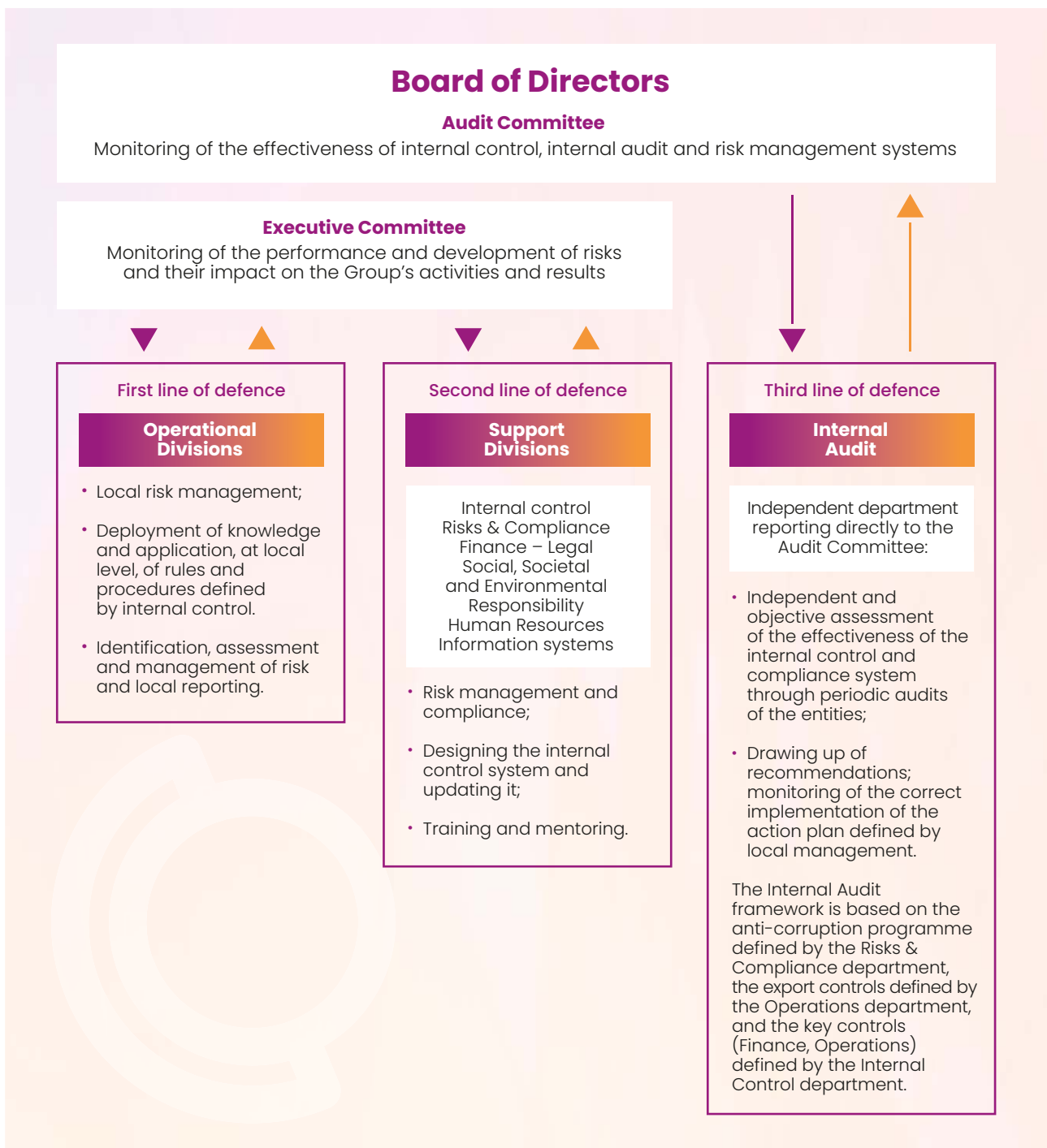
- compliance with the Group's seven fundamental ethical principles, as well as the instructions and guidelines set by the Board of Directors and/or Executive Management;
- the proper functioning of the Group's internal processes, in particular those designed to safeguard its assets. This includes, among other things, the application by the subsidiaries of the policies, procedures and directives that have been transmitted to them;
- the reliability of accounting and financial information.

2.2.2 Organisational framework of risk management and internal control

Risk management is the responsibility of each operational or functional entity. This work is led by the Risks & Compliance department, with the participation of the Legal and Finance teams, and under the supervision of the Audit Committee.

The Audit Committee is responsible for reviewing the effectiveness and consistency of internal controls and risk management systems, under the supervision of the Board of Directors.

The risk management process ensures that risks are identified and managed at all levels of the Group's organisation.



The internal control and risk management system covers all the controlled companies included in the Group's consolidation scope.

2.2.3 Internal control and risk management players

The Risks & Compliance and Internal Control departments manage the internal control and risk management systems. They report to the Executive Committee, which monitors them. The Audit Committee ensures that the internal control and risk management system is effective, particularly by reviewing the conclusions of the Internal Audit.

The Group reorganised these departments during the 2022 financial year. As a result, the Risks & Compliance, Internal Control and Internal Audit departments, which were previously grouped together in the same department, now operate in three separate departments in order to ensure good governance in terms of independence and efficiency. Each of the departments has also been strengthened.

Audit Committee

The Audit Committee periodically reviews the internal control and risk management system. The organisation, mission and work of the Audit Committee in 2022 are described in greater detail in the Board of Directors' report on Corporate Governance in Chapter 4, section 4.2.8.2 "Audit Committee" of the 2022 Universal Registration Document.

Risks & Compliance Department

The Risks & Compliance department is responsible for regularly updating the Group's risk mapping, including the mapping of corruption-related risks, and for leading the anti-corruption programme (updates, training, awareness-raising, managing the self-assessment campaign etc.). The Risks & Compliance Department reports to the Group's Legal Department.

Internal Control Department

The main purpose of the Internal Control department is to identify the key controls that enable operational and financial risks (excluding corruption-related risks) to be mitigated, to define and deploy the corresponding procedures, policies and guidelines, and to monitor the internal control system (updates, training, awareness-raising, managing the annual self-assessment campaign, integration of these controls, where possible, into the Group's Integrated Management Software etc.).

The Internal Control department reports to the Group Finance Department.

Human Resources Department

The quality of human resources and the cohesion of management are key factors in the Group's success.

The Group's Human Resources Department, in coordination with the Risks & Compliance Department, ensures that the subsidiaries implement human resources policies that are adapted to their specific contexts and challenges, but always meet the best local standards. While the principle of autonomy and empowerment of subsidiaries is applied, the Group Human Resources Department is responsible for ensuring the consistency of the policies implemented and their alignment with the Group's values and the actions defined at Executive Committee level. The Human Resources Department takes sanctions if necessary, in accordance with policies that are implemented within the Group.

Internal Audit Department

The Internal Audit Department independently and objectively assesses the functioning of the internal control, compliance and risk management system. This assessment covers compliance with the anti-corruption programme defined by the Risks & Compliance department, export controls defined by the Operations department and financial and operational controls defined by the Internal Control department.

Based on the results of its audits, the Internal Audit department draws up recommendations to improve the effectiveness of the internal control and risk management system and ensures the correct implementation of the action plan defined at local Management level.

The Internal Audit department is independent and reports directly to the Audit Committee on a quarterly basis.

The audit plan is approved by the Audit Committee annually.

2.2.4 Internal control and risk management analysis process

The identification, assessment, prioritisation and management of the risks faced by the Group are closely and regularly monitored. The analysis of internal control and risk management is performed by the Internal Audit department, which, as an independent body within the Group, assesses the effectiveness of the main internal control processes of the Group's audited entities.

Risk analysis

As part of the risk management process, the Risks & Compliance department, with input from the Executive Committee and the regional and local Management, establishes a register that presents the risks faced by the Group and provides guidance to senior management on the major risks as presented in section 2.1 "Risk Factors" of this Chapter 2. The information presented in this register includes:

- a mapping of risks, allowing the Board of Directors and the Group's Executive Management to have a visual representation of the probability of the occurrence of a risk and the impact on the Group (both quantitatively and qualitatively) should that risk occur, enabling it to better understand how to allocate resources and seek to strengthen mitigation actions;
- an identification of significant risks in each category;
- for each significant risk, an overview of its potential causes and consequences, and existing and planned mitigation measures;
- an indication on the level of the probability of the occurrence for each risk identified and the impact on the Group should that risk occur; and
- the identity of the risk owners and sponsors (members of the Executive Committee) who have been assigned as responsible for implementing mitigating actions under the Board of Directors' supervision.

This register is regularly updated to reflect changes in risks and the implementation of mitigation measures.

The risk map established in 2021 was expanded in 2022 with the specific risk mapping for corruption. It will be updated in 2023, though there was no significant change to the main risks in 2022.

The Internal Audit Department conducts regular reviews of risk management processes. These reviews cover the Group's compliance with anti-corruption and export control laws and regulations, as well as key controls defined by internal control. These reviews give rise to a corrective action plan where necessary.

Analysis of internal control

The Group continues to improve its internal control framework, including by strengthening its governance, providing regular training for all relevant employees, and introducing improved technology to monitor the implementation of the controls.

The operational and functional divisions play a key role in the internal control system. They work with the Internal Control Department to update the procedures specific to the processes under their responsibility. Thanks to regular dialogue between the Internal Internal Control department department and the operational and functional departments, it is possible to:

- remain constantly alert to new risks that may arise or to changes in existing risks;
- ensure the relevance of the controls in place;
- identify any new controls that should be put in place to mitigate risks;
- identify corrective actions where necessary.

2.2.5 Internal control and risk management environment

The internal control and risk management system is based on a decentralised organisation with a clear definition of responsibilities, notably through job descriptions, delegations of authority and widely communicated policies and procedures. It includes principles and values governing the behaviour and ethics of all the Group's employees, presented in a set of rules and procedures.

Rules and procedures of the Group Country Manual

The Internal Control department has drawn up a collection of internal control guidelines and procedures called the Country Manual, which was distributed to all employees in July 2022. This Country Manual is applicable at all levels within the Group. Each Country Manager is responsible for ensuring that it is properly applied and distributed.

The Country Manual defines the main principles and fundamental rules on which the Group's activities are based, and specifies the Group's expectations and requirements with regard to processes and controls (including their formalisation) for each of the key cycles, particularly in the following areas:

- the Group's fundamental principles, governance and organisation;
- rules and guidelines for the sales, purchasing, import/export, inventory and logistics, treasury, fixed assets, tax etc.;
- guidelines for the Group's human resources, marketing, communication and IT management.

The Country Manual was developed jointly by the Internal Control department and each of the relevant departments, with input from financial managers and directors at both local and regional levels. It will be updated periodically to take account of changes in the

Group's activities, its environment and risks, and will be enriched with the feedback received from employees and its application by the Group and the countries.

This Country Manual is available in the Finance and Risks & Compliance sections of the Group's intranet.

Code of conduct

The Group's ethical principles are set out in the Code of Conduct, which contains the Group's commitments and rules of conduct towards its main stakeholders, namely employees, vendors, business partners, the environment and civil society.

This Code of Conduct must be signed by all Exclusive Networks Group employees, on an electronic platform, after they have answered an electronic questionnaire as part of a training course.

Group ethical principles

Honesty and integrity, fairness of commercial practices, data confidentiality, professional behaviour, professional skills and added value, social respect, environmental care.

Delegation of authority

Delegation of authority matrices, specific to each region, define the authorisations required to enter into transactions and to carry out the Group's key activities.

These delegation of authority matrices defined, depending on the issues at stake, three levels of decisions corresponding to the three levels of the Group's organisation (local at entity level, regional and at Group level) according to the nature, the strategic issue and the amount of the impact at stake.

2.2.6 Evaluation of internal control and monitoring of action plans

With regard to the risks identified and assessed, the Internal Control department defines and updates the various components of the internal control system, working in particular in close collaboration with the Group's corporate and operational divisions.

The annual self-assessment questionnaire on financial management control

The Group carries out a self-assessment campaign each year within each entity to ensure that the key controls are correctly understood, performed at the defined frequency and properly documented.

In this regard, a self-assessment questionnaire is sent to the Finance Directors and senior management of each subsidiary and returned to the Group Internal Control department. Based on the responses given, the Internal Control department defines an action plan in coordination with the subsidiary. These self-assessments identify areas for improvement and good practices, to initiating action plans and to strengthening the internal control system.

Exceptionally, the annual self-assessment campaign will take place in the first half of 2023.

Over and above the annual self-assessment campaign and the hierarchical oversight exercised by operational

managers at all levels, in application of the rules of delegation of authority in force in the Group, the functional departments play a special role in identifying and mitigating risks by providing support to operational staff, by intervening preventively, particularly in the form of advice, by reminding employees of the importance of rules and procedures, or by carrying out reviews on the application of the rules.

Monitoring of action plans

Action plans are regularly monitored. In this context, meetings between the Internal Control department and the Financial Departments of the subsidiaries concerned are organised to ensure that the corrective measures defined during the review of the self-assessment questionnaire or during the review of the conclusions of internal or external audits are implemented.

This monitoring may result in specific communications to all subsidiaries. For example, during the 2022 financial year, specific communication and monitoring was carried out on the mandatory double approval of payments above a certain threshold defined by the Group, as well as on the approval process for low margin deals (clarification of items to be included and excluded in the margin calculation, collection of required approvals etc.).

2.2.7 External monitoring system

The role of the Statutory Auditors is to certify the regularity, fairness and true and fair view of the Group's corporate and consolidated financial statements on an annual basis and to issue a limited review report on the Group's half-yearly consolidated statements.

When performing their duties, the Statutory Auditors present the Audit Committee with a summary of their work and of the accounting options adopted for the preparation of the financial statements.

When they examine the accounts, the Statutory Auditors submit a report to the Audit Committee highlighting the essential aspects of the scope of consolidation, the

results of the statutory audit, in particular the accounting options adopted, the audit adjustments and the significant internal control weaknesses identified during their work.

The main recommendations of the Statutory Auditors on these internal control weaknesses are the subject of an action plan and a follow-up presented to the Audit Committee and Executive Management at least once a year.

External audit engagements are shared between Mazars and Deloitte, the Company's Statutory Auditors.

2.3 Materiality analysis of sustainability issues

Within the meaning of Article L. 225-102-1 of the French Commercial Code, in the Extra-Financial Performance Statement, the Exclusive Networks Group reports on the significant risks that its activities could generate in terms of social, environmental, societal and governance issues, for itself as well as for its stakeholders. These risks have been assessed in relation to the Group's materiality matrix.

Methodology note

The materiality analysis enables to identify and prioritise the most relevant sustainability issues for the Group and its stakeholders.

As part of its corporate social responsibility, the Exclusive Networks Group wished to implement its first materiality matrix with the support of an independent consultancy, in order to strengthen the robustness and prioritisation of its main stakes, and to enhance its overall risk management approach (see Chapter 2.2). The aim is to ensure that the Group reports on its most important environmental, social and governance challenges, identifies present and future risks and opportunities, and defines its sustainability programme taking into account the prioritisation of these risks and opportunities.

For this first exercise, the matrix was built based on the consultation of:

- on the one hand, internal stakeholders, including the Group's Executive Committee as well as executives representing all functions and the geographical areas in which the Group operates;
- on the other hand, external stakeholders, independent members of the Board of Directors and shareholders.

The double materiality approach was adopted in order to address the various risk factors symmetrically when assessing their impacts, of the Group on its ecosystem and vice versa.

Firstly, the main issues were identified on the basis of a sector benchmark carried out on vendors, customers and competitors representative of the Group's activities.

Next, nearly 20 individual interviews were conducted, during which people were asked about:

- the group's strategic objectives and the main environmental, social and governance risks and opportunities most likely to have an impact on the Exclusive Networks Group in the future;
- the assessment of the importance of these impacts based on a quantitative rating scale.

The probability of occurrence was determined according to the following scale:

1	2	3	4
Rare	Possible	Likely	Very likely

The impacts of the issues, whether financial, reputational, legal or human capital related, were assessed according to their importance on the following scale:

1	2	3	4
Not significant	Minor	Moderate	Major

The materiality matrix allows the Exclusive Networks Group to prioritise its major social, environmental, societal and governance issues based on net risks, i.e. taking into account the control and continuous improvement measures already in place.

Main findings

At the end of the interviews, we noted a great convergence between the internal and external stakeholders as to the importance of the issues.

The major issues of the Exclusive Networks Group:

- some of them can be considered as sectoral risks, as they are common to all stakeholders operating in this field. This is the case for the shortage of cybersecurity skills, as well as for the cybersecurity risk itself;
- others are specific to the Group, due to its business model and global presence. This is the case for export control, linked to the distribution of Dual-use products, and the presence in certain countries that may be considered "at risk" on various subjects.

Four major trends emerge from the materiality analysis, presented below in order of priority:

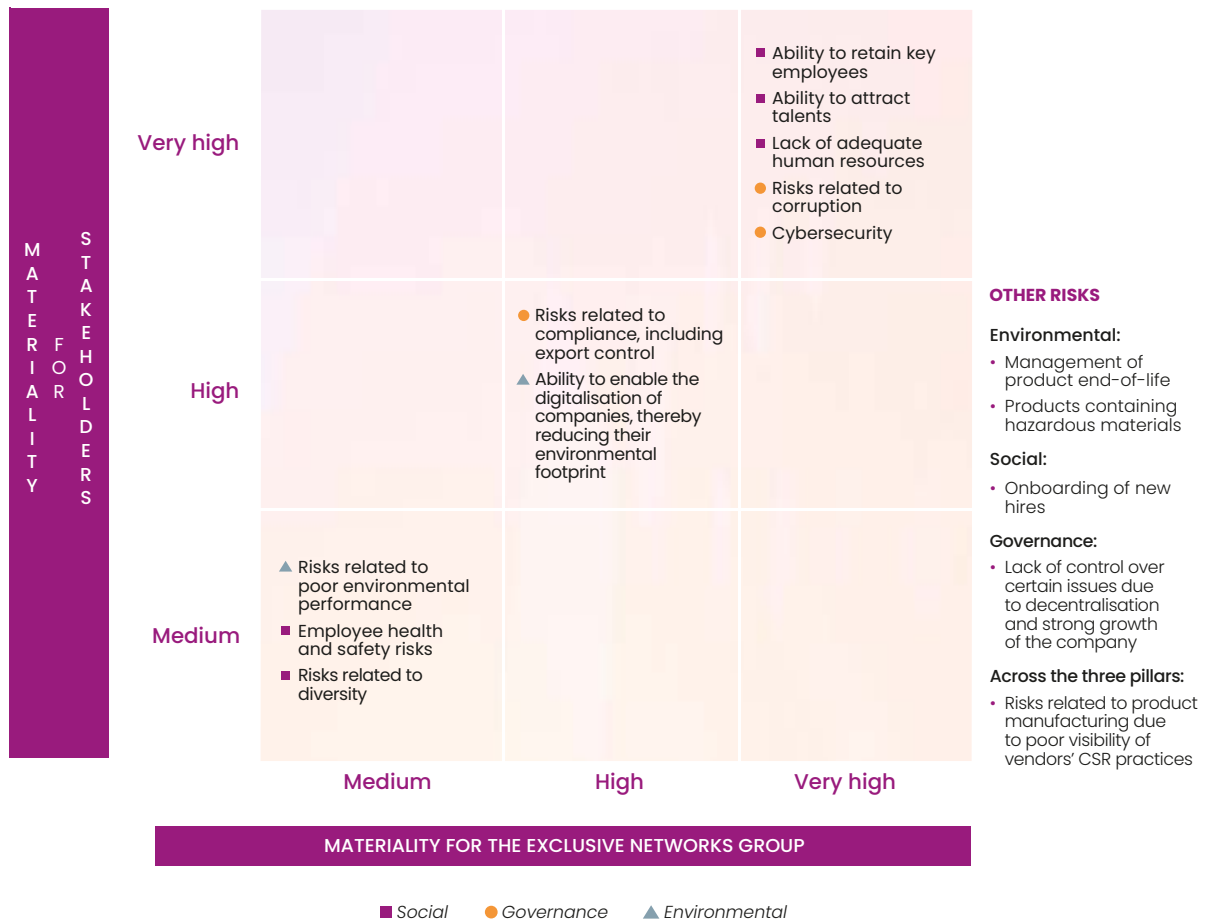
1. Unsurprisingly, the management of human resources issues emerges as the Group's first key success factor for achieving its ambitions and pursuing its development.
2. Next in order of priority is the control of corruption risk and, more generally, the risk of regulatory compliance, a consequence of the Group's rapid growth and its development at the global level.
3. Thirdly, as with many companies, cybersecurity is one of the Group's main challenges, since its business model makes it a reputational risk as well as an operational risk.
4. Lastly, environmental issues are cited by all the stakeholders, but with less importance, due to the opportunity to develop fully digital activities on the one hand, and on the other hand to weaker discussion levers with the vendors regarding the environmental footprint of hardware.

[GRI 3-1]

Risks and opportunities

Materiality analysis of sustainability issues

Materiality matrix of the Exclusive Networks Group's social, environmental, societal and governance stakes



The materiality matrix has allowed us to confirm the main issues of the Exclusive Networks Group regarding social, environmental, societal and governance matters, and as such constitutes the reference document from which this extra-financial performance statement has been structured.




Based on this analysis, the issues that are subject to monitoring and action plans as required by Article L. 225-102-1 are the following:

1. The ability to attract and retain talents, as well as the lack of competent human resources, covered in section 3.4;
2. Corruption and other regulatory compliance issues, covered in section 3.6;
3. Cybersecurity, covered in sections 3.6.3 and 3.6.4;
4. The ability to reduce our environmental footprint, covered in section 3.5.

These issues have been integrated into the overall risk management approach, as described in Chapter 2.

[GRI 3-2-a]

3 Our key performance indicators and results

Topics (+SDG)	Commitments	Indicators	2022 ¹	Target
 SDG 5.1 & 5.5	HR			
	Attracting and retaining talents			
	Measure employee engagement annually	Engagement rate	71%	77% by 2025
	Develop and retain our employees	Tenure	4.4 years	4.5 years by 2025
	Diversity, equity and inclusion			
	Increase the proportion of women in senior management positions	Proportion of women in senior management positions	34%	40% by 2025
	Train all employees on diversity, equity and inclusion	Proportion of employees trained	ND	100% by 2025
 SDG 12.4, 12.5 & 12.6	Climate			
	Climate change			
	Commit to reducing the Group's carbon footprint	Full Scope 3 carbon footprint inventory	ND	2023
		Decarbonation trajectory and related action plan	ND	2024
	Act ethically and with integrity			
	Train our employees to ethics and combating corruption	Proportion of employees who have certified the Group's Code of Conduct	ND	100% by 2025
 SDG 16.5	Ensure the integrity of our business partners	Proportion of due diligence performed on high-risk third parties	ND	100% by 2023
	Control, monitor and assess the implementation of the Group's compliance programme	Audit of all countries including anti-corruption	ND	Audit of all countries at least every five years, audit plan covering >30% of revenue
Cybersecurity	Protect our data and operations			
	Protecting our operations and IT systems	Cyber Exposure Score	Medium	≤ Low by 2025

1 Since this is the first year of publication of the Exclusive Networks Group's sustainability KPIs, the 2022 results are the baseline year and in some cases are not available.
 2 Members of the Group Executive Committee and their N-1, Regional General Managers, Country Managers and their Management Committees, in countries with revenue of more than €100 million.

As the scope of the report will be expanded in the coming years to eventually cover all consolidated companies, the 2022 results as well as the targets cover the Group's entire scope of consolidation.

4 Attracting and retaining talent

4.1 Cybersecurity – a sector with a severe skills shortage

While cyber threats continue to increase in number and become more sophisticated, the cybersecurity industry is suffering from a severe skills shortage. Exclusive Networks Group estimates that three million positions are currently vacant at the global level.

There are several reasons for this:

- technology has advanced at such a rapid pace that the necessary qualifications are struggling to keep up. This has been exacerbated by the Covid pandemic, which pushed companies to accelerate their digital transformation: in Europe, it is estimated that the demand for cybersecurity professionals increased by 22% in 2021;
- insufficient alignment between the education system and the expectations of the labour market: at present, the schools that provide IT courses do not cover the full range of skills sought by employers, so the new generation is not yet prepared;
- employers also have a role to play in moving away from unrealistic expectations and niche job descriptions, which eliminate excellent candidates from the process who could be assets to the company. For example, prioritising computer science and technology degrees in the job requirements fails

to account for people with both technical and non-technical skills that can be easily upskilled into this profession. In addition to looking for already qualified profiles, building on people's potential is another way to expand opportunities;

- the pressure on many employees, combined with the shortage of staff, has led to burnout with many people leaving the profession, which has made the shortage worse. More than one third of cybersecurity employees are exploring new careers.

With a shortage of qualified professionals, salaries are rising, increasing corporate spending in an already uncertain economy. On a global scale, steps are being taken to address the cybersecurity skills shortage: in the UK, for example, the government has launched a €50 million cyber-school to support the training of cyber-experts. New schools and training courses dedicated to cybersecurity are also being created in France and in other countries.

In this difficult industry context, in order to have the human resources that will allow the Exclusive Networks Group to continue its development, the key policies and programmes implemented by the Human Resources Department focus on commitment, recognition, attrition, talent retention and the employer brand.

4.2 Human Resources mission and organisation

Human Resources mission

“Guarantee the future of the Exclusive Networks Group by attracting, developing and retaining talents, in order to contribute to the improvement of the company’s performance and to ensure its longevity”.

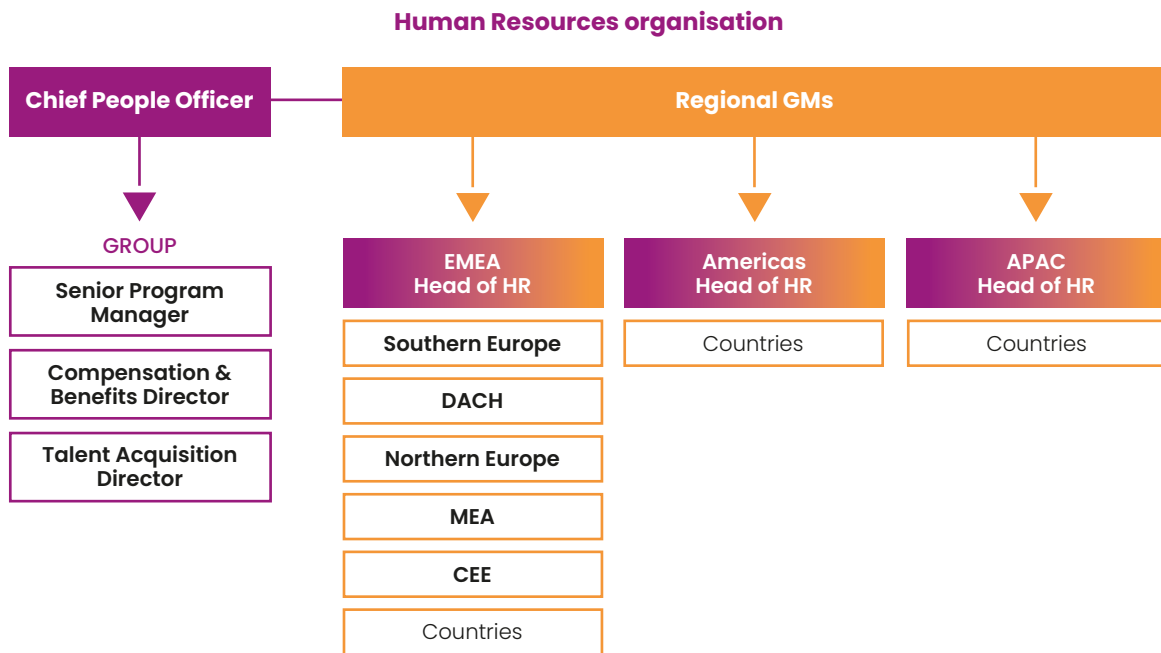
To this end, the commitments of the Human Resources teams are:

- to work in close partnership with management;
- to focus efforts on high added-value tasks;
- to support the company’s strategy by optimising employee performance;
- to provide an inclusive employee journey in a consistent and equitable manner;
- to adapt programmes and initiatives to local markets and to have a local HR plan;
- to provide a link between employees and management.

Organisation

To meet the Group’s social and development challenges, the Human Resources Department is headed by the Chief People Officer, a member of the Group Executive Committee, and operates at two levels:

- a Group-level organisation, which brings together expertise in Tools, Data and Programmes, Compensation and Benefits, Recruitment and Skills Development;
- operational Human Resources departments, which report to the Country Managers.



In line with the way the whole Group operates, the roles and responsibilities of Human Resources are distributed between Group and operational teams in order to maintain the agility of each country:

Human Resources mission



[GRI 3-3-c]

An HR IT System for better business management

Since 2021⁽¹⁾, in order to carry out its missions in a group in strong international growth, the Group Human Resources Department has acquired and implemented a single HR IT system (Human Resources IT System) in all its subsidiaries, enabling it to better manage its activities:

- automate and optimise the administrative tasks related to human resources management across the Group;
- centralise information and update it in real time;
- improve the process as well as the stages of the employee's career in the company, from recruitment to departure;
- automate and improve the reliability of processes such as performance reviews, job changes and compensation;

- back it up with a dashboard that allows to analyse the staff, turnover, etc. or any other indicator, whenever necessary and to monitor developments and trends on an ongoing basis;
- generate different dashboards that can be configured as required via Power BI;
- connect to other external applications, such as the annual employee survey platform or interview management;
- provide employees with a simple and autonomous access to all their administrative documents (contracts, training, leave balance, etc.).

Thanks to this tool, Human Resources teams are more efficient and have reliable data at all times, enabling them to manage their activity and focus on higher added value tasks.

4.3 Employee commitment

Your voice matters

Since 2021, the Human Resources Department has implemented an annual survey addressed to all Group employees called "Your voice matters".

The survey, launched each year with the support of the Group's Chief Executive Officer, is anonymous and focuses on the following themes:

- commitment and pride in belonging;
- leadership and trust in management;
- direct management;
- communication and cooperation among teams;
- ability to perform one's duties efficiently;
- involvement;
- work-life balance;
- feedback and recognition;
- training and personal development.

2022 campaign: results and main findings

The response rate to the 2022 survey was 80%, close to the 2021 level.

The overall engagement rate was 72%, with a very low percentage of unsatisfied employees (6%). We noted, however, that employees from recently acquired companies consistently gave lower ratings.

- The main strengths highlighted by employees are the relationship with their direct manager, the fact that their work has an important value for the company, teamwork, a clear role and precise duties.

- The topics on which the Exclusive Networks Group should focus its attention are recognition, training and personal development, as well as the work-life balance. This last point echoes the pressure that the entire cybersecurity sector is under due to the skills shortage (see section 4.1).
- Compared with the previous year, employee satisfaction with training and personal development has increased, although this remains an area where further efforts are needed. This can be seen as the first results of the action plan implemented by Human Resources, as well as a stronger involvement of managers in the development of their employees.
- Lastly, the survey confirms that the attrition risk is higher for experienced employees and for certain key skills.

After the survey was completed, the Chief Executive Officer and Chief People Officer hosted a webinar to share the main findings with all employees.

At the end of this campaign, the main focus was set on the improvement of career paths, the implementation of new recognition programmes, and a communication plan aimed at creating a more direct link between the Chief Executive Officer, the Group Executive Committee and all employees.

The Exclusive Networks Group has set itself the goal of reaching a 77% engagement rate by 2025. This rate is measured by aggregating several questions on pride in belonging to the Group, recommending the Group as an employer, motivation to work for the Group and projecting oneself in the company for more than two years ahead.

(1) Given that the HRIS was deployed only during 2021, it is not always possible to compare the workplace data in this report with previous years.

4.4 Performance and talent programme

As the findings of the materiality analysis show, attracting and developing talent is the Exclusive Networks Group’s main challenge in terms of sustainability (see section 2.3).

To this end, the Group strives to build a strong employer brand in order to attract talents from all countries, ages and origins, to contribute to their development and make them want to stay with the company. In this connection, the Group’s Human Resources Department designs and implements a number of programmes aimed at the professional development of employees, giving them the opportunity to continue to learn and evolve (see section 4.5), with the aim of promoting employee retention and reducing the risk of skills loss.

The strategy includes a number of schemes, which are implemented with different groups of employees.

Performance assessment and career development

Since 2021, the Group’s Human Resources Department has introduced an annual interview allowing all employees to discuss with their manager about their performance assessment, objectives for the coming year, training and development opportunities in their function and career development prospects. This process concerns all Group employees present on 30 September of the previous year.

Action	2022 result
Discuss their performance assessment and career prospects with each employee [GRI 404-3-a]	81% of employees completed a performance and career development review with their manager

Talent identification and retention programme

To address the skills shortage and improve talent retention, the Group’s Human Resources Department has set up a specific talent identification and retention program called Rise Up. It aims to identify a number of talents across the Group, covering various functions, technical or leadership skills, and geographical areas. The aim is to build up a talent pool that will be one of the key success factors in helping the Group to achieve its development objectives.

With the support of local HR managers, country managers and managers, the first phase of the programme consisted of identifying a number of high value-added employees, then assessing their performance and their potential for development and career advancement. After identifying these persons, an individualised development plan was put in place for each one of them. The plan was implemented at local and Group level and included both group and individual components, as well as mentoring. A community was also created to foster team spirit and strengthening ties with the company.

This process is designed to ensure that high potential individuals are identified, supported through a rewarding development pathway, to realise their full professional potential and bring their expertise to the Group.

The retention of employees who join the Rise Up programme is measured by a specific indicator, monitored by the Group Executive Committee and the Board of Directors, which cannot be published for confidentiality reasons.

Long-term compensation

Since its Initial Public Offering, the Exclusive Networks Group has set up a free share allocation plan, which aims to associate and align the financial interests of the managers and a number of key contributors with those of the shareholders, as well as to retain them in the long-term. Shares vest only if performance conditions in line with the Group’s strategy are met, and also if the employee is still working in the company.

The performance indicators used for this first plan are based on the Group’s financial performance. The purpose of this additional compensation mechanism is to motivate and retain beneficiaries by directly involving them in the Group’s development.

Succession plans

To ensure business continuity, the Exclusive Networks Group has set up a succession plan for a number of strategic functions, both at a global and local level. Given the very tight labour market in the cybersecurity sector and for certain functions (section 4.1), the aim is to anticipate the departure of a key employee, so that it does not jeopardise the continuity of the organisation and the achievement of the company’s objectives.

The first phase consists in identifying these key functions, which may be management positions or highly specialised skills essential to the Group’s development. In a second phase, a survey is carried out internally with the support of Human Resources managers and managers, to identify employees likely to move into these positions in the short or medium term, as well as specific training plans to support their skills development. This is

why the succession plan is closely linked to the Rise Up programme. The Human Resources Department is also attentive to the diversity of the people identified in the succession plan, whether in terms of gender, profile or nationality.

Governance

All these measures are regularly reviewed by the Group's Executive Committee. The Long Term Incentive Plan and the succession plans are also submitted to the Nomination and Compensation Committee for approval and presented to the Board of Directors.

4.5 Training and skills development

The skills development policy of the Exclusive Networks Group is directly linked to the company's strategy. Two types of training are proposed to employees:

- "technical" training, which aims to help employees to maintain and develop their technical skills in their job. This training is essential in the cybersecurity sector, where innovation is constant. This may include training or certification provided by vendors on new products or technologies, which in some cases may require that staff working on these products be certified;
- training to develop the behavioural and personal skills of employees (soft skills).

New skills development programme

Following the findings of the first annual employee engagement survey conducted in 2021, the Exclusive Networks Group committed to implementing a professional and personal development programme for its employees.

The Group's Human Resources Department therefore launched a pilot programme in the form of an e-learning platform, under the slogan "Learn, Commit, Grow: a unique experience to be at the heart of your personal development". This campaign was sent to a first group of employees, identified by their managers in collaboration with local HR managers.

The encouraging results and the involvement of employees in this programme led the Group to renew it in 2022 and to extend it to more than 600 people, including employees identified as "talents" (see section 4.4).


The personal development platform selected by the Human Resources Department is recognised as a best in class, with a digital library of more than 16,000 courses covering a wide range of technical, business, software, marketing and creative subjects, available in more than 10 languages.

The benefits of this programme are:

- unlimited personal access;
- multi-device access;
- multiple formats available (videos, courses, learning programmes);
- flexible duration (from two minutes to several hours);
- several levels, from beginner to advanced;
- personalised course recommendations.

Throughout the year, the main training modules taken are leadership and management, security, business software and sales. Examples of modules that were popular with employees include "Cybersecurity Basics", "Six Morning Habits of Effective People", "Improving Concentration" and "Expressing Yourself Confidently and Effectively"...

[GRI 404-2-a]

Actions	2022 results
Maintain and develop the technical and business skills of employees	674 certified employees with 1,395 new certifications
Implement a personal development programme [GRI 404-1-a]/SDG 4.3 & 4.4	228 video courses, i.e. nearly 10 hours per employee
	524 employees attended at least one course
	152 employees attended at least one training module (>3 hours)
	€955,000 committed to all training programmes, representing a contribution rate of 0.5% ^(a)

(a) Figures based on the full consolidation scope of the Group for consistency with the published accounts.

4.6 Exclusive Academy: tomorrow's skills

Launch of Exclusive Academy, a world-class cybersecurity training programme

In response to the global skills shortage, Exclusive Networks launched Exclusive Academy on 11 October 2022, a major concrete step forward to fill the talents and skills gap in the cybersecurity sector.

Thanks to the Exclusive Academy, an initiative firstly launched in France, some twenty participants will benefit from a three-year specialised training course given by highly qualified and fully operational cyber-experts, thus meeting the needs of the job market. As part of the Exclusive Academy, approximately 20 participants will benefit from specialised training over a three-year period, from highly qualified and operational cyber-experts who meet the needs of the job market. The Exclusive Academy will offer practical field experience as well as theoretical training, culminating in high level qualifications. The practical, hands-on experience in the field is a key differentiator for the programme. Students will spend 9 weeks working on technical projects in the field in the first year, 12 weeks in the second year and 14 weeks in the third year. The programme will also offer 12 weeks of classes in the first year, 10 weeks in the second and then 8 weeks in the final year.

The students will come from the partner schools Guardia (a cyber security school based in Paris and Lyon) and Oteria Cyber School (a cyber security school based in Paris), following interviews by Jean-Marc Muselli, Director of Services at Exclusive Networks France. The courses will be led by Exclusive Networks' trainers, security, and network engineers, who have a thorough knowledge of the brands and all the technologies distributed by the Group.

Jesper Trolle, CEO of Exclusive Networks, comments: "This is Exclusive Networks' response to a critical challenge facing the cyber industry: to recruit, train and retain experts to stay on the cutting edge of technology. Only 15% of cybersecurity professionals in the world got to their position through cybersecurity training. This creates a huge mismatch between the needs of the industry and the supply of training. Today, I am extremely proud of the work accomplished by the Exclusive Networks teams. With this initiative, we are providing a sustainable solution to one of the biggest cybersecurity challenges in the world and sending a strong message to students and young talents, but also to the entire cybersecurity ecosystem.

The Exclusive Academy programme will be extended to new countries in 2023.

[GRI 404-2-a]/SDG 4.3 & 4.4



4.7 Diversity, inclusion, equity and equal opportunities

The Exclusive Group is committed to providing a caring work environment that promotes well-being, diversity, equity and inclusion. As such, the Group seeks to recruit employees from diverse backgrounds across its global operations and to treat everyone fairly.

This approach is supported in 2022 by the formalisation of a Group Diversity, Equity and Inclusion Policy, which is currently being rolled out. This Policy is intended to be regularly updated, in line with progress made on the various indicators.

Diversity, Equity and Inclusion Policy of the Exclusive Networks Group

Diversity, Equity & Inclusion is the daily reality of how we live and work within the company and of how we interact together with our business partners. We embed diversity, equity & inclusion in our organization, promote equal access to opportunity for all our employees, and hold

our leaders accountable for all members of their teams. This is how we will continue to achieve superior business results, sustainable growth, and drive innovation, to keep our competitive advantage within our business.



This policy supports and aims at contributing to the achievement of the UN Sustainable Development Goals and in particular Goal 5. Exclusive Networks is committed to the achievement of these goals and has identified specific objectives to be achieved by 2025 with regular review and reporting.

To kick off the implementation of this Policy, the Group launched a training course for all employees in early 2023 to raise awareness of this important issue.

Governance and implementation

Governance

The Executive Committee is responsible for approving the diversity, equity and inclusion objectives and initiatives submitted to it by the Human Resources Department and for monitoring the results. Upon proposal from the Executive Committee, the Board decides on the gender balance targets in the managerial functions. The Executive Committee presents the Board with the methods of implementation, the results obtained during the previous year, including, where applicable, the reasons why the objectives were not achieved and remedial the measures.

Application

When implementing this Group Policy, the respective prevailing national and international law, and the respective cultural practices, as well as - if applicable - the rights of social partners must be observed. The necessary adjustments are to be made in cooperation with local Human Resources.

Reporting and future developments

The Exclusive Networks Group may have to adapt its processes and objectives in view of the progress made, or to take into account new needs and business objectives.

Objectives

With the launch of this new Policy, the Exclusive Networks Group wishes to focus its efforts on two major issues, each with an associated action plan, performance indicators and an implementation schedule.

Objective No.1: representation of women in management positions

The Group wants to increase the proportion of women in management positions at Group, regional and country level, and reach 40% by 2025.

Management positions refer to:

- members of the Group Executive Committee and their N-1;
- Regional General Managers;
- Country Managers and their Management Committee, in countries with revenue of more than €100 million.

The following indicators are monitored to achieve this objective:

- ensure that short lists for management positions include women;
- increase the proportion of women among the participants in the Rise-up Programme;
- increase the number of women in the Long Term Incentive Plan;
- increase the proportion of women returning to work after parental leave;
- increase the proportion of women promoted in the Group.

Objective No. 2: improve awareness and understanding of Diversity, Inclusion and Equity

The Exclusive Networks Group wishes to train its entire staff in diversity, equity and inclusion issues by 2025:

- 100% of employees undergo diversity, equity and inclusion training;
- 100% of managers undergo diversity leadership training.

The following indicators are monitored to achieve this objective:


- the percentage of employees and executives who have completed the training;
- the implementation of inclusive hiring processes.

A progress report will be presented annually to the Board of Directors on the initiatives implemented and on the progress of these objectives.

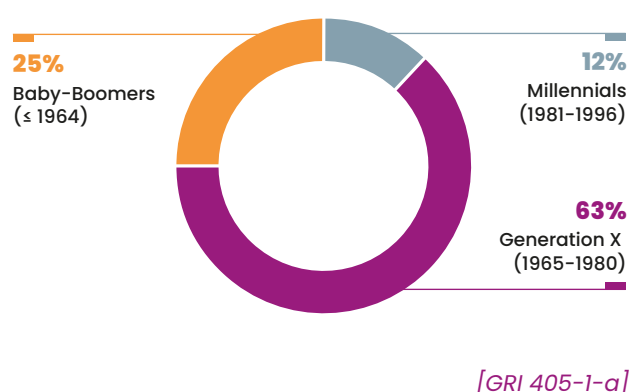
Attracting and retaining talent

Diversity, inclusion, equity and equal opportunities

Gender diversity in the Exclusive Networks Group

Actions	2022 results
Improve gender balance in the Group [GRI 405-1-a]/SDG 5.5 	38% of the members of the Board of Directors are women 24% of governance members are women 34% of management positions are held by women
[GRI 405-1-b]	41% of employees are women
[GRI 401-1-a]	40% of employees recruited are women

Age distribution of governance members



Average gender pay gap by employee category

The gender pay gap measures the difference between the average total remuneration of women compared with the average total remuneration of men by job level:

- the calculation is based on the total compensation of employees, including base salary, target variable compensation, and other benefits;
- the number of employees taken into account includes "permanent" employees, regardless of their contract, and not trainees and apprentices;
- for reasons of relevance, when there are fewer than five male or female employees per job level, the calculation is not made.

On the scope of this report, there is a pay gap of 11.6% in favour of men, considering that the calculation was not made for certain countries due to the minimum number of employees per level.

[GRI 405-2-a/405-2-b]/SDG 8.5



Gender Equality Index⁽¹⁾

Only Exclusive Networks SAS is subject to the Gender Equality Index, a regulatory indicator for French companies with more than 50 employees. In 2022, the index was 86/100.

[GRI 405-2-a]/SDG 5.5 & 8.5



Equity ratios

To be consistent with the information contained in the Board of Directors' corporate governance report found in Chapter 4 of the 2022 Universal Registration Document, the figures below take into account all Exclusive Networks' employees in France (fixed-term and open-ended contracts), continuously present throughout 2022, which constitute an enlarged scope representative of Exclusive Networks' activities in France.

Action	2022 results
Measure the equity ratio between the company's two most senior executives and employees [GRI 2-21]	Ratio of the Chairperson of the Board of Directors' compensation to average compensation: 3 Ratio of the Chairperson of the Board of Directors' compensation to median compensation: 4 Ratio of the Chief Executive Officer compensation to average compensation: 18 Ratio of the Chief Executive Officer compensation to median compensation: 25

(1) Index required by French legislation, applicable to France only.


4.8 Health and safety

Preserving staff health and safety

Within the scope of this report, there was only one work-related accident in 2022 that resulted in 15 days' absence from work, which explains a severity rate close

to zero (accidents that resulted in at least a one-day absence from work are taken into account).

The absenteeism rate is also low, including compared to service industries.

Action	2022 results
Protect health and ensure the safety of our employees [GRI 403-9-a]/SDG 8.8 	Frequency ratio: 0.28 <hr/> Severity rate: 0 <hr/> Absenteeism rate ^(a) : 1.80

(a) Absence is defined as the non-attendance at work when attendance was expected (parental leave is excluded).

As a result of the external growth carried out by the Exclusive Networks Group in recent years, the staff is spread over a large number of companies (see section 8.1). The nature of the Group's activities as well as the small number of employees per company explains why very few of them are certified according to a health and safety standard, without reflecting the importance of this subject for the Group and the commitment of the Human Resources Managers. As a result 10% of the workforce is represented in a collective health or safety body while 8% is employed in a company with a health and safety certification.

[GRI 403-1/403-4]

Improving health conditions at work: stress awareness month

In April, Exclusive Networks UK organised a stress awareness campaign for employees, proposing them a number of tips and activities to help them deal with stress. The campaign was organised in cooperation with the charity Mind, with which Exclusive Networks UK has a charity partnership for the year 2022 (see section 7.1), and whose philosophy is to raise public awareness about mental health.

The main advice was: to get some rest, time for yourself, exercise and if possible go outdoors. With this in mind, a number of activities were organised throughout the month to help each employee to take time to look after their own mental health and de-stress.

"Free time at 3pm": knowing that it can be difficult to find time for oneself, the company encouraged employees to choose a day to leave early and do something for themselves. Whether it was flying a kite, swimming, running, or trying something new, everyone was free to choose.

In the office, a number of activities were proposed in break rooms to help de-stress, such as books, crafts, board games or a yoga session. In addition, as research has shown that spending time with animals helps to reduce stress, animal visits were organised. To get out and about, group nature walks were proposed at lunchtime.

Employees were also able to take advantage of an online platform that offers secure and confidential information and advice on well-being and stress management.

[GRI 403-7]/SDG 3.4

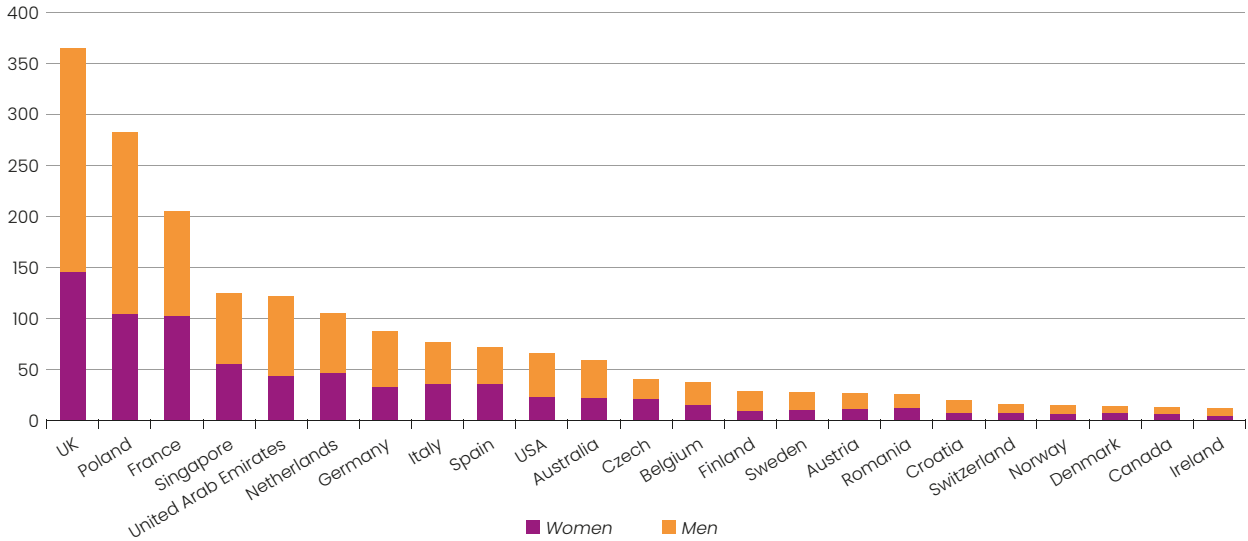


4.9 #WeAreExclusive

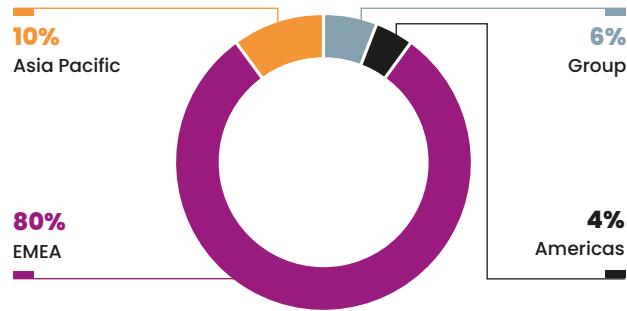
Average total workforce and breakdown of employees by country, age, gender and geographical area

For the scope used for this report, the average annual workforce for the year 2022 was 1,838 employees, 41% of whom are women and 59% men, distributed geographically as follows:

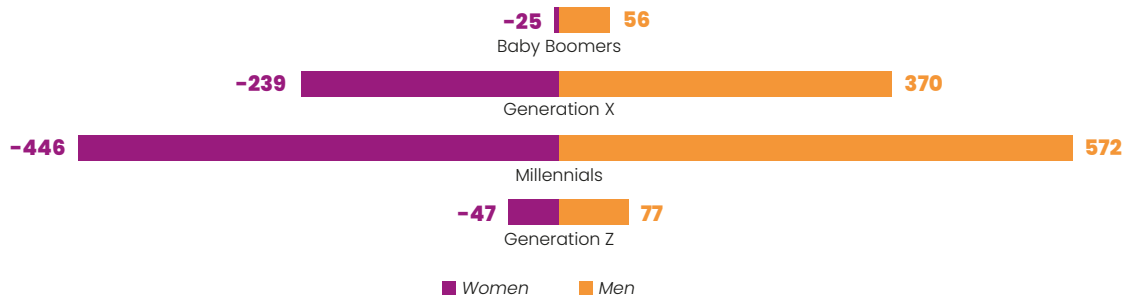
Average workforce by gender



Breakdown of the workforce by geographical area

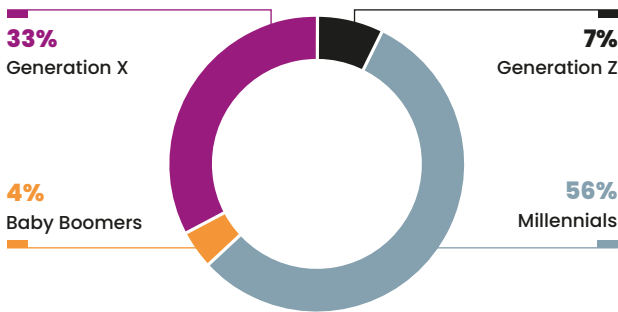


Age pyramid*



* Generation Z (<26 years), Millennials (26-41 years), Generation X (42-57 years), Baby Boomers (58 years and over).

Breakdown of the workforce by generation



For the scope of this report, the average age is just under 34 years, with more than half of the workforce belonging to the Millennials generation (between 26 and 41 years old).

Average length of service is 4.6 years and there was a net growth in the workforce of 6.7% in 2022.

[GRI 2-7-a/2-7-e]

Proportion of employees with fixed-term/ open-ended contracts

The Exclusive Networks Group offers stable employment contracts to its employees: 97% of the contracts are open-ended and of the remaining 3%, almost 2% are trainees or apprentices.

Breakdown of contracts: full-time and part-time

94% of employees work full time, with full-time recruitment being the norm. The vast majority of part-time employees have chosen to work on part-time contracts.

We note that this distribution differs according to gender: 11% of the Group's female employees work part-time, compared with 3% of the male employees.

Workforce as at 31 December 2022

As at 31 December 2022, there were 1,922 employees in the scope of consolidation of this report, and 2,558 in the Exclusive Networks Group as a whole (75% of the Group's workforce is covered by the extra-financial performance statement).

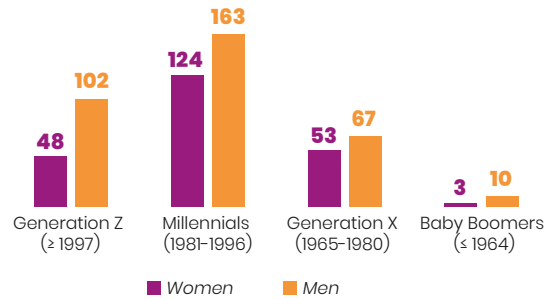
Based on the number of new hires and departures during the year, the Group's total workforce is up 5.7% compared with 31 December 2021.

[GRI 2-7-b]

Recruitments

On the scope taken into account for this report, 571 recruitments were made in 2022, distributed as follows:

Recruitment by generation and gender



As with the Group's workforce, 50% of recruitments involved employees from the Millennials generation (26 to 41 years). We also note that 26% of the employees who joined the Group were under 26, which can be explained by the setting up of the Exclusive Academy (see Chapter 4.6), and by a large number of interns and apprentices, a sign of the Group's community involvement to training young people.

The proportion in terms of parity is stable, with 60% of male new hires.

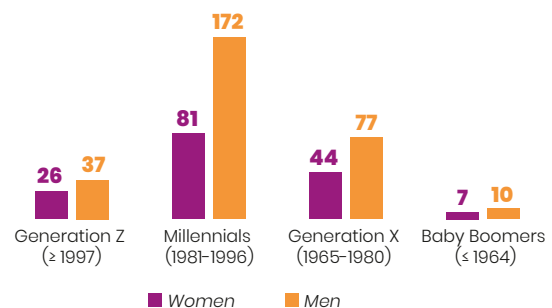
Geographically, the distribution of hires is close to that of the workforce, with 78% for the EMEA region, 10% for the Asia-Pacific region, 8% for the Group functions and 5% for the Americas region.

[GRI 401-1-a]

Departures

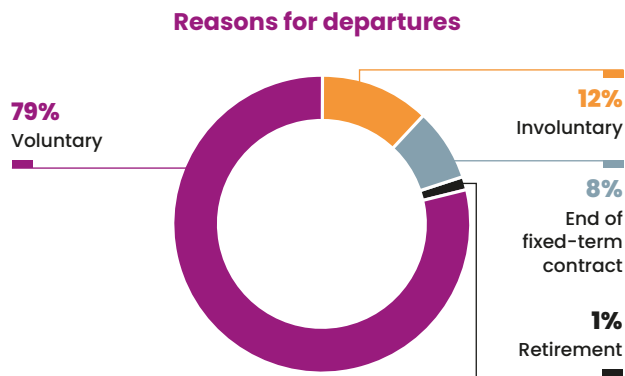
On the scope taken into account for this report, 455 people left the Group in 2022, with a slight over-representation of men, as well as the Asia-Pacific region and Group functions, that represent however only 16% of the total workforce.

Departures by generation and gender

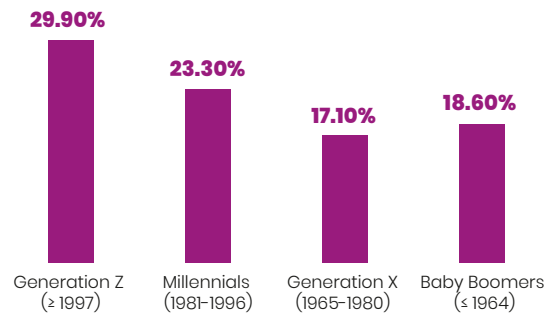


Attracting and retaining talent

#WeAreExclusive



Turnover of permanent employees



We note that in 80% of cases, it is the employee who chooses to leave the company, and half of the departures due to the end of a contract are attributable to the employee's student status (interns and apprentices). This situation reflects the strong skills shortage in the cybersecurity sector worldwide (see section 3.4.1). Technical engineers and sales functions are the professions with the highest turnover.

Among permanent employees, there is a correlation between turnover and age, with a gap of more than 10 points between Generation Z and Baby Boomers, and a turnover of men 30% higher than that of women.

[GRI 401-1-b]

Compensation and changes⁽¹⁾

The annual payroll for 2022, including salaries and social security contributions, taken from the consolidated financial statements of the Exclusive Networks Group, is €183 million, up 19% compared with 2021, as a result of the increase in the workforce, exchange rate impacts and the integration of acquisitions made in 2021.

(1) Figures based on the full consolidation scope of the Group for consistency with the published accounts.

5 Environmental footprint

5.1 Energy consumption

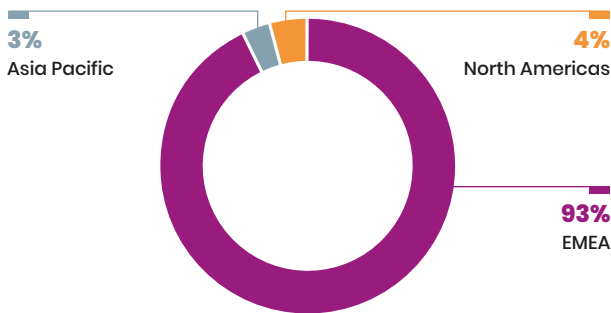
Energy consumption of the Exclusive Networks Group sites consolidated for this report (Scopes 1 and 2)

Categories	Quantities	Units	Scope
Heating oil	7,700	L	1
Diesel fuel from mobile sources	179,654	L	1
Petrol fuel from mobile sources	199,845	L	1
City gas heating	3,346,804	kWh	2
Electricity from mobile sources	29,846	kWh	2
Electricity	3,904,122	kWh	2
Of which renewable electricity	702,742	kWh	2
Heating network	24,519	kWh	2

[GRI 302-1-a/302-1-b/302-1-c]

Cumulatively, over the scope of consolidation of this report, energy consumption, including all energy sources, amounts to 8,894,627 kWh and is broken down as follows:

Geographical breakdown of energy consumption



[GRI 302-1-e]

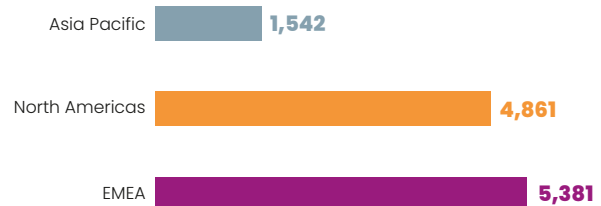
Internal energy intensity ratio

To calculate the internal energy intensity ratio, i.e. for Scopes 1 and 2 only, the total energy consumption is related to the average number of employees over the period. For 2022, the internal energy intensity ratio was 4,839 kWh per employee.

[GRI 302-3-d]/SDG 7.3



Energy intensity ratio by geographical area



There is a significant difference between the energy intensity of the Asia Pacific region compared with the other two geographic regions, as the only internal energy consumption in this region is electricity for the premises.

[GRI 302-3-a/302-3-b/302-3-c]

5.2 Carbon footprint

Greenhouse gas footprint of the Exclusive Networks Group

In 2022, for the scope of this report, the Exclusive Networks Group's consolidated greenhouse gas emissions amounted to 663,139 tonnes of carbon equivalent with an uncertainty of 14.3%, taking into account the limits described below.

Emission categories	No.	Emission items	CO ₂ (t CO ₂ e)	CH ₄ (t CO ₂ e)	
Scope 1	1-1	Direct emissions from stationary combustion sources	266	1	
	1-2	Direct emissions from mobile combustion sources	2,701	1	
	1-3	Direct emissions from processes	0	0	
	1-4	Direct fugitive emissions	0	0	
	TOTAL SCOPE 1			2,967	2
Scope 2	2-1	Indirect emissions from electricity consumption	1,445	0	
	2-2	Indirect emissions from the consumption of steam, heat or refrigeration	3	0	
	TOTAL SCOPE 2			1,448	0
Upstream Scope 3 emissions					
Scope 3	3-1	Purchased products and services	121,018	0	
	3-2	Fixed assets	28	0	
	3-3	Fuel and energy related emissions (not included in Scope 1 or Scope 2)	813	20	
	3-4	Upstream transportation and distribution	26,029	25	
	3-5	Waste generated	41	0	
	3-6	Business travel	660	0	
	3-7	Employee commuting	4,877	0	
	3-8	Upstream leased assets	0	0	
		Other indirect upstream emissions	0	0	
	Downstream Scope 3 emissions				
	3-9	Downstream transportation and distribution	3,936	22	
	3-10	Processing of sold products	0	0	
	3-11	Use of products sold	497,436	0	
	3-12	End of life of products sold	3,189	0	
	3-13	Downstream leased assets	0	0	
3-14	Franchises	0	0		
3-15	Investments	0	0		
	Other downstream indirect emissions	0	0		
TOTAL SCOPE 3			658,027	66	
TOTAL			662,442	68	

[GRI 305-1-a/305-2-a/305-3-a]

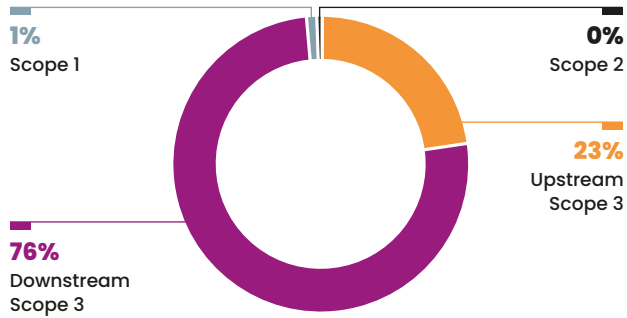
Greenhouse gas emissions

N2O (t CO ₂ e)	HFCs (t CO ₂ e)	PFCs (t CO ₂ e)	SF6 (t CO ₂ e)	Other gases (t CO ₂ e)	Total (t CO ₂ e)	CO ₂ b (t CO ₂ e)	Uncertainty (t CO ₂ e)
3	0	0	0	0	269	0	126
4	0	0	0	0	2,706	33	1,226
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
7	0	0	0	0	2,976	33	1,232
0	0	0	0	0	1,445	0	261
0	0	0	0	0	3	0	0
0	0	0	0	0	1,448	0	261
0	0	0	0	0	121,018	0	36,246
0	0	0	0	0	28	0	16
6	0	0	0	0	839	-33	298
368	0	0	0	206	26,628	0	17,156
0	0	0	0	0	41	0	25
0	0	0	0	0	660	0	98
0	0	0	0	0	4,877	0	1,911
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
22	0	0	0	0	4,000	0	1,210
0	0	0	0	0	0	0	0
0	0	0	0	0	497,436	0	84,357
0	0	0	0	0	3,189	0	3,020
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
396	0	0	0	206	658,715	-33	93,481
403	0	0	0	206	663,139	0	94,974

Environmental footprint

Carbon footprint

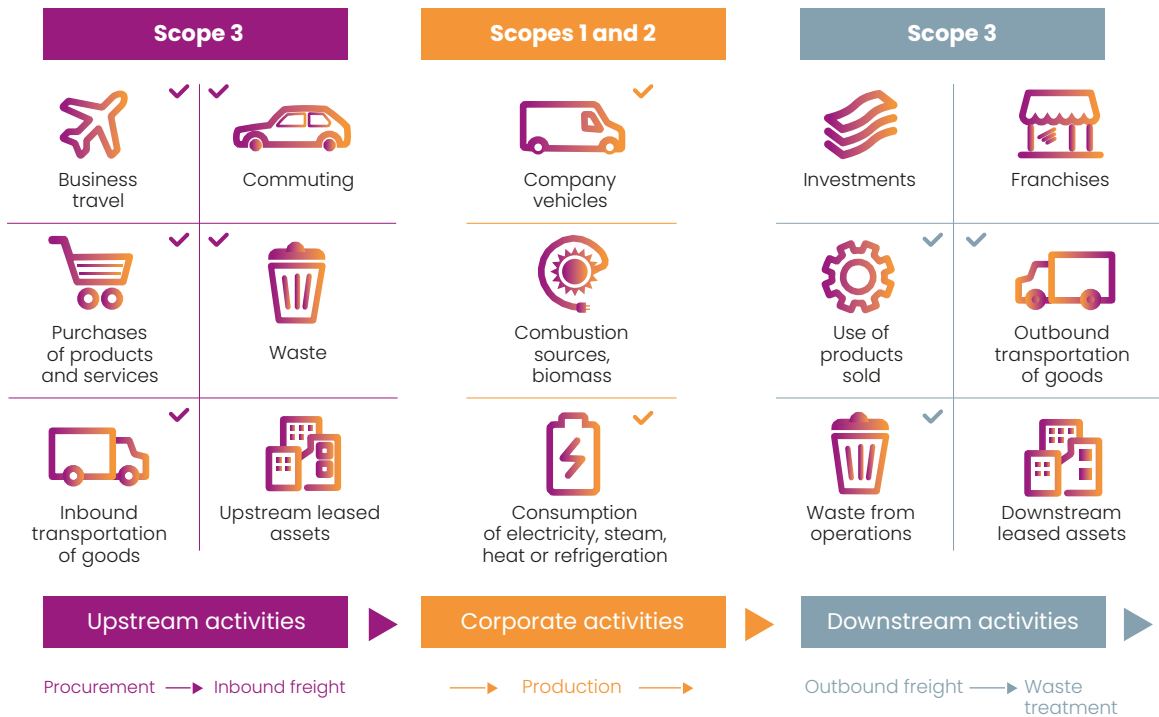
Breakdown of CO₂ emissions by scope



Like other companies whose activity is entirely tertiary, 99% of the Exclusive Networks Group’s carbon emissions fall under Scope 3, i.e. upstream and downstream of the Group’s own activities.

As the Scope 3 information is not under the company’s control, its collection requires the organisation of a specific project launched in 2022 and which will continue through 2023. As a result, the tables below identify the Scope 3 categories that have been considered for this report and those that are under process.

Exhaustive measurement of Scope 3 emissions will enable the Group to identify which actions should be implemented for reducing its greenhouse gas emissions, to assess them and to plan them out with a view to establishing its decarbonation trajectory.



Items	Recorded	Comments
Scope 1		
1 Direct emissions from stationary combustion sources	YES	Based on invoices.
2 Direct emissions from combustion engine mobile sources	YES	Fuel consumption
3 Direct emissions from non-energy processes	NO	Not applicable.
4 Direct fugitive emissions	NO	Data not available in rented premises.
5 Emissions from biomass (soil and forests)	NO	Not applicable.
Scope 2		
6 Indirect emissions from electricity consumption	YES	Based on invoices.
7 Indirect emissions from the consumption of steam, heat or refrigeration	YES	Based on invoices.
Scope 3		
8 Energy-related emissions not included in the "direct GHG emissions" and "indirect energy GHG emissions" categories	YES	Automatic calculation in the ADEME tool based on estimates.
9 Purchases of products or services	YES	Partial calculation on products only, approximately 1,500 tonnes of material including packaging. The calculation for services will be carried out in 2023.
10 Capital goods	YES	Partial calculation on computer equipment and vehicles held (property leases and vehicle leasing will be carried out in 2023).
11 Waste	YES	Extrapolation of 2021 figures.
12 Upstream transportation of goods	YES	Data extracted from the balance sheets of logistics operators.
13 Business travel	YES	Extrapolation of data extracted from centralised travel agencies.
14 Upstream leased assets	NO	
15 Investments	NO	
16 Transport of visitors and clients	NO	
17 Downstream transportation of goods	YES	Extrapolation of data from the balance sheets of logistics operators on the basis of "upstream mass = downstream mass".
18 Use of products sold	YES	Electricity consumption in the country of sale, estimated for a five-year life span (0.65MWh/kg hardware).
19 End of life of products sold	YES	Application of the electronic waste emission factor from the ADEME database to the mass sold.
20 Downstream franchise	NO	Not applicable.
21 Downstream leased assets	NO	
22 Employee commuting	YES	Extrapolation of 2021 figures.
23 Other indirect emissions	NO	

[GRI 305-3-d]/SDG 7.3, 12.4 & 12.5



Given:

- that the products marketed are imported from the vendors' manufacturing sites, which are mainly located in Asia;

- that stocks are limited, given the very large number of references and the speed with which these devices evolve to guarantee their effectiveness,

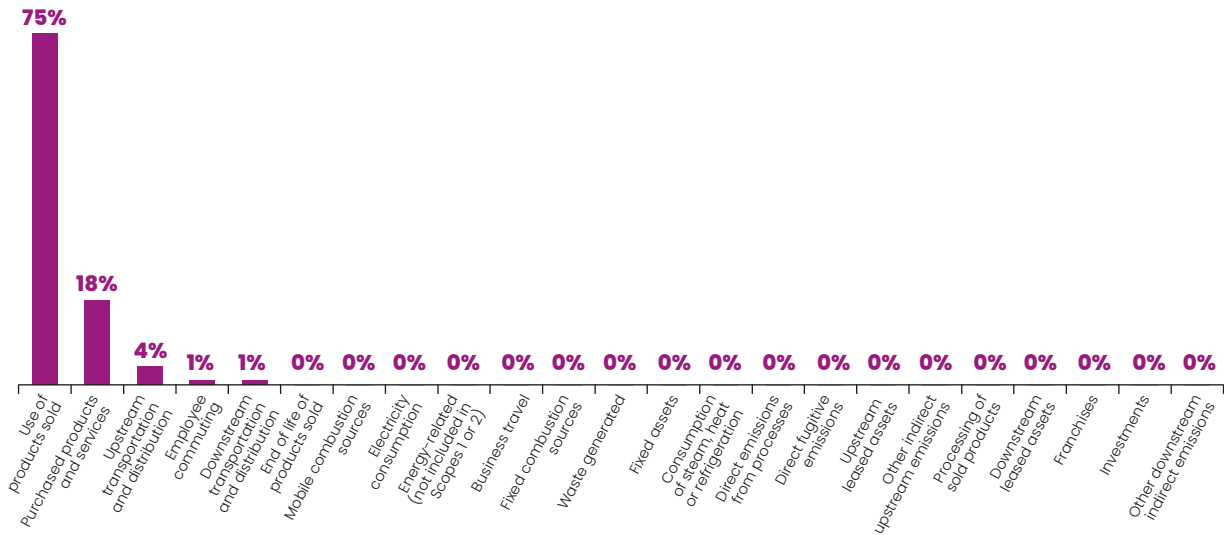
It is not currently possible to use rail or waterway transport for these materials.

Environmental footprint

Carbon footprint

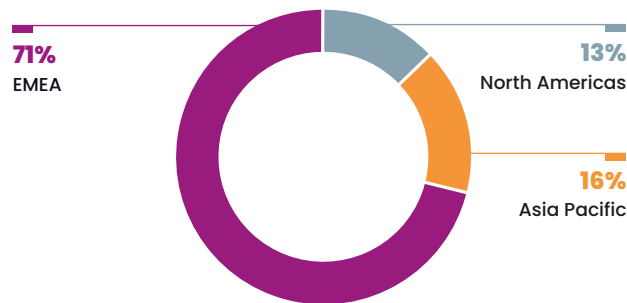
Breakdown of CO₂ emissions by category and geographical area

Breakdown of CO₂ emissions by category

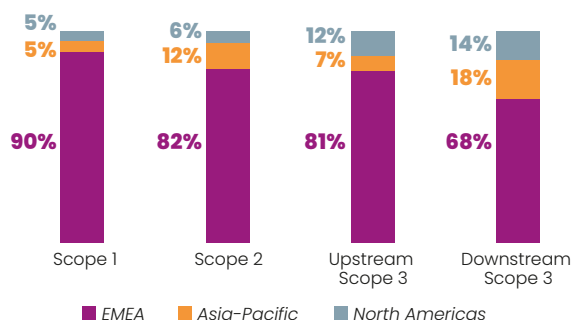


The chart above illustrates the Group’s main carbon footprint issues, with the use of products sold accounting for 74% of the total. It should be noted that the “products and services purchased” category is expected to increase, as only the impact of products has been taken into account at this stage.

Geographical breakdown of emissions



Geographical distribution of emissions by scope



The relative differences in downstream Scope 3 are explained by the higher electricity emission factor in the Asia-Pacific and North America regions, which penalises the “use of products sold” item.

For the calculation of the Greenhouse Gas Emissions Assessment:

- the following greenhouse gases were taken into account, converted into tonnes of CO₂ equivalent (or tCO₂e) according to their Global Warming Potential: CO₂, CH₄, N₂O, HFC, SF₆, PFC, NF₃ and CFC;
- the Group’s carbon footprint was calculated using the ADEME-Association Bilan Carbone (ABC) calculation tool in its version 8.8 of October 2022, following the rules of the GHG Protocol and with a level of uncertainty for each item. This tool allows results to be displayed in several standard formats, including the GHG Protocol format;
- the emission factors are taken from the ADEME database, unless otherwise stated.

[GRI 305-1-b=>g/305-2-b=>g/305-3-b=>g]

GHG emissions intensity ratio

For the scope determined for this report, the greenhouse gas intensity ratios calculated on the number of employees and on turnover are as follows:

Action	2022 results
Measure and monitoring greenhouse gas intensity ratios [GRI 305-4-a/305-4-b/305-4-c/305-4-d/305-4-f/305-4-g]	2.4 tCO ₂ e/employee (GHG intensity Scopes 1 and 2)
	357.7 tCO ₂ e/employee (GHG intensity for all scopes)
	GHG intensity Scopes 1 and 2 on revenue: not significant
	0.22 tCO ₂ e/€k (GHG intensity for all scopes)

5.3 Other environmental indicators

5.3.1 Water consumption

On the scope of consolidation defined for the year 2022, the total water consumption of the Exclusive Networks Group is estimated at 22,153 m³.

Since the Group rents all the sites from which it operates, for the vast majority of countries it was not possible to collect the exact water consumption, as this information was not made available by the lessors. This is due to the nature of the leases which, in some countries, may consist of a rental price per sq. meter including energy, water, as well as services such as cleaning, waste collection, etc.

As a result an estimate of consumption has been calculated on the basis of an average of 50 litres of water consumed per employee per day, multiplied by the number of days worked in the 23 countries.

It should be noted that this estimate is probably over-estimated, given the large number of countries where employees are allowed to work remote several days a week.

[GRI 303-5-a/303-5-d]

5.3.2 Waste

Description of waste generated by the company's activity and/or in its value chain

Since the Group rents all the sites from which it operates, in most countries it was not possible to determine the precise volume of tertiary waste. In fact, this information is often not known by the lessors, because household waste is collected by municipal services who do not weigh it or give a breakdown by occupant. Furthermore, in some countries, leases consist of a rental price per sq. meter including energy, water, as well as services such as cleaning, waste collection, etc.

As a result an estimate was calculated based on an average of 120 kilograms of tertiary waste per employee per year, half of which is paper or cardboard⁽¹⁾, multiplied by the average workforce in the 23 countries.

It is also not possible to identify the nature of the Group's downstream waste treatment, which is managed either by municipalities or by private service providers, which in both cases don't disclose information per occupant.

The Exclusive Networks Group takes all the necessary steps to ensure that the waste generated by its activities is sorted so that it can be recycled or recovered, as far as local waste treatment structures allow.

[GRI 306-1/306-3-b]/SDG 12.4 & 12.5



Action	2022 results
Identify and measure waste related to the company's direct activity [GRI 306-3-a]	110t: household waste
	110t: paper and cardboard
	224.4t: Waste Electrical and Electronic Equipment (WEEE)

(1) Source: ADEME guide to workplace eco-responsibility ("Écoresponsable au bureau"), September 2022.

5.4 Green Taxonomy

5.4.1 What is the Green Taxonomy?

European Regulation (EU) 2020/852 of 18 June 2020, known as the "Taxonomy Regulation", is one of the flagship measures of the European Green Pact, which aims to:

- redirect capital towards sustainable investments;
- managing the financial risks of climate change and related social issues;
- promote transparency and a long-term view of economic and financial activities.

The Taxonomy establishes a classification system for economic activities that can be considered environmentally sustainable, distinguishing between activities carried out on behalf of clients, investments and ongoing operations. Three indicators are therefore expected, expressed as a percentage of the "alignment":

- revenue;
- capital expenditure (CapEx);
- operating expenditure (OpEx).

An "aligned" activity is one that is considered sustainable because it contributes to one or more of the following environmental objectives:

- climate change mitigation;

- adaptation to climate change;
- sustainable use and protection of water and marine resources;
- transition to a circular economy;
- pollution prevention and control;
- the protection and restoration of biodiversity and ecosystems.

Note: for 2022, only the first two objectives were to be considered.

The classification of activities is based on a five-step approach:

- identify the activities considered "taxonomy-eligible", based on the Delegated Regulation (EU) 2021/2139 of 4 June 2021;
- qualify the substantial contribution of the activity to the environmental objective;
- ensure that the activity Does Not Cause Significant Harm to any of the objectives;
- ensure compliance with the OECD and UN guidelines for business, in particular with regard to fundamental rights at work and human rights;
- calculate the indicator by relating aligned activities to total activities.

5.4.2 Green Taxonomy indicators

Revenue indicator

As stated in the business model presented in chapter 1, the Exclusive Networks Group is a global cybersecurity specialist that markets a wide range of services and products to its partners and end customers. These activities are not listed in the appendices of the

Delegated Regulation (EU) 2021/2139 of 4 June 2021 as contributing substantially to the first two environmental objectives, neither because of their activity code, nor because of their description. As such, they are not eligible.

As a result for 2022, the share of the Exclusive Networks Group's revenue from services or products falling under taxonomy-aligned economic activities was 0%.

Proportion of turnover from products or services associated with Taxonomy-aligned economic activities - disclosure covering year 2022

Economic activities (1)	Code(s) (2)	Absolute turnover (3) €	Proportion of turnover (4) %	Substantial contribution criteria					
				Climate change mitigation (5) %	Climate change adaptation (6) %	Water and marine resources (7) %	Circular economy (8) %	Pollution (9) %	Biodiversity and ecosystems (10) %
A. TAXONOMY-ELIGIBLE ACTIVITIES				0%					
A.1 Environmentally sustainable activities (Taxonomy-aligned)									
Activity 1 [1]			%	%	%	%	%	%	%
Activity 2			%	%	%	%	%	%	%
Turnover of environmentally sustainable activities (Taxonomy-aligned) (A.1)		- €	0%	%	%	%	%	%	%
A.2 Taxonomy-Eligible but not environmentally sustainable activities (not Taxonomy-aligned activities)									
Activity 1									
Activity 3									
Turnover of Taxonomy-eligible but not environmentally sustainable activities (not Taxonomy-aligned activities) (A)		- €	0%						
TOTAL (A.1 + A.2)		- €	0%						
B. TAXONOMY-NON-ELIGIBLE ACTIVITIES									
Turnover of Taxonomy-non-eligible activities (B)		€3,404 million	100%						
TOTAL (A + B)		€3,404 MILLION	100%						

DNSh criteria

('Does Not Significantly Harm')

Climate change mitigation (11)	Climate change adaptation (12)	Water and marine resources (13)	Circular economy (14)	Pollution (15)	Biodiversity and ecosystems (16)	Minimum safeguards (17)	Taxonomy-aligned proportion of turnover, year N (18)	Taxonomy-aligned proportion of turnover, year N-1 (19)	Category (enabling activity) (20)	Category (transitional activity) (21)
Y/N	Y/N	Y/N	Y/N	Y/N	Y/N	Y/N	%	%	E	T
							%		E	
							%			
							%			
							%		%	

Environmental footprint

Green Taxonomy

Capital expenditure (CapEx) indicator

The CapEx to be considered corresponds to new acquisitions of plant, property and equipment and intangible assets during the financial year, before depreciation, amortisation or re-evaluation. Thus, the new rights of use of the leased assets are taken into account as soon as the lease contracts are signed, and not the financing terms. Capital expenditure also includes new assets resulting from business mergers carried out during the year.

For 2022, capital expenditure amounted to €23.7 million for the Exclusive Networks Group, distributed as follows:

- intangible assets: €1.1 million corresponding to IT developments;
- property, plant and equipment: €4.8 million corresponding to demonstration and office equipment;
- right of use: €17.8 million corresponding to new rental leases as well as new vehicle leasing contracts.

Proportion of CapEx from products or services associated with Taxonomy-aligned economic activities – disclosure covering year 2022

Economic activities (1)	Code(s) (2)	Absolute CapEx (3) Currency	Proportion of CapEx (4) %	Substantial contribution criteria					
				Climate change mitigation (5) &	Climate change adaptation (6) %	Water and marine resources (7) %	Circular economy (8) %	Pollution (9) %	Biodiversity and ecosystems (10) %
A. TAXONOMY-ELIGIBLE ACTIVITIES									
A.1 Environmentally sustainable activities (Taxonomy-aligned)									
Activity 1[1]			%	%	%	%	%	%	%
Activity 2			%	%	%	%	%	%	%
CapEx of environmentally sustainable activities (Taxonomy-aligned) (A.1)		- €	0%	%	%	%	%	%	%
A.2 Taxonomy-Eligible but not environmentally sustainable activities (not Taxonomy-aligned activities)									
Activity 1									
Activity 3									
CapEx of Taxonomy-eligible but not environmentally sustainable activities (not Taxonomy-aligned activities) (A.2)		- €	0%						
TOTAL (A.1 + A.2)		- €	0%						
B. TAXONOMY-NON-ELIGIBLE ACTIVITIES									
CapEx of Taxonomy-non-eligible activities (B)		€24 million	100%						
TOTAL (A + B)		€24 MILLION	100%						

Eligible capital expenditure comprises expenditure that is:

- related to potentially sustainable activities;
- part of a plan to make or expand a sustainable activity;
- related to economic activities referred to as "individual eligible measures" in the Taxonomy aimed at reducing the environmental footprint of the company, such as expenditure on premises, vehicles and data hosting.

Within the meaning of the Delegated Regulation (EU) 2021/2139 of 4 June 2021, the activities of the Exclusive Networks Group are not considered to contribute substantially to the first two environmental objectives and are therefore not eligible. Therefore, only the capital expenditure relating to individual measures can be taken into account.

Since the Exclusive Networks Group did not incur any capital expenditure under these individual measures in 2022, the share of the Group's CapEx relating to eligible economic activities and consequently aligned with the Taxonomy is not significant.

DNSH criteria

(Does Not Significantly Harm')

Climate change mitigation (11)	Climate change adaptation (12)	Water and marine resources (13)	Circular economy (14)	Pollution (15)	Biodiversity and ecosystems(16)	Minimum safeguards (17)	Taxonomy-aligned proportion of CapEx, year N (18)	Taxonomy-aligned proportion of CapEx, year N-1 (19)	Category (enabling activity) (20)	Category (transitional activity) (21)
Y/N	Y/N	Y/N	Y/N	Y/N	Y/N	Y/N	%	%	E	T
Y	Y	Y	Y	Y	Y	Y	%		E	
Y	Y	Y	Y	Y	Y	Y	%			
							%			
							%			
							%			
							%			
							%			

Environmental footprint

Green Taxonomy

OpEx indicator

The OpEx to be considered includes those:

- related to eligible activities;
- which are part of a plan to expand or make an activity sustainable;
- related to economic activities referred to as “individual measures” in the Taxonomy aimed at reducing the company’s environmental footprint, such as expenditure on premises, vehicles and data hosting.

Not all operating expenses are to be taken into account. Only Research and Development costs,

building refurbishment costs, short term lease charges, maintenance, upkeep and repair of assets and any other direct expenditure related to the routine maintenance of property and equipment necessary for their proper functioning should be considered.

For 2022, operating expenses amounted to €332 million for the Exclusive Networks Group, distributed as follows:

- staff costs: €183 million;
- depreciation of assets: €73 million;
- other current and non-current operating expenses: €76.5 million, of which €27 million correspond to external expenses.

Proportion of OpEx from products or services associated with Taxonomy-aligned economic activities – disclosure covering year 2022

Economic activities (1)	Co- de(s) (2)	Absolute OpEx (3) Currency	Proportion of OpEx (4) %	Substantial contribution criteria					
				Climate change mitiga- tion (5) %	Climate change adap- tation (6) %	Water and marine resources (7) %	Circular eco- nomy (8) %	Pollu- tion (9) %	Biodi- versity and ecosys- tems(10) %
A. TAXONOMY-ELIGIBLE ACTIVITIES									
A.1 Environmentally sustainable activities (Taxonomy-aligned)									
Activity 1[1]			%	%	%	%	%	%	%
Activity 2			%	%	%	%	%	%	%
OpEx of environmentally sustainable activities (Taxonomy-aligned) (A.1)		- €	0%	%	%	%	%	%	%
A.2 Taxonomy-Eligible but not environmentally sustainable activities (not Taxonomy-aligned activities)									
Activity 1									
Activity 3									
OpEx of Taxonomy-eligible but not environmentally sustainable activities (not Taxonomy-aligned activities) (A.2)		- €	0%						
TOTAL (A.1 + A.2)		- €	0%						
B. TAXONOMY-NON-ELIGIBLE ACTIVITIES									
OpEx of Taxonomy-non-eligible activities (B)		€332 million	100%						
TOTAL (A + B)		€332 MILLION	100%						

The Exclusive Networks Group’s business model is based primarily on human resources. Consequently, operating expenses are mainly composed of staff expenses, depreciation of assets, and other operating expenses such as rentals, travel expenses, marketing and advertising expenses, which do not fall within the scope defined in the Taxonomy. Moreover, the Group does not have any Research and Development expenses.

Within the meaning of the Delegated Regulation (EU) 2021/2139 of 4 June 2021, the activities of the

Exclusive Networks Group are not considered to contribute substantially to the first two environmental objectives and are therefore not eligible. Therefore, only operating expenditure relating to individual measures can be taken into account.

Since the Exclusive Networks Group did not incur any operating expenditure under these individual measures in 2022, the share of the Group’s OPEX relating to taxonomy-eligible economic activities and consequently taxonomy-aligned activities is not significant.

DNSH criteria

(Does Not Significantly Harm')

Climate change mitigation (11)	Climate change adaptation (12)	Water and marine resources (13)	Circular economy (14)	Pollution (15)	Biodiversity and ecosystems (16)	Minimum safeguards (17)	Taxonomy-aligned proportion of OpEx, year N (18)	Taxonomy-aligned proportion of OpEx, year N-1 (19)	Category (enabling activity) (20)	Category (transitional activity) (21)
Y/N	Y/N	Y/N	Y/N	Y/N	Y/N	Y/N	%	%	E	T
Y	Y	Y	Y	Y	Y	Y	%		E	
Y	Y	Y	Y	Y	Y	Y	%			
							%			
							%			
							%		%	

Ethics, fair practices, compliance and security

Compliance governance and organisation

Furthermore, in response to Article R. 225-105 of the French Commercial Code and for the 2022 financial year:

- the Exclusive Networks Group's strategic orientations in terms of social, societal and environmental responsibility are defined by the Board of Directors, upon the proposal of the Executive Committee. Implementation is carried out locally at the country level.
- the Exclusive Networks Group has no provisions or guarantees for environmental risk;
- the resources allocated by the Group to the prevention of environmental risks and pollution are not significant.

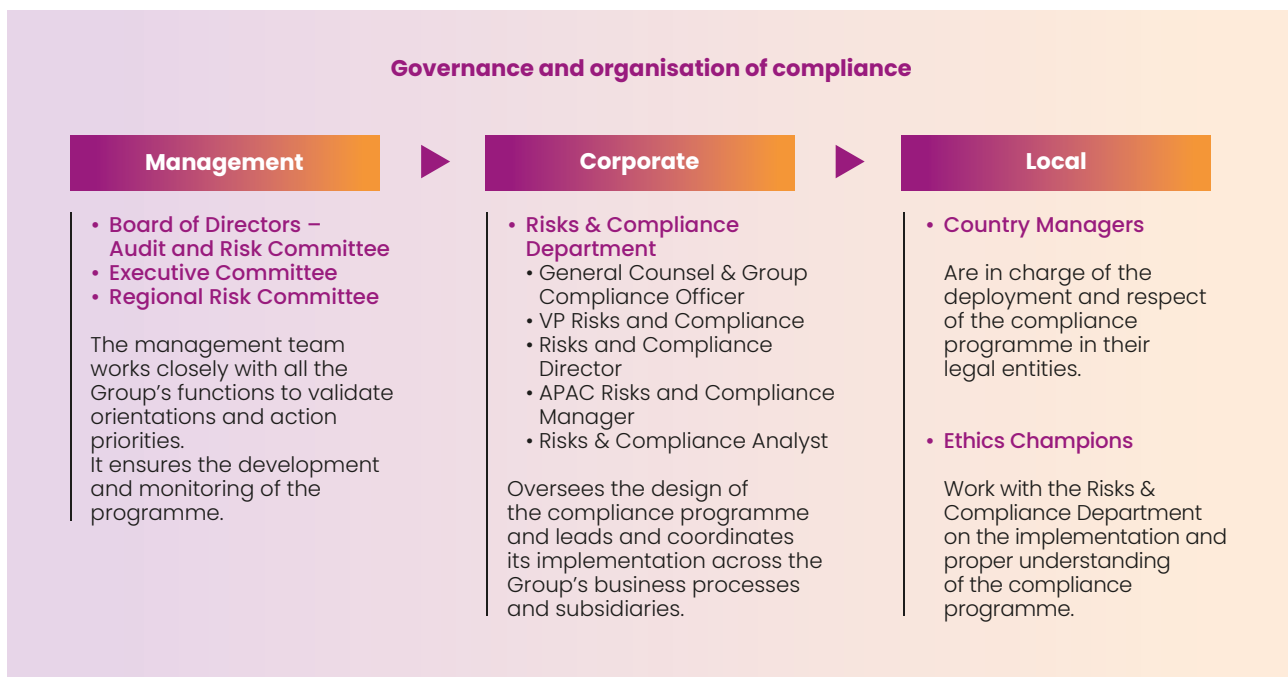
6 Ethics, fair practices, compliance and security

6.1 Compliance governance and organisation

In the conduct of its business, the Exclusive Networks Group promotes a culture of integrity and compliance, based on respect and adaptation to new standards and applicable legislation, both in France and in the

countries where it carries out its activities and where its employees operate.

A dedicated organization has been in place since 2013 to develop and manage the compliance programme.



At corporate level

The Group General Counsel & Group Compliance Officer:

- reports to the Group Chief Executive Officer on these matters;
- defines and organises the Compliance function and ensures its implementation within the Group;
- brings the issue before the various governance bodies (Group Executive Committee, Audit Committee, Board of Directors);
- decides freely, and at its sole discretion, on any internal investigation that it deems appropriate and which will be entrusted to Internal Audit.

The Risks & Compliance Director:

- reports to the Group General Counsel & Group Compliance Officer;
- designs the compliance program and first of all the one related to the anti-corruption system;
- manages and controls the implementation and updating of the programme, and leads the Compliance network within the Group;
- ensures a regulatory watch as well as best practices;
- organises and runs Compliance training courses within the Group;
- is the point of contact for the operational departments;
- contributes, where appropriate, to internal or external investigations relating to the programme, or likely to be initiated in the event of use of the internal whistleblowing system.

To comply with best practices and the recommendations of the supervisory authorities, in 2022 an internal reorganisation was carried out, aimed at separating the operational functions of the Risks & Compliance department, internal control and internal audit. The Risks & Compliance department is now independent and reports to the Group General Counsel & Group Compliance Officer. At the same time, an Internal Control department was created which reports to the Group Chief Financial Officer. The Internal Audit department reports to the Audit Committee as an independent control body.

At local level

- The Regional Risk Committee brings together the SVP of the region concerned, the Group General Counsel & Group Compliance Officer, the Internal Control Director, the Internal Audit Director, the Risks & Compliance Director, the Regional Finance Director, the Regional HR Director and the Regional Risks & Compliance Manager. It is already in place for the Asia Pacific region and will soon be implemented in the Europe, Middle East and Africa (EMEA) region.
- The Country Manager is responsible for the implementation and compliance with the programme in the legal entities under his/her responsibility.
- The Ethics Champions network implements the compliance programme in cooperation with the Risks & Compliance department, and ensures that it is properly taken into account and understood.

[GRI 3-3]/SDG 16.5



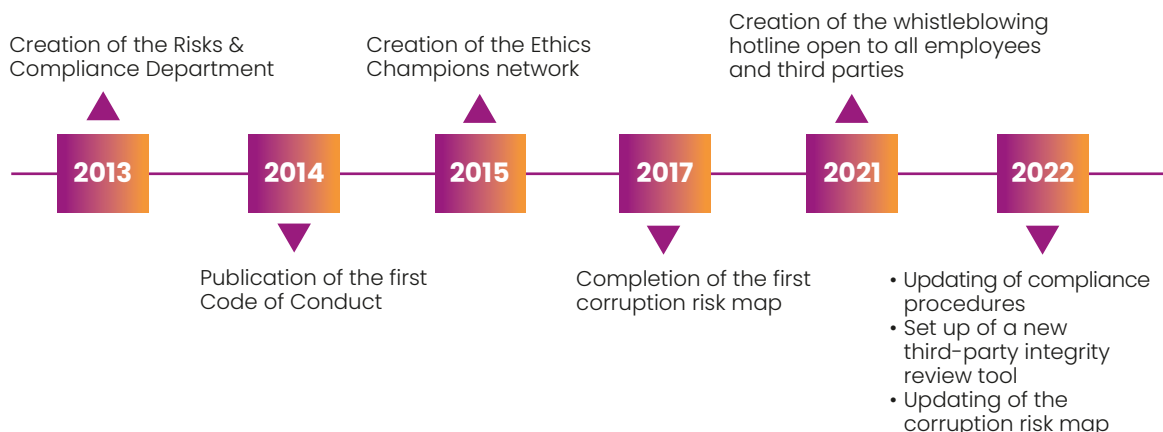
6.2 Ethics, prevention and anti-corruption

A mature compliance programme

The Exclusive Networks Group is strongly committed to adopting and promoting honest and ethical

behaviour in all its relationships and with all its partners. This principle has led the Group to define rules of conduct in terms of ethics, intended for its employees as well as for all its business partners and stakeholders.

Key dates in the Group's compliance policy

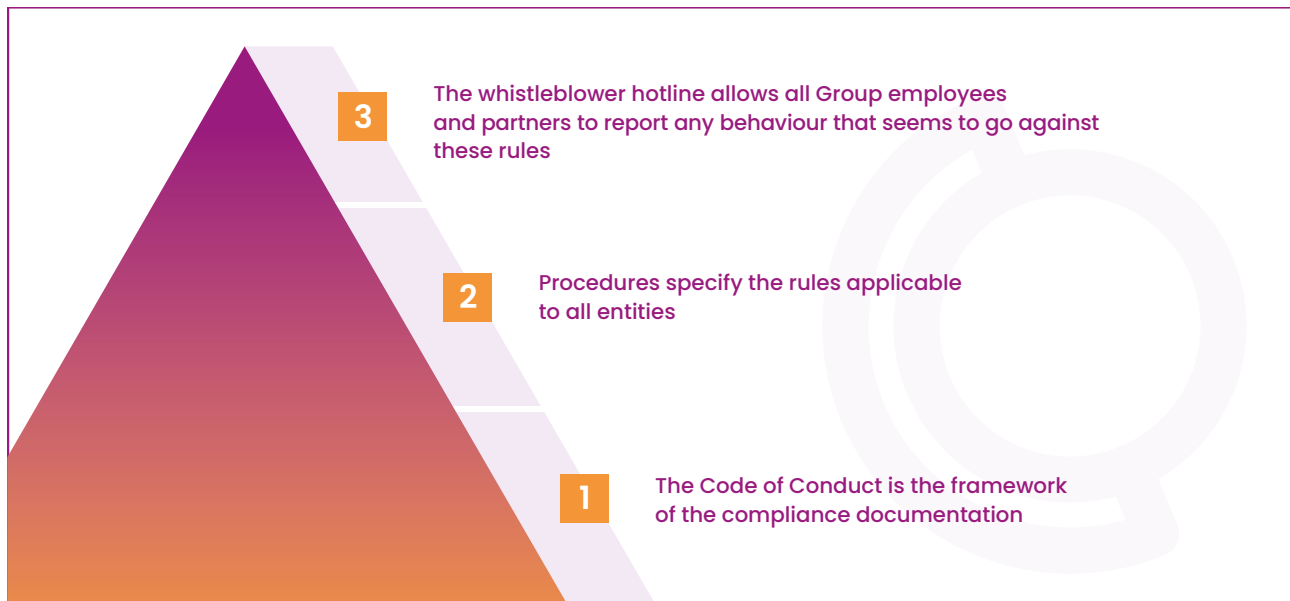


Ethics, fair practices, compliance and security

Ethics, prevention and anti-corruption

Through its internal policies and procedures, the Group establishes the guiding principles applicable to all its subsidiaries, intended to provide employees with the

rules of conduct and the behaviour to adopt in terms of business ethics and combating corruption. The compliance programme is structured as follows:



The policies and procedures that make up the Exclusive Networks Group's anti-corruption programme include the Code of Conduct, the Conflict of Interest Policy, or the Gifts and Entertainment Policy. All procedures and policies are addressed individually to each employee as soon as they are hired via the Group's e-learning platform. Employees complete an acknowledgement of receipt and a questionnaire to ensure that they understand them.

In order to strongly address the risk of corruption or non-compliance with internal business ethics rules and procedures (see Chapter 2 and section 2.3), the Exclusive Networks Group regularly updates and evolves its compliance programme, to take into account its corruption risk mapping as well as new regulatory and legal obligations.

In 2022, the Exclusive Networks Group updated and completed its corruption risk management system on three major dimensions:

- risk matrix;
- third party due diligence;
- employees' training.

[GRI 3-3-c]/SDG 16.5



Update of the corruption risk matrix

The Group's activities and processes are subject to regular risk assessment (see Chapter 2), which aims to provide appropriate and proportionate remediation solutions to detect and prevent these risks.

In 2022, Exclusive Networks undertook a complete overhaul of its corruption risk matrix, in accordance with the recommendations of the supervisory authorities. This major project covers all of the Group's operating companies. Supported by all the Group's functions and an independent consultancy firm, the methodology was designed taking into account the recommendations of the French Anti-Corruption Agency and best practices according to international standards.

This 8-month project is being carried out according to the following process:

- kick-off with by the Executive Committee;
- inventory of risks and controls in place;
- interviews conducted first with the Country Managers and Ethics Champions, to enable the preparation of workshops for all companies, gathered by country or region;
- country-specific workshops, with the participation of employees from various functions and reporting levels, each of them aiming to identify the main risks, processes and controls in place, and possible actions;
- summary of the working groups and preparation, by company and then at Group level, of gross and net risk matrix and remediation plans;

- presentation and validation with each Country Manager of the matrix and remediation plan by country (2023);
- presentation and validation by the Executive Committee and the Group Audit Committee of the matrix and remediation plans consolidated at Group level (2023).

This project has made it possible to map the corruption risks of each operational subsidiary. All the results are currently being consolidated and will lead to the updating of the action plan considering to the main net risks, taking into account the effectiveness of the measures already in place.

Actions	2022 results
Develop or update the corruption risk matrix for all the Group's operating companies	59 corruption risk matrices completed
Involve operational managers in the identification and prevention of corruption risks and take their vision into account	44 individual interviews conducted with Country Managers
Involve employees from all functions and reporting levels in the working groups to get a hands-on view	463 employees participated in the risk assessment

[GRI 205-1-b]/SDG 16.5





Third-party due diligences

All third parties with whom the Exclusive Networks Group is planning to initiate or continue a business relationship are subject to a specific and appropriate onboarding process, aimed at determining the level of the potential corruption risk of each third party, and implementing the necessary mitigation measures to ensure compliance with the ethical standards of the Group.

In 2022, the Group evolved the due diligence process for third parties and deployed a new dedicated tool to

ensure that third parties meet the company's ethical requirements. The tool is accessible to all employees and allows the company to quickly identify if there are any red flags, risk of corruption or ethical misconduct. When the tool detects red flags, the third party is considered to be "at risk": additional checks are then initiated and submitted to the Risks & Compliance department and the relevant Country Manager for validation.

This new third-party integrity review is being rolled out progressively and will continue in 2023.

Action	2022 results
Assess the integrity of third parties with whom the Group has or will have business relations [GRI 205-1-a]/SDG 16.5 	4,968 third parties assessed in the integrity review tool
[GRI 205-2-c]/SDG 16.5 	141 third parties with a medium or high risk formally approved the "Ethics & Code of conduct for third parties"

The Exclusive Networks Group has set itself the goal of completing 100% of the due diligence on high-risk third parties in 2023.

Communication, awareness and training actions

Since 2015, compliance training has been provided several times a year:

- by the Risks & Compliance department, during seminars organised face-to-face with the participation of the Group’s Chief Executive Officer at the beginning of the year, and more occasionally during the year, during face-to-face or online meetings;
- by the Ethics Champions, directly with their local teams, after having themselves been trained by the Risks & Compliance Department;

- by the Risks & Compliance Department, when a new Chief Financial Officer or Country Manager is onboarded.

Training courses organised by the Risks & Compliance department are adapted to the functions of the participants (marketing, finance, Executive Management or Ethics Champions) whenever possible. The courses organised by the Ethics Champions are usually for all employees in the region, based on the training materials prepared by the Risks & Compliance department.

Action	2022 results
Train our employees to Ethics and combating corruption	45 training sessions organised
	13 Onboarding* sessions conducted with the Internal Control department
	One Ethics Champions training course

* Onboarding: integration process of new Financial Directors or Country Managers.

The Exclusive Networks Group has set itself the objective that 100% of its employees will have certified⁽¹⁾ the Code of Conduct by 2025.

[GRI 205-2-e]/SDG 16.5



Whistleblowing system

In accordance with the whistleblowing procedure, employees are invited to notify the Group of any facts that may violate the principles of the Code of Conduct, particularly in the case of corruption. To this end, the Exclusive Networks Group has set up a whistleblowing system in all the countries where it operates, allowing each employee and external persons to send a report in a confidential and secure manner, accessible from the Group’s websites.

This system supplements other reporting channels, such as the line manager, the Human Resources Department, the Legal Department, etc.

All reports are treated confidentially under the supervision of the Group’s Ethics Officer, ensuring that there are no sanctions or retaliatory measures for any person who makes a report in good faith. This principle is guaranteed by the Group and reaffirmed in the whistleblowing procedure.

Action	2022 results
Establish a procedure and system for collecting and handling alerts, enabling employees and third parties to report situations that are contrary to the Code of Conduct or that may constitute a crime, offence or harm to the general interest.	62% of employees certified in the whistleblowing procedure*
	Four alerts received on the platform, three of which were admissible

* Certified: refers to employees who have acknowledged receipt of the procedure and have passed the comprehension test.

All alerts are internal, and no alerts from external stakeholders have been received.


[GRI 2-26]

1 Certified: refers to employees who have acknowledged receipt of the procedure and have passed the comprehension test.

Management of the compliance programme

Regular audits are conducted jointly by the Group’s Internal Audit department and an independent

consulting firm. They conduct tests and interviews to identify risky practices or any deviations and the corrective actions to be taken.

Action	2022 results
Control, monitor and evaluate the implementation of the Group’s compliance programme [GRI 205-3]/SDG 16.5	14 audits carried out covering anti-corruption
	No proven cases of corruption identified
	No employees dismissed or sanctioned for corruption
	No conviction for corruption against the Exclusive Networks Group, one of its subsidiaries or one of its employees

The Exclusive Networks Group has set itself the objective that all countries will be audited at least every five years covering anti-corruption, and that the audit plan will cover 30% of the revenue.

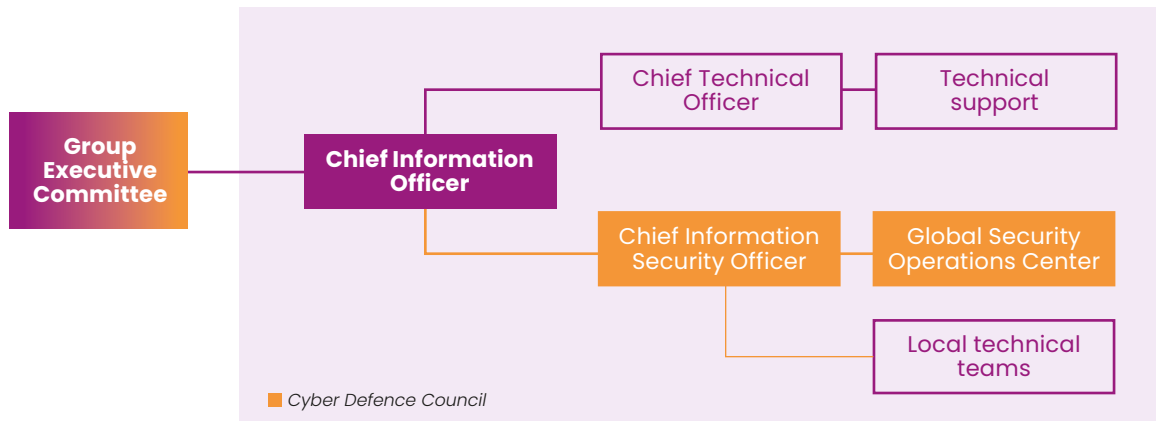
6.3 Cybersecurity governance and organisation

IT systems security organisation inside the Group

Within the Exclusive Networks Group, the IT systems security department is under the authority of the Chief Information Security Officer (CISO). The CISO has full authority over the entire security infrastructure of the Group, both at the central level and in the countries where the Group operates.

The Group’s security strategy is proposed by the CISO and approved by the Cyber Defence Council, which reports to the Group Chief Information Officer (CIO), himself a member of the Group Executive Committee. To ensure effective deployment of the policy and related security measures, there is a functional link between the CISO and each of the local IT managers.

Security organisation



In parallel, the Global Security Operations Center (GSOC) department is in charge of managing security incidents in the entire Exclusive Networks Group, including local infrastructures and offices.

To do so, the GSOC department performs the following three duties:

- monitoring, incident response and reporting on the entire security infrastructure of the Group worldwide;

- deploying, configuring and managing all security infrastructure and devices to ensure a centralised, harmonised and automated global security standard;
- supporting the user helpdesk, infrastructure team and employees.

The GSOC department is further supported by an external Managed Endpoint Detection & Response service, which monitors and deals with security incidents

on a 24/7 basis and can initiate legal investigations if necessary.

The Cyber Defence Council

The mission of the Exclusive Networks Group's Cyber Defence Council is to strengthen the skills, cooperation and information sharing of cyber defence with the countries in which the Group is present.

It is made up of the Group's main IT managers as well as delegates from each country, and meets very regularly. In cooperation with vendors, partners, other Group departments and subsidiaries, it is the body that enables the Group to:

- deploy cybersecurity tools, incident response services and assessment to protect the Group's networks from cyber threats;

- protect against cyberattacks;
- upgrade the infrastructure to make it more secure and resilient to new potential threats.

Governance

The CISO writes and regularly updates the policies, processes and procedures related to the cyber defence of the Exclusive Networks Group. Examples are the General Security Policy, the Security Incident Management Plan or the Usage Policy.

All these policies have been communicated individually to each employee via the Group's e-learning platform and are available on the Group's Intranet.

6.4 Information system protection

Deployment of security tools: protecting the company's activities from cyber attacks

Over the past 18 months, the following security tools have been deployed in a centralised, standardised and automated process:

1. Asset management: life cycles, asset and software inventory;
2. Security Information and Event Management and User and Entity Behavioural Analysis, using artificial intelligence;
3. Email security;
4. Managed Endpoint Detection & Response, using artificial intelligence and behavioural analysis;
5. Vulnerability management;
6. Endpoint and patch management;
7. Identity and Access Management, using artificial intelligence and behavioural analysis;
8. Cloud Access Security Broker and Secure Access Service Edge using artificial intelligence and behavioural analysis;

9. Security Orchestration Automation and Response (SOAR);
10. Threat Intelligence: a Malware Information Sharing Platform (MISP) instance that enables the identification, analysis and sharing of cyber threat intelligence with other organisations.

Most of the selected vendors and solutions come from the portfolio of the Group's cybersecurity products and solutions, and are recognised as "Magic Quadrant leaders" by Gartner, the renowned technology evaluation firm.

One of the tools used to evaluate the security of the information system is the Cyber Exposure Score, and the Group has set itself the objective of achieving a score of less than or equal to "Low" on this index by 2025.

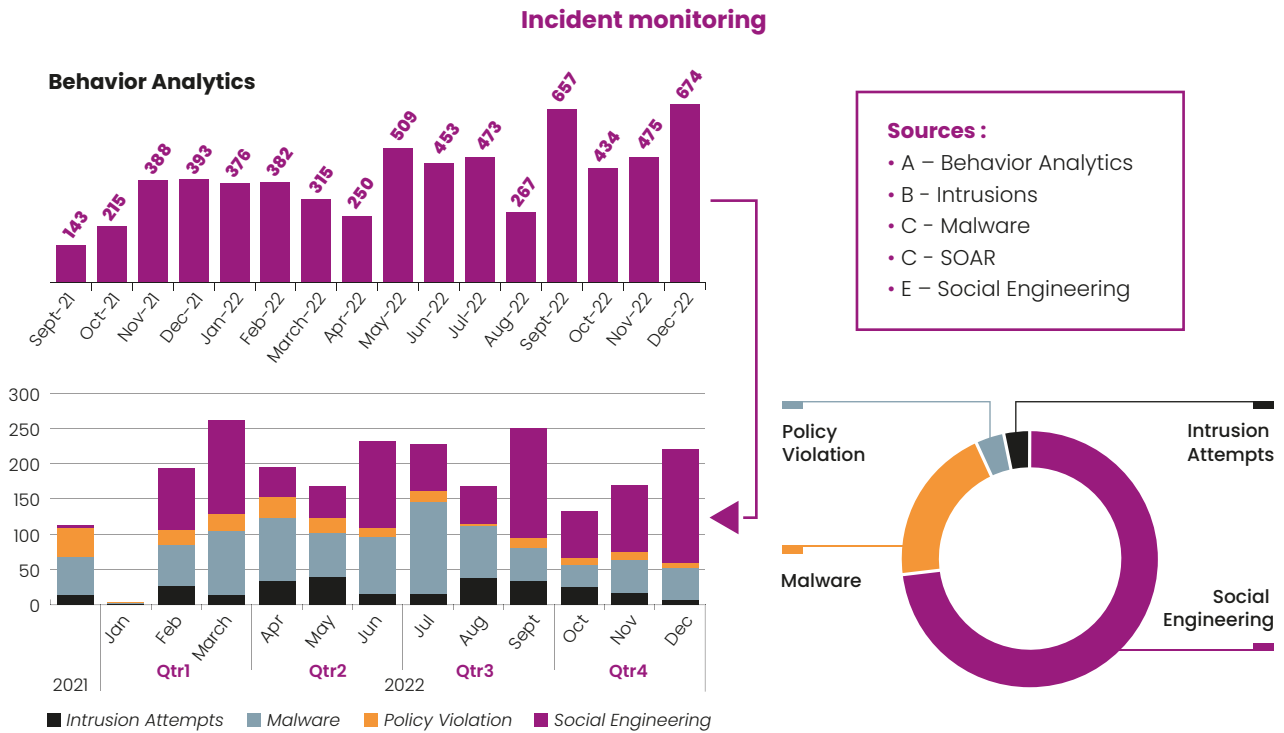
[GRI 3-3-c]

Reporting

Regular reporting is carried out and sent to the Group Chief Information Officer and the Cyber Defence Committee.

It is based on a security incident management plan, which determines a classification, processes and associated procedures.

Example of a report* presented to the Cyber Defence Committee:



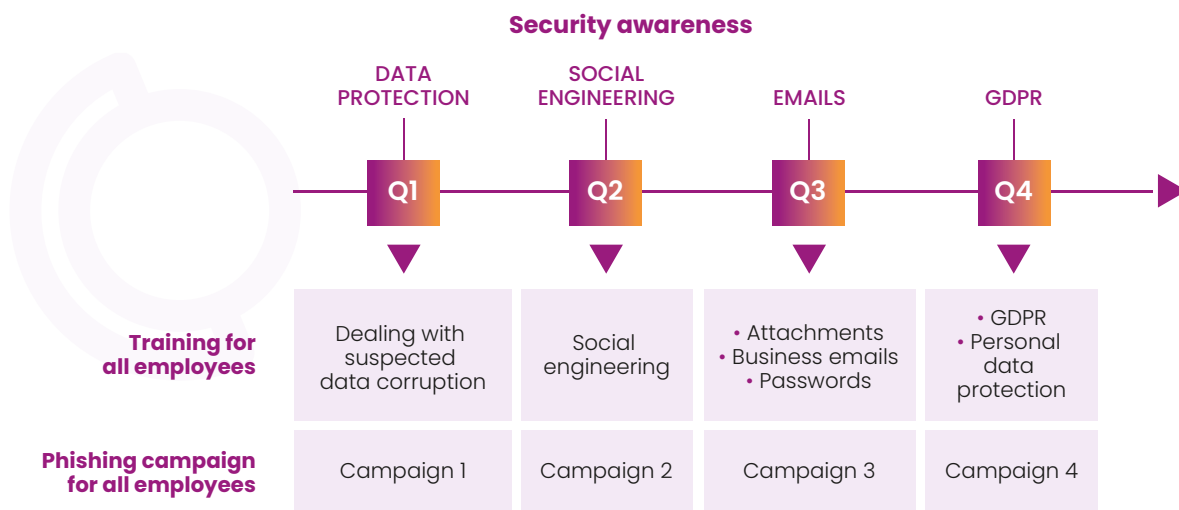
*For confidentiality reasons, the figures are not representative

Employee training

To take the human dimension of security and confidentiality into account, the CISO and the entire IT department of the Exclusive Networks Group have set up a training programme for all employees.

Deployed on a monthly basis, the trainings are addressed individually to each employee through the Group's e-learning platform. The training participation rate is monitored by the CISO and sent to line managers.

Example of training deployed in 2022:



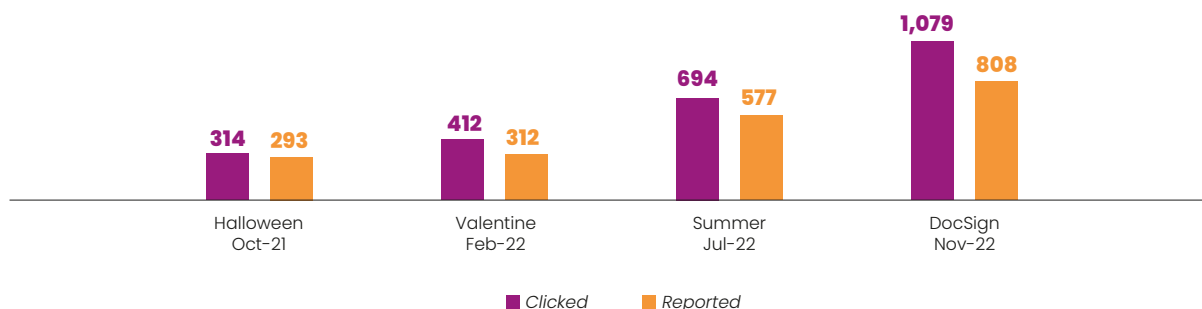
In 2022, 11 training modules were delivered to all Group employees.

[GRI 3-3-c]/SDG 4.4



To ensure that employees understand and take into account security measures, and thus measure the effectiveness of training, the CISO also carries out cyber attack simulation campaigns, for example on phishing*:

Phishing campaigns



* For confidentiality reasons, the figures are not representative

Certification projects

Trusted Introducer Service (TI) was created by the European Computer Emergency Response Team (CERT) community in 2000, to meet common needs and to establish a service infrastructure providing essential support to all computer security and incident response teams.

The TI certification is intended for teams responsible for security, response and handling of security incidents

within their organisation. It provides an independent assessment of their level of maturity and is a mark of trust recognised by stakeholders. To maintain this level of standard over time, a re-certification is required every three years.

The Trusted Introducer process has four category levels: listed, accredited, certified and associate. Already recognised at the “accreditation” level, the GSOC department has started the process to reach the “certification” level.

6.5 Data protection

The Group collects and processes personal data primarily for two purposes:

- as an employer, to comply with its legal obligations and to implement skills development policies (see Chapter 4.5);
- in the course of its activities, for the marketing of its products and services.

In this respect, the Group is subject to international regulations such as Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 General Data Protection Regulation (GDPR), as well as to local legislation applicable in the countries in which it operates, including the Data Protection Act 2018 for the UK (non-exhaustive list).

In order to respect the right to protection of personal data and privacy, the Group has set up an organisation that reports to the Group General Counsel & Group Compliance Officer, comprising:

- the Group Data Protection Officer, in charge of advising and supporting the company to ensure compliance of processing, and promoting the principles and rules of personal data protection to all employees;
- the team of Legal Counsels, in charge of ensuring that the applicable legislation on the protection of personal data is properly taken into account in contracts;
- a specialised consultancy firm, providing support on various subjects and in particular on the consideration of local regulations outside Europe.

The objectives of this organisation are to:

- establish policies and procedures relating to the protection of personal data;
- provide operational staff with analysis and decision-making tools, as well as standard contractual clauses;
- ensure the presence and compliance of clauses relating to the confidentiality of personal data in contracts, whether with vendors, customers or service providers of the Group;
- ensure that the data collected is minimised and that the principle of “Privacy by Design” is taken into account to at the design stage of a system involving the processing of personal data;
- respond to requests from any person wishing to exercise their right to access, rectify, oppose or delete data, whether an employee or a third party;
- design and deliver the employee awareness programme;
- ensure regulatory intelligence.

In 2022, the Group rolled out an e-learning personal data awareness programme for all staff with two training modules. This process will continue in 2023, with the implementation of new sessions.

6.6 Transparency and the fight against tax avoidance

Organisation of the tax function

Exclusive Networks' Tax Department is organised around a central team, integrated into the Group's Finance Department, which relies on local finance teams and external advisors to ensure that the Group pays the taxes due in the jurisdictions where it operates and that the risks are identified, assessed and under control.

The Tax Department is responsible for ensuring compliance with applicable local and international tax laws and regulations, minimising tax exposure by managing tax risk, limiting double taxation and taking advantage of any tax incentives or reliefs to which the Group may be entitled.

Compliance, transparency and fiscal responsibility

The Exclusive Networks Group has offices in 47 countries. Due to the global and cross-border nature of its distribution business and the complexity of the international tax environment, the Group faces tax uncertainties and risks inherent to its business.

This is due to the number and complexity of tax regulations, both local and international (including transfer pricing rules and principles governing the application of withholding taxes), and their interpretation in each country.

In this global and complex environment, the Exclusive Networks Group aims to comply with all applicable tax rules and regulations in the countries where it operates, ensuring that the right amount of tax is paid in the jurisdictions where it generates profits and value. Consequently, Exclusive Networks strives to comply with local and international rules, including the "OECD Transfer Pricing Guidelines for Multinational Enterprises and Tax Administrations". Exclusive Networks handles tax issues with integrity and does not engage in any artificial tax schemes.

Each of the Group's foreign locations is intended to expand the Group's business by providing a local presence where operational and commercial needs require it.

[GRI 3-3-c]

6.7 Export control

As an international company and given the nature of the goods and services it markets (see description of the risk in Chapter 2.1), the Exclusive Networks Group implements all necessary measures to comply with applicable laws and regulations concerning:

- export control of Dual-use items and technologies;
- trade restriction measures against certain countries subject to sanctions or embargoes, decided by the United Nations Security Council, the United States via the Office of Foreign Assets Control (OFAC), or the European Union within the framework of foreign and security policy decisions (CFSP).

Given the nature of the products and solutions marketed, which are considered Dual-use because they incorporate encryption technology, the cybersecurity sector is sensitive and subject to these regulations and controls.

The Exclusive Networks Group operates worldwide in compliance with these laws, which often have an extraterritorial scope, are cumulative and evolve regularly. Their objectives are to preserve global geopolitical balance, international, national or regional security, and to fight against the diversion

and proliferation of certain equipments. Export control compliance is therefore an important issue for the Group.

The Group applies these controls in all the countries in which it operates, and more specifically:

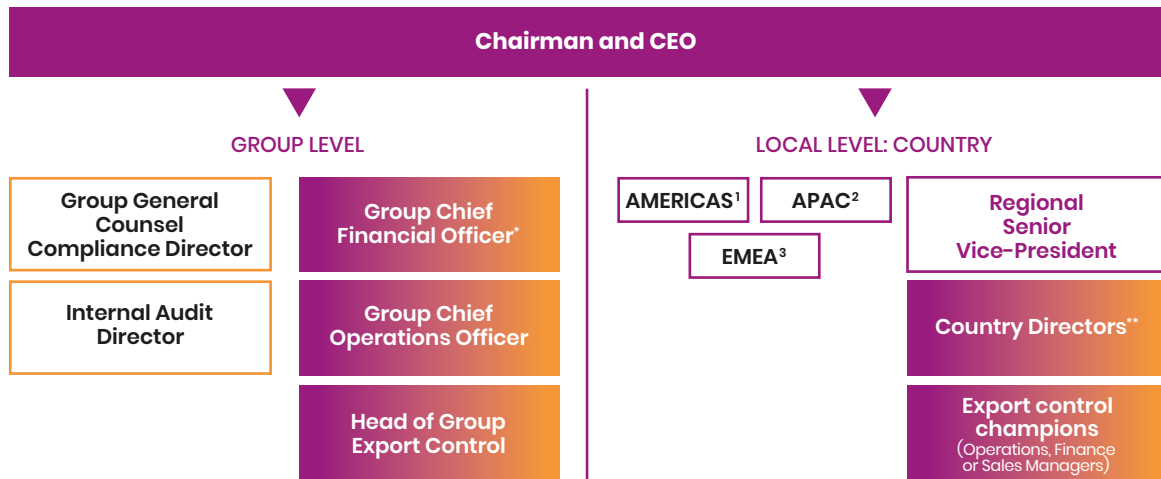
- in the European Union, in compliance with EU Regulation No. 821/2021 of 20 May 2021 establishing the Union regime for the control of exports, brokering, technical assistance, transit and transfers of Dual-use items;
- in the United States, in accordance with the EAR – Export Control Regulations 15 CFR section 730 *et seq*;
- in Singapore or the United Kingdom, in accordance with applicable local regulations.

As the export or re-export of certain equipments is subject to obtaining an export licence or an exemption granted by the authorities of the exporting countries, the Group is informed at all times by the vendors of restrictions on the goods and services supplied. Vendors have a dedicated organisation that enables them to exercise strict control over their manufacturing and sales processes in order to comply with these obligations.

Organisation of export control in the Exclusive Networks Group

In order to face these challenges together with a of strong international expansion, the Group has set up an organisation and an internal compliance programme

called the Internal Compliance Programme (ICP), which it constantly adapts to control these risks. In this context, the position of Export Control Manager was created in 2022, reporting to the Group’s Director of Operations, to strengthen the existing organisation.



- Function in charge of export control reporting to the CEO.
- Other stakeholders in the Group export control organisation.
- * Function with legal responsibility for export control by delegation from the CEO.
- ** Function with legal responsibility for export control of local entity.

Local operational entities:
 (1) **AMERICAS:** Canada, USA.
 (2) **APAC:** Australia, Hong Kong, India, Indonesia, Malaysia, New Zealand & Pacific Islands, Philippines, Singapore, Thailand, Vietnam.
 (3) **EMEA:** Austria, Belgium, Bosnia, Bulgaria, Croatia, Czech Republic, Denmark, Finland, France, Germany, Hungary, Ireland, Israel, Italy, Kenya, Mauritius, Norway, Netherlands, Northern Africa, Poland, Portugal, Romania, Saudi Arabia, Serbia, Slovakia, Slovenia, Southern Africa, Spain, Sweden, Switzerland, Turkey, United Arab Emirates, United Kingdom.

The first line of risk control consists of the Country Managers and Export Control Champions of the Group’s main subsidiaries. The second line of risk control is provided by the Group Export Control Manager, who defines the export control strategy and associated procedures, and ensures regulatory monitoring, which is particularly critical given the geopolitical situation and the speed with which sanction regimes change.

Internal Compliance Programme:

- is the bible of procedures to be followed by the Group and its subsidiaries to comply with regulations, such as the procedure for establishing the declaration of final destination and end use;
- includes training components;

- refers to other internal Group procedures, such as the third party screening system (see section 6.2).

In addition, the Group regularly conducts audits, either by the Internal Audit Department or by independent firms.

The main improvements that will be undertaken in 2023 are to overhaul the Internal Compliance Programme, to strengthen coordination between the Export Control Champions, and to make the training modules available on the Group’s e-learning platform, in order to accelerate their deployment to all employees.

[GRI 3-3-c]

7 Other regulatory issues

7.1 Respect for human rights

The Exclusive Networks Group fosters a culture of respect for people, both for its employees and in its business relationships, and is committed to respecting human rights in all countries in which it operates.

This commitment includes:

- respect for fundamental human rights, as described in the Universal Declaration of Human Rights adopted by the United Nations General Assembly on 10 December 1948, and in the International Labour Organisation Declaration on Fundamental Principles and Rights at Work adopted in 1998 and amended in 2022;
- decent working conditions: the Group puts in place an organisation and the necessary means to:
 - preserve the health and safety of its employees,
 - comply with the social legislation and regulations applicable in all countries where its employees are located, particularly with regard to working hours, rest and holidays,
 - ensure that its employees are fairly compensated in accordance with their qualifications and skills (see section 4.7 above);
- equal opportunity: the Group has put in place a Policy and procedures to:
 - prohibit and address any situation of discrimination of individuals, both at the time of hiring and throughout their working contract (see section 4.7),
 - promote diversity and inclusion as an asset to the company,
 - develop the skills of its employees, to enable them to continue to learn and develop their skills and abilities, which are the levers of the Group's success in the cybersecurity sector;
- respect dignity in the relationship with and among our employees, as described in section 1.2 "Our values" of this Extra-Financial Performance Statement.

In view of:

- the Group's rapid growth in recent years;
- its international development and its current presence on five continents;
- the expectations of its stakeholders on this major issue,

the Group plans to finalise a formal commitment on these issues in 2023, involving both the governance and all employees.

Exclusive Networks UK's support for the charitable sector

For several years now, Exclusive Networks UK and its personnel have supported a different charity each year: in 2022, the Mind charity that was chosen.

Mind is a charity based in England and Wales that helps people with mental illnesses to cope better and raises awareness about them. One in four people suffer from mental health problems, and most of them do not get the help they need. Mind has set itself the task of changing minds and offering help in everyday life, whether information, advice or local services.

The organisation is organised around a network of 130 local Minds, which offer support and specialist care close to the people who need it: 443,000 people benefited from Mind's advice and help in 2021.

SDG 3.4



7.2 Collective agreements

Collective agreements concluded in the company and their impact on the company's economic performance and on employee working conditions

In response to Article L. 225-102-1 of the French Commercial Code, the Exclusive Networks Group is careful to establish a constant and quality dialogue with its employees, in compliance with the legislation in force in each country where it is established, as well as in countries where it is not legally required to do so.

Labour relations in each country are placed under the authority of the Country Manager and the Human Resources Manager, who are responsible for:

- organising all legal bodies in accordance with local legislation;

- conducting regular meetings and dialogue with employee representatives and labour-related partners, where they exist.

As a result of the external growth carried out by the Group in recent years, the staff is spread over a large number of companies (see section 8.1). As a result, 13% of the workforce is covered by a collective agreement and few companies have formal collective agreements in place, although this does not reflect the absence of labour-related dialogue.

[GRI 2-30]

Categories	Company	Nature of the agreement
Agreements with an impact on compensation	Exclusive Networks SAS	Amendment to the profit-sharing agreement
Agreements with an impact on working conditions	Exclusive Networks SAS	Agreement on flat-rate pay agreements for the year
	Everest SubBidCo	Agreement on flat-rate pay agreements for the year

In addition to the local collective agreements, the Group's Human Resources Department introduced a Global Hybrid Work Policy in 2021, intended as a guide for both management and employees. It defines the philosophy of the Exclusive Networks Group with regard to flexible working and is implemented and adapted at

local level, taking into account applicable regulations and the specific characteristics of each company.

A large number of Group companies have implemented hybrid working arrangements based on this global policy, without necessarily being subject to a formal collective agreement.

7.3 Societal commitments to the circular economy

In response to Article L. 225-102-1 of the French Commercial Code, the Exclusive Networks Group's approach to the circular economy consists of two approaches:

- the lifespan, reuse and recycling of computer equipment for its own use;
- taking into account the end of life of its customers' hardware.

Management of the Group's own computer equipment and IT infrastructure

The Group has launched a reflection covering the entire life cycle of its computer equipment and IT infrastructures in order to reduce their environmental footprint. The main focuses identified are:

- the lifespan of equipment, particularly laptops and mobile phones: desktop monitors have a longer lifespan due to their use and less technical

obsolescence. Some countries have already determined the lifespan of some devices: the aim will be to establish a global approach for the whole Group, and to integrate the repair service offer into the choice of local service providers;

- the end-of-life management of this equipment, with a view to implementing reuse solutions through reconditioning or donations, thus contributing to reducing the consumption of resources and waste.

The deployment of this action plan will be integrated into the plan to reduce the environmental footprint of the Exclusive Networks Group (see Chapter 5).

[GRI 306-2]/SDG 12.4 & 12.5



Global Services Operation (GSO) for the end-of-life management of customers' equipment

For several years now, the Group has been offering its customers an end-of-life management service for their replaced equipment, thus helping them to reduce their own environmental footprint.

- a remote configuration implemented locally:
 - the use of remote connectivity, combined with a global network of technical engineers, consultants and project managers, reduces the environmental impact of the service by minimising travel;
- hardware maintenance:
 - Exclusive Networks proposes to its clients to extend the life of their equipment thanks to a global maintenance service based on local teams, thus limiting the consumption of new resources and reducing waste. The process benefits both the front and back end of the value chain;
- end-of-life management of equipment: the Group proposes to its customers to take charge of the end-of-life of replaced equipment in order to simplify this process:
 - audit of equipment to determine what can be reused and resold, or recycled,

- decommissioning of equipment in the environments in which it is installed and preparation for logistics,
- removal and transportation of decommissioned equipment to its final destination (resale warehouse or customer-designated warehouse, destruction and recycling plant),
- where the equipment taken back is in working order and can be reused, those with residual value are resold on the second-hand market for the customers:
- both the data erasure for reuse and the shredding and destruction are Blancco certified, a NATO-approved scheme certified by many government agencies,
- the recycling or destruction of Waste Electrical and Electronic Equipment (WEEE) is certified in accordance with local regulations,
- bio-leach recovery allows the valuable rare earth materials contained in printed circuit boards to be extracted in an environmentally friendly manner, without generating hazardous waste as more common material extraction methods do.

[GRI 306-2]/SDG 12.4 & 12.5



7.4 Food, food waste and food insecurity; animal welfare

In response to Article L. 225-102-1 of the French Commercial Code, the Exclusive Networks Group does not purchase, process or market food, nor does it interact with the animal world, either directly or across its entire value chain. In this respect:

- the fight against food waste;

- the fight against food insecurity;
- respect for animal welfare;
- responsible, fair and sustainable food.

Are not major issues for the Exclusive Networks Group, and therefore not the subject of action plans.

7.5 Physical and sports activities

In response to Article L. 225-102-1 of the French Commercial Code, the materiality analysis presented in section 2.3 shows that the practice of physical and sports activities is not a major issue for the Exclusive

Networks Group. In this respect, there is currently no specific action plan on this issue, beyond the local initiatives implemented in some countries.

Methodology note

Scope of consolidation

8 Methodology note

This report is a consolidated Extra-financial Performance Statement, in compliance with the Law No. 2021-1104 – Article 138 of 22 August 2021, on the fight against climate change and the strengthening of resilience to its impact. The Exclusive Networks Group has chosen to include certain additional social, environmental and societal data, in the interests of transparency and in order to meet the expectations of its stakeholders.

It is published each year with the Group's Management Report and covers the financial year from 1 January to 31 December 2022.

[GRI 2-3-a]/SDG 12.6



8.1 Scope of consolidation

For its second Extra-financial Performance Statement, the Exclusive Networks Group has mobilised significant resources in order to make the data more reliable, to publish a greater number of indicators and information, and to set up key performance indicators.

Given the very sharp increase in activity in 2022, resulting in a significant workload for all employees, the Group decided to focus on making the data collection more reliable, rather than covering all the controlled companies with a high level of uncertainty on the data. As a result, a scope of 23 countries was decided, covering all the companies controlled by the Group in each of these countries.

The Group will conduct an improvement process at the end of the financial year in order to identify areas for improvement, with a view to simplifying and increasing the reliability of data collection in the countries, and to extend the number of countries and companies taken into account for the Extra-financial Performance Statement as from the next financial year.

These 23 countries cover 52 companies, representing 87% of the Group's consolidated revenue and 75% of the total workforce, spread over 45 locations. The scope of consolidation is consistent for all information published in the report, except for some data on the full scope of consolidation for reasons of consistency with the figures published in the Management Report, in which case this difference is reported.

List of countries, companies and addresses of consolidated sites:

Country	Company	Address	Type
AUSTRALIA	Exclusive Networks PTY Ltd	Level 5, 20 Rodborough Road, Frenchs Forest NSW 2086, Sydney	REGISTERED OFFICE
		3/10 Southport Street, West Leederville, Perth WA 6007	OFFICES
		443 Auburn Road, Hawthorn, Victoria. Melbourne 3122	
		Pacific View Business Park, Warehouse 5, 10 Rodborough Road, Frenchs Forest NSW 2086	WAREHOUSE
AUSTRIA	Exclusive Networks Austria GmbH	Heinrich Bablik-Straße 17 K21 Top N06 2345 Brunn am Gebirge. Austria	REGISTERED OFFICE
		LIEBERMANNSTR. F06 402/1. 2345, BRUNN AM GEBIRGE	WAREHOUSE*
BELGIUM	Exclusive Networks BeLux B.V.	A. Stocletlaan 202 Duffel (Antwerp) 2570, Belgium	REGISTERED OFFICE WAREHOUSE
CANADA	Exclusive Networks Canada Inc.	A101, 9000 Bill Fox Way. Burnaby, BC, V5J 5J3. Vancouver	REGISTERED OFFICE WAREHOUSE
CZECH REPUBLIC	Exclusive Networks Czechia s.r.o.	Šafaříkova 201/17, 120 00 Praha. 12000	REGISTERED OFFICE WAREHOUSE
CROATIA	Exclusive Networks Croatia d.o.o.	Nikole Cara 6, 51000 Rijeka. Croatia	REGISTERED OFFICE
		Remetinečka cesta 5a, 10000 Zagreb Zagreb	OFFICES
		Nikole Cara 6, 51000 Rijek, Croatia	WAREHOUSE

* The sites in italics correspond to subcontracted premises.

Country	Company	Address	Type
DENMARK	Exclusive Networks Denmark A/S	Strandvejen 58, 2900 Hellerup, Denmark	REGISTERED OFFICE
		<i>Danmarksgade 6B, 4690 Haslev</i>	WAREHOUSE
FINLAND	Exclusive Networks Finland OY	Säterinkatu 6, 02600 Espoo, Finland	REGISTERED OFFICE
		<i>Vanha porvoontie 229, Ovi A9, 01380 Vantaa</i>	WAREHOUSE
FRANCE	Ignition Technology Finland Oy	Tekniikantie 2 B 2150, Espoo Finland	REGISTERED OFFICE
	Exclusive Networks SA		
	Exclusive Networks SAS		
	Exclusive Capital SAS		
	Exclusive France Holding SAS	20 quai du Point du Jour – 92100 Boulogne-Billancourt France	REGISTERED OFFICE
	Everest SubBidCo SAS		
	Exclusive on Demand SAS		
	Ignition France SAS	3 rue Nationale. 92100 Boulogne-Billancourt France	REGISTERED OFFICE
GERMANY	Exclusive Networks Deutschland Beteiligungs GmbH	40 avenue Théroigne de Méricourt, 34000 Montpellier, France	
		2 avenue des Améthystes – 44300 Nantes, France	OFFICES
	Exclusive Networks SAS	La Maison du Coworking, 205 chemin des Peupliers, 59700 Marcq-en-Barœul, France	
		Parc du Jubin – Bât. D – 27 chemin des Peupliers, 69570 Dardilly, Lyon, France	WAREHOUSE
GERMANY	Exclusive Networks Deutschland Beteiligungs GmbH	Hardenbergstraße 9a, 10623. Berlin, Germany	REGISTERED OFFICE
		Balanstraße 73/Haus 21 B, 81541 München, Germany	OFFICES
	Exclusive Networks Deutschland Beteiligungs GmbH	Martin-Luther-King-Weg 8, 48155 Münster, Germany	
		Königsberger Str. 260, 48157 Münster, Germany	WAREHOUSE
IRELAND	Exclusive Networks Ireland Limited	Unit 8, 2009 Orchard Business Centre, Orchard Avenue, Citywest Business Campus, Dublin 24, D24 YC8C, Ireland	REGISTERED OFFICE
		Via Umbria 27/A CAP. 10199 San Mauro Torinese Italy	WAREHOUSE
ITALY	Exclusive Networks SRL	Via Torri Bianche 6, Palazzo Tiglio, 1 piano Vimercate, Milano 20871 (MB)	
		Via di Grotte Portella 6/8, Frascati (RM) c/o Centro Direzionale La Piramide, Rome 00044	OFFICES
NETHERLANDS	Exclusive Networks BV	Ekkersrijt 4601. 5692 DR SON EN BREUGEL	REGISTERED OFFICE
		Gelderlandhaven 7a 3433 PG Nieuwegein	WAREHOUSE
			OFFICES

* The sites in italics correspond to subcontracted premises.

Methodology note

Scope of consolidation

Country	Company	Address	Type
NORWAY	Exclusive Networks Norway AS	Martin Linges vei 25 Fornebu, 1364, Oslo, Norway	REGISTERED OFFICE
		<i>Blakervegen 109, 1920 Sørumsand</i>	WAREHOUSE
POLAND	Exclusive Networks Poland SA	ul. Zawia 61 Kraków, 30-390 Kraków, Poland	REGISTERED OFFICE
		ul. Borsucza 32, 02-213 Warszawa	WAREHOUSE
		ul. Tęczowa 13, 53-601 Wrocław	OFFICES
		ul. Przemysłowa 5 pok. 45, 46, 47, 35-105 Rzeszów	SHARED OFFICE
	ul. Piłsudskiego 12 I piętro, 38-400 Krosno		
	ul. Roździeńskiego 188a, 40-203 Katowice		
	ul. Wolska 11a pok.4 i 5 II p., 20-411 Lublin		
		ul. Grunwaldzka 229/34 – 3rd floor, 85-793 Bydgoszcz	
	ul. Lutniana 39 pok.105 I piętro, 71-425 Szczecin		
	Compendium Centrum Edukacyjne Spółka z o.o.	ul. Tatarska 5 Kraków, 30-103 Poland	REGISTERED OFFICE
ROMANIA	Exclusive Networks Technology Romania SRL	Grigore Romniceanu 20, S5, 050576 Bucharest	REGISTERED OFFICE
			WAREHOUSE
SINGAPORE	Exclusive Networks Asia Pte Ltd	3 Kallang Junction #04 – 02. Vanguard Campus Singapore 339265	REGISTERED OFFICE
		5 Pereira Road #02-03 Asiadwide Industrial Building 368025	OFFICES
		WAREHOUSE	
	BridgingMinds Singapore Pte Ltd	190 Middle Road, #12-10/11 Fortune Centre, Singapore 188979	
	Exclusive Networks Singapore Pte Ltd		REGISTERED OFFICE
	Itec Intelligent Services PTE Ltd	3 Kallang Junction #04 – 02, Singapore 339265	
	Exclusive On Demand APAC Pte Ltd		
SPAIN	Exclusive Networks SL	Calle Arturo Soria 336, 8 piso. 28033 Madrid, Spain	REGISTERED OFFICE
		Avda. Diagonal, 177 5ª Planta 08018, Barcelona	OFFICES
		<i>A/A Antonio Cerrillo Ircologic Avda. Fuentemar, n 43, Naves 3C y 4 28823 Coslada</i>	WAREHOUSE
SWEDEN	Exclusive Networks Sweden AB	Slättervägen 20. 170 67 Solna, Sweden	REGISTERED OFFICE
		<i>Hyttögatan 6, 752 28 Uppsala</i>	WAREHOUSE
SWITZERLAND	Exclusive Networks Switzerland AG	Thurgauerstrasse 40, 8050. Zürich, Switzerland	REGISTERED OFFICE
UAE	Exclusive Group Mena Ltd	Free Zone Offshore company. JAFZA, Dubai, UAE	REGISTERED OFFICE
		<i>DHL International, G 13 LIU WEST RING ROAD, DUBAI AIRPORT FREE ZONE DUBAI, UNITED ARAB EMIRATES</i>	WAREHOUSE
	Networks Distributors FZ-LLC	3502 & 3507 35th Floor, Shatha Tower. Dubai Media City	REGISTERED OFFICE

* The sites in italics correspond to subcontracted premises.

Country	Company	Address	Type
UK	Exclusive Networks Ltd		
	Ignition Bidco Ltd		
	Everest UK Finco Ltd	Alresford House Mill Lane Alton. GU34 2QJ Hampshire, United Kingdom	
	Everest UK Hedgeco Limited		
	Itec Intelligent Services Ltd	Rosa 18 Mulberry Business Park Fishponds Road, RG41 2GY Wokingham United Kingdom	REGISTERED OFFICE
	Ignition Technology Ltd		
	Ignition Technology Group Ltd	Cody Technology Park, Old Ively Road, GU14 0LX, Farnborough. United Kingdom	
	Nuaware Ltd	C/O Rodliffe Accounting Ltd 1 Canada Sq 37th Floor, Canary Wharf, London, United Kingdom, E14 5AA	
	Exclusive Networks Ltd	6-7 Kings Court, Willie Snaith Road, Newmarket, Suffolk, CB8 7SG	
		Laurel House, Ransom Wood Business Park, Southwell Road West, Mansfield, NG21 0HJ	OFFICES
6th Floor, 20 St Dunstons Hill, London EC3R 8HL			
USA	Exclusive Networks USA Inc.	Unit 3, Riverwey Industrial Park, Newman Lane, Alton, Hampshire GU34 2QL	WAREHOUSE
		2075 Zanker Road, 95131, San Jose, California, USA	REGISTERED OFFICE
	Itec Intelligent Services Inc	3030 N. Rocky Point Dr. W Suite 150 33607, Tampa Florida – USA	WAREHOUSE
	Exclusive On Demand USA		REGISTERED OFFICE
	Exclusive Americas Holdings Inc.	251 Little Falls Drive, 19808, Wilmington, Delaware – USA	
	Exclusive Networks USA Inc.	4049 Willow Lake Boulevard, 38118 Memphis TN – USA	WAREHOUSE

* The sites in italics correspond to subcontracted premises.

[GRI 2-1-d/2-2-a/2-2-c]

8.2 Methodological information on indicators

Preparation of this Sustainability Report

The Group Executive Committee validates the list of consolidated companies on the proposal of the Group Sustainability Director, who is also responsible for:

- preparing the reporting framework;
- defining the nature and source of the information to be collected and ensuring its reliability;
- organising the collection of information, whether centralised or locally, in order to consolidate it;
- writing this report.

The process follows a defined timetable, shared with the main contributors, to enable the information to be verified by the notified body within the time frame required. In the future, all data will be archived, to enable consistency checks to be carried out and the results obtained to be put into perspective.

Where possible, the indicators and information in this report are prepared in accordance with the Global Reporting Index (GRI) Guidelines, according to the most recent versions of the standards available as at 30 June 2022. When the GRI framework is used it will be identified by the term "GRI-xx". The other indicators and information are either specific to the company, as they relate to subjects that are unique to it, or aim to comply with Articles L. 225-102-1 and L. 22-10-36 of the French Commercial Code.

Information relating to social data

Regarding the social data published in this report:

- average annual workforce and other figures presented in chapter 4: all persons paid during the year 2022 in one of the 23 consolidated countries are taken into account, regardless of their employment agreement (fixed-term or open-ended, apprentices and trainees). Temporary workers and service providers are not taken into account;
 - the data are collected from extractions of the Human Resources Information System described in section 4.2, and then consolidated using a data analysis software. The average workforce is calculated based on each monthly average using cross-reference tables;
- [GRI 2-7-c]*
- health and safety: accidents resulting in at least one day's absence from work are taken into account for the calculation of frequency and severity rates;
 - training: all training categories are taken into account. Scope may be technical or regulatory, relate to adaptation in the position or aim to develop employees' skills.

Information on environmental data

Regarding the environmental data published in this report:

- all data published in chapter 5 is in accordance with the GHG Protocol Corporate Standard 2015;
- to ensure that all the expected information is communicated within the given time frame, certain missing data concerning Scopes 1 and 2 and representing less than 10% of the subtotal have been extrapolated;
- scope 3 emissions are estimated on the basis of generic assumptions, which may be subject to change as part of the methodological improvements planned for 2023;
- the Exclusive Networks Group includes the environmental footprint of all the vehicles used in its activities, which are mainly leased, in the accounting of its greenhouse gas emissions;
- the mass of equipment purchased from vendors, i.e. nearly 1,500 tonnes of electronic equipment, is considered equivalent to that of products sold to customers.

Calculation of the Greenhouse Gas Emissions Assessment:

- the following greenhouse gases were taken into account, converted into tonnes of CO₂ equivalent (or tCO₂e) according to their Global Warming Potential: CO₂, CH₄, N₂O, HFC, SF₆, PFC, NF₃ and CFC;
- the Group's carbon footprint was calculated using the ADEME-Association Bilan Carbone (ABC) calculation tool in its version 8.8 of October 2022, following the rules of the GHG Protocol and with a level of uncertainty for each item. This tool allows results to be displayed in several standard formats, including the GHG Protocol format;
- the emission factors are taken from the ADEME database, unless otherwise stated;
- the change in the Group's Greenhouse Gas Emissions Assessment compared with 2021 is not solely due to changes in its activities, consumption and emissions. The collection of the source data required to establish the 2021 Greenhouse Gas Emissions Assessment proved to be too limited, resulting in excessively high levels of uncertainty. This is why the Group launched a specific project in 2022, lasting several months, aimed at building a robust Greenhouse Gas Emissions Assessment, which will form the basis for establishing a trajectory for reducing its emissions (see sections 5.2 and 8.1).

Nature of the data collected:

- energy used in buildings, i.e. electricity, gas and fuel oil: based on invoices;
- vehicle fleets: fuel consumed (petrol or diesel), based on invoices or estimates;
- equipment purchases and sales: mass of equipment multiplied by a representative electronic equipment emission factor;
- inbound and outbound transport: mass data extraction, distances travelled and transport modes from logistics providers, and application of an emission factor per transport mode (air or road);
- business travel: data extracted from travel providers, extrapolated to the organisational scope;
- commuting: estimate based on an average distance travelled per day and per employee, broken down by mode of transport (car, train, bus, motorbike, bicycle), obtained as part of an internal survey conducted in 2021;
- waste produced on the sites: estimate of the mass of tertiary waste per employee and per year based on the ADEME guide to workplace eco-responsibility ("Écoresponsable au bureau"), September 2022;
- use of products sold: estimate of the average electricity consumption of a typical equipment over a five-year period, multiplied by the electricity emission factor of the country of sale;
- end of life of products sold: mass of equipment sold multiplied by the emission factor for electronic waste from the ADEME database.







*[GRI 2-4-a/305-1-b/305-1-e/305-1-f/305-1-g/
305-2-c/305-2-e/305-2-g/305-3-b/305-3-f/
305-3-g/305-4-c/305-4-d/305-3-f/305-3-g]*

Methodology note

Extra-financial performance statement/GRI/SDG cross-reference table

8.3 Extra-financial performance statement/GRI/SDG cross-reference table




Information theme	Indicator baseline	Information description	Chapter	Page	SDG
Business model					
	Article R. 225-105 of the French Commercial Code	Business model of all companies for which the Exclusive Networks Group prepares consolidated financial statements	1	p. 02	
Risks and opportunities					
	Article R. 225-105 of the French Commercial Code	Key risks and opportunities related to the Group's activity, including its business relationships, products and services	2	p. 05	
Materiality					
Materiality matrix	GRI 3-1	Process for determining materiality issues	2.3	p. 26	
	GRI 3-2-a	List of materiality issues			
Key performance indicators					
	Article R. 225-105 of the French Commercial Code	Key performance indicators aimed at preventing and mitigating the occurrence of the Group's main sustainability risks	3	p. 29	
Employment					
Social data	Average total workforce and breakdown of employees by age, gender, professional category, type of contract, region, country	GRI 2-7-a	Average total workforce and breakdown by gender/region/country	4.9	p. 40
		GRI 2-7-b	Proportion of employees employed on fixed-term or permanent contracts		
			Proportion of employees employed on full-time or part-time contracts		
		GRI 2-7-c	Information on data collection and consolidation, methodologies and assumptions		
		GRI 2-7-e	Significant changes in the number of employees during the period and compared with previous periods		
	Hirings, departures, turnover and retention of talent	GRI 401-1-a	Breakdown of hires by age, gender and region		
		GRI 401-1-b	Employee turnover by age, gender and region		
		Company	Breakdown of departures by age, gender and region		
		Article R. 225-105 of the French Commercial Code	Breakdown of departures by reason and gender		
	Payroll and changes	Company	Average tenure	4.8	p. 39
		Article R. 225-105 of the French Commercial Code	Absenteeism rate		
		Article R. 225-105 of the French Commercial Code	Wages, salaries and social security charges, change vs Y-1	4.9	p. 40





Information theme	Indicator baseline	Information description	Chapter	Page	SDG
Diversity and equal opportunities					
Diversity and equal opportunities	GRI 405-1-a	Breakdown of governance members by gender and age	4.7	p. 36	  SDG: 5.5 & 8.5
	GRI 405-1-b	Breakdown of employees by gender, employee category and age			
	Company	Average age and age pyramid (male-female)			
Measures taken to promote gender equality	GRI 2-21	Equity ratio	4.5	p. 35	 SDG 4.3 & 4.4
	GRI 405-2-a	Average gender pay gap by employee category and main locations of operation			
	GRI 405-2-b	Description of methodology and main locations			
Training					
Training programmes, number of hours of training and training contribution rate	GRI 404-2-a	Description of training programmes to improve employee skills	4.4 & 4.5	p. 34	 SDG 4.3 & 4.4
	GRI 404-3-a	Proportion of employees who receive an appraisal and career development interview	4.4	p. 34	
	Company	Training expenditure Rate of contribution to training (training budget/total payroll)	4.5	p. 35	
Labour relations					
Collective agreements with trade unions or employees representatives	Article R. 225-105 of the French Commercial Code	List of agreements signed	7.2	p. 70	
Annual staff survey	Company	Proportion of employees who responded to the company annual survey Engagement rate	4.3	p. 33	
Health and safety					
Occupational accidents, frequency and severity	GRI 403-9-a	Number and frequency rate of occupational accidents Number and severity of occupational accidents	4.8	p. 39	  SDG 8.8 & 3.4
	GRI 403-9-g	Information on data collection, standards, methodologies and assumptions			
Occupational health and safety	GRI 403-7	UK stress awareness month			

Social data

Methodology note




Extra-financial performance statement/GRI/SDG cross-reference table

Information theme	Indicator baseline	Information description	Chapter	Page	SDG
Sustainable use of resources					
Internal energy consumption	GRI 302-1-a	Fuel consumption from non-renewable sources	5.1	p. 43	
	GRI 302-1-a	Diesel fuel consumption			
	GRI 302-1-a	Petrol fuel consumption			
	GRI 302-1-c	Electricity consumption			
	GRI 302-1-b	Renewable electricity consumption			
	GRI 302-1-c	City gas consumption			
	GRI 302-1-c	Consumption from heating networks			
	GRI 302-1-e	Total energy consumption			
	GRI 302-1-f	Standards, methodologies, assumptions and calculation tools used			
	GRI 302-1-g	Source of conversion factors used			
External energy consumption (Scope 3)	GRI 302-2-a	Energy used outside the organisation			
	GRI 302-2-b	Standards, methodologies, assumptions and calculation tools used			
	GRI 302-2-c	Source of conversion factors used			
Energy intensity	GRI 302-3-a	Energy intensity ratio by geographical area			 SDG 7.3
	GRI 302-3-b	Denominator chosen to calculate the ratio			
	GRI 302-3-c	Types of energy included in the ratio			
	GRI 302-3-d	Internal energy ratio			
Greenhouse gas emissions	GRI 305-1-a	GHG Scope 1	5.2	p. 44	  SDG 7.3 12.4 & 12.5
	GRI 305-1-b	Description of gases taken into account			
	GRI 305-1-e	Source of emission factors			
	GRI 305-1-f	Consolidation approach			
	GRI 305-1-g	Standards, methodologies, assumptions and calculation tools used			
	GRI 305-2-a	GHG Scope 2			
	GRI 305-2-c	Description of gases taken into account			
	GRI 305-2-e	Source of emission factors			
	GRI 305-2-f	Consolidation approach			
	GRI 305-2-g	Standards, methodologies, assumptions and calculation tools used			
	GRI 305-3-a	GHG Scope 3			
	GRI 305-3-b	Description of gases taken into account			
	GRI 305-3-d	Categories of emissions taken into account			
	GRI 305-3-f	Source of emission factors			
	GRI 305-3-g	Standards, methodologies, assumptions and calculation tools used			
	Company	Breakdown of CO2 emissions by category/country/region			
	GRI 305-4-a	GHG emissions intensity ratio			
GRI 305-4-b	Denominator chosen to calculate the ratio				

Information theme	Indicator baseline	Information description	Chapter	Page	SDG	
Environmental data	Greenhouse gas emissions	GRI 305-4-c	Categories of emissions taken into account (Scope 1/2/3)	5.2	p. 44	  SDG 7.3 12.4 & 12.5
		GRI 305-4-d	Description of gases taken into account			
		GRI 305-3-f	Source of emission factors			
		GRI 305-3-g	Standards, methodologies, assumptions and calculation tools used			
	Water consumption	GRI 303-5-a	Quantity of water consumed	5.3	p. 50	
		GRI 303-5-d	Information on data collection and consolidation, methodologies and assumptions			
	Waste management					
	Waste	GRI 306-1	Description of waste generated by the company's activity and/or in its value chain	5.3	p. 50	 SDG 12.4 & 12.5
		GRI 306-3-a	Tonnage and breakdown by waste category			
		GRI 306-3-b	Information on data collection			
Other information						
Green Taxonomy	Regulation (EU) 2020/852 of 18 June 2020	Revenue, CapEx and OpEX indicators	5.4	p. 51		
	Article R. 225-105 of the French Commercial Code	Amount of provisions and guarantees for environmental risks				
Societal data	Anti-corruption					
	Anti-corruption policy	GRI 3-3	Anti-corruption policy, organisation and risk management	6.1	p. 58	
	Corruption risk assessment	GRI 205-1-a	Total number and percentage of transactions assessed for corruption-related risks			
			Proportion of due diligences performed on third parties			
	Corruption risk prevention: communication, training, audits	GRI 205-1-b	Significant corruption-related risks identified in risk assessment	6.2	p. 59	 SDG 16.5
		GRI 205-2-c	Number and percentage of business partners to whom the anti-bribery policy has been communicated by type of business partner and by region			
		GRI 205-2-e	Number and percentage of employees trained to anti-corruption			
		Company	Number of internal anti-corruption audits			
Proven incidents of bribery and actions taken	GRI 205-3	Number of proven cases of corruption				
		Number of employees dismissed or sanctioned for corruption				
		Number of corruption-related convictions against the Group or one of its subsidiaries				

Methodology note

Extra-financial performance statement/GRI/SDG cross-reference table

Information theme	Indicator baseline	Information description	Chapter	Page	SDG
Ethics and fair practice					
Ethics	GRI 2-26	Number of ethics alerts received	6.2	p. 59	
Data security	Company	Cyber Exposure Score	6.3	p. 63	 SDG 4.4
	Company	Training of employees in cybersecurity	6.4	p. 64	
	Company	Training of employees in personal data protection	6.5	p. 66	
Other regulatory issues					
Societal data	Articles L. 225-102-1 and L. 22-10-36 of the French Commercial Code	Consequences on climate change of the Company's activity and the use of the goods and services it produces	5	p. 43	
		Societal commitments to sustainable development and the circular economy	7.3	p. 70	 SDG 12.4 & 12.5
		Societal commitments in favour of the fight against food waste and food insecurity, responsible, fair and sustainable food, and animal welfare	7.4	p. 71	
		Actions to promote physical activity and sport	7.5	p. 71	
		Effects of the Company's activity on the respect of human rights	7.1	p. 69	
		Combating tax avoidance	6.6	p. 67	
Methodological note					
	GRI 2-1-d	Number and addresses of sites			
	GRI 2-2-a/2-2-c	List of countries and companies considered and approach used	8.1	p. 72	 SDG 12.6
		Coverage rate on Group workforce			
		Coverage rate on Group revenue			
	GRI 2-3-a	Reporting period and frequency of sustainability reporting	8	p. 72	
	GRI 2-4-a	Restatement of previously published information	8.2	p. 76	
GRI 2-5	External assurance: independent notified body report	9	p. 83		

9 Opinion of the independent notified body

In accordance with Decree 2017-1265 of 9 August 2017, issued for the application of Ordinance 2017-1180 on the publication of extra-financial information, the verification of the Exclusive Networks Group's sustainable

development information has been entrusted to the CSR notified body Finexfi, to ensure the transparency and fairness of the information provided in this report.

[GRI 2-5]

Opinion of the audit organisation

for the year ended 31 December 2022

This is a free translation into English of the CRS Auditor's report issued in French and is provided solely for the convenience of English-speaking readers. This report should be read in conjunction with, and construed in accordance with, French law and professional standards applicable in France.

To the Shareholders,

In our capacity as independent third party, CSR auditor of Exclusive Networks (hereinafter the "Entity"), and accredited by COFRAC Inspection under number 3-2013 (a), we have performed work to provide a reasoned opinion that expresses a limited level of assurance on the historical information (observed and extrapolated, hereinafter the "Information") of the consolidated extra-financial statement (hereinafter the "Statement"), prepared in accordance with the Entity's procedures (hereinafter the "Guidelines"), for the financial year ended December 31st, 2022, presented in the Management Report of the Entity, in application of the provisions of Articles L. 225-102-1, R. 225-105 and R. 225-105-1 of the Commercial Code.

(a) scope of accreditation available on www.cofrac.fr

Conclusion

Based on the procedures we performed, as described in the "Nature and scope of our work" and the evidence we collected, nothing has come to our attention that causes us to believe that the Statement is not presented in accordance with the applicable regulatory requirements and that the Information, taken as a whole, is not presented fairly in accordance with the Guidelines.

Preparation of the Statement

The lack of a commonly used framework or established practice on which to base the assessment and evaluation of information allows for the use of alternative accepted methodologies that may affect comparability between entities and over time.

The Information has been prepared in accordance with the Guidelines, the main elements of which are presented in the Statement.

Restrictions due to the preparation of the Information

The Information may contain inherent uncertainty about the state of scientific or economic knowledge and the quality of external data used. Some of the information is dependent on the methodological choices, assumptions and/or estimates made in preparing the Information and presented in the Statement

The entity's responsibility

The Board of Directors is responsible for :

- selecting or setting appropriate criteria for the preparation of the Information;
- preparing the Statement with reference to legal and regulatory requirements, including a presentation of the business model, a description of the principal extra-financial risks, a presentation of the policies implemented considering those risks and the outcomes of said policies, including key performance indicators where applicable; and also, the Information required by Article 8 of Regulation (EU) 2020/852 (EU Taxonomy);
- and implementing internal control procedures deemed necessary to the preparation of information, free from material misstatements, whether due to fraud or error.

Responsibility of the independent third party

Based on our work, our responsibility is to provide a report expressing a limited assurance conclusion on:

- the compliance of the Statement with the requirements of article R. 225-105 of the French Commercial Code;
- the fairness of Information provided in accordance with article R. 225 105 I, 3 and II of the French Commercial Code, i.e., the outcomes, including key performance indicators, and the measures implemented considering the principal risks.

As it is our responsibility to express an independent conclusion on the Information prepared by management, we are not authorized to be involved in the preparation of such Information, as this could compromise our independence.

Opinion of the independent notified body

Extra-financial performance statement/GRI/SDG cross-reference table

This is not our responsibility to express an opinion on:

- the Entity's compliance with other applicable legal and regulatory requirements (in particular with regard to the information required by Article 8 of Regulation (EU) 2020/852, the French duty of care law and anti-corruption and tax evasion legislation);
- the fairness of the information n required by Article 8 of Regulation (EU) 2020/852;
- the compliance of products and services with applicable regulations

Regulatory provisions and applicable professional standards

The work described below was performed with reference to the provisions of articles A. 225-1 et seq. of the French Commercial Code, as well as with the professional guidance of the French Institute of Statutory Auditors ("CNCC") applicable to such engagements and with ISAE 3000 (revised)

Independence and quality control

Our independence is defined by the requirements of article L. 822-11-3 of the French Commercial Code and the French Code of Ethics (Code de déontologie) of our profession. In addition, we have implemented a system of quality control including documented policies and procedures regarding compliance with applicable legal and regulatory requirements, the ethical requirements and the professional doctrine of the French National Association of Auditors.

Means and resources

Our work was carried out by a team of 2 people between January 15, 2023 and March 24, 2023 and took a total of two weeks.

We were assisted in our work by our specialists in sustainable development and corporate social responsibility. We conducted 15 interviews with people responsible for preparing the Statement, representing among general management, administration and finance, risk management, compliance, human resources, health and safety, environment and purchasing.

Nature and scope of our work

We planned and performed our work considering the risk of material misstatement of the Information.

We estimate that the procedures we have carried out in the exercise of our professional judgment enable us to provide a limited assurance conclusion:

- we obtained an understanding of all the consolidated entities' activities, the description of the social and environmental risks associated with their activities;
- we assessed the suitability of the Guidelines with respect to their relevance, completeness, reliability, objectivity and understandability, with due consideration of industry best practices, when appropriate;
- we verified that the Statement includes each category of social and environmental information set out in article L. 225-102-1 III, as well as information regarding compliance with human rights and anti-corruption;
- we have verified that the Statement presents the information required by II of Article R. 225-105 when relevant to the principal risks and includes, where appropriate, an explanation of the reasons for the absence of the information required by the second paragraph of III of Article L. 225-102-1 ;
- we verified that the Statement presents the business model and the principal risks associated with all the consolidated entities' activities, including where relevant and proportionate, the risks associated with their business relationships and products or services, as well as their policies, measures and the outcomes, including key performance indicators related to the principal risks;
- we referred to documentary sources and conducted interviews to:
 - assess the process used to identify and confirm the principal risks and the consistency of the outcomes and the key performance indicators used with respect to the principal risks and the policies presented, and
 - corroborate the qualitative information (measures and outcomes) that we considered to be the most important presented in the appendix. Our work was performed at the consolidation entity level. Our work was carried out at the level of the consolidating entity and in a selection of entities¹;

¹ Exclusive Networks SA, Exclusive Networks France SA, Exclusive Holding, Exclusive on demand

- we asked what internal control and risk management procedures the entity has put in place and assessed the data collection process implemented by the entity to ensure the completeness and fairness of the Information;
- for the key performance indicators and other quantitative outcomes that we considered to be the most important presented in the appendix;
- we implemented :
 - analytical procedures to verify the proper consolidation of the data collected and the consistency of any changes in those data;
 - tests of details based on sampling or other selection methods, consisting of verifying the correct application of definitions and procedures and reconciling the data with supporting documents.

This work was carried out on a selection of contributing entities and covered between 29% and 100% of the consolidated data selected for these tests;

- we assessed the overall consistency of the Statement based on our knowledge of all the consolidated entities.

The procedures performed in a limited assurance engagement are less extensive than those required for a reasonable assurance engagement performed in accordance with the professional guidance of the French Institute of Statutory Auditors ("CNCC"); a higher level of assurance would have required us to carry out more extensive procedures.

French original signed by : independent Verifier

Lyon, March 27, 2023

FINEXFI

Isabelle Lhoste

Partner

ANNEX 1

- Social indicators :
 - Business Model
 - Cod of Conducts
 - Mains risks and opportunities
 - Review chapter #WeAreExclusive
 - The average number of employees
 - Distribution of employees by region
 - Age pyramid,
 - Distribution of employees by generation
 - gender
 - Recruitment by generation and by gender
 - Dismisses
 - Environmental footprint
 - Energy consumption – scopes 1 et 2
 - GHG emissions by scope



Exclusive Networks SA
French *Société anonyme* with a share capital of €7,333,622.88
Registered office : 20, Quai du Point du Jour – 92100 Boulogne Billancourt (France)
Phone +33 1 41 34 53 04 – Fax. 01 41 31 47 86
RCS Nanterre 839 082 450

Designed & published by  **LABRADOR** +33 (0)1 53 06 30 80

