# 4

# RISK FACTORS AND MANAGEMENT



*Components of the Annual Financial Report are identified in this table of contents with the sign* AFR

*The Non-Financial Statement is indentified in this table of contents with the sign* NFS

# 4.1 RISK FACTORS

Investors are advised to carefully read the financial and non-financial risks described in this section, as well as the other information contained in this Universal Registration Document, before taking any investment decisions.

In accordance with Regulation (EU) No. 2017/1129 ("Prospectus III") and in compliance with the ESMA Guidelines, at the date this Universal Registration Document was filed, the risks presented below are the main risks considered specific to the Bureau Veritas Group and/or to its securities that Bureau Veritas believes could have a significant net impact on the Group, its businesses, its financial position, its earnings and/or its outlook should they materialize. The occurrence of one or more of these risks could result in a decrease in the value of the Company's shares, and investors could lose all or part of their investment.

The Group's various operating departments, as well as support functions both in and outside France, identify and assess risk along with the related risk management procedures on an ongoing basis. Reports are regularly submitted to the Executive Committee, the Audit & Risk Committee and the Board of Directors. They help to prepare and update the risk map described in section 4.2 – Internal control and risk management procedures, of this Universal Registration Document.

The Group has also taken out various insurance policies, as described in further detail in section 4.3 – Insurance, of this Universal Registration Document. The Group's insurance strategy is to best protect the Group's employees and assets against the occurrence of identified major insurable risks that may affect it.

In any event, other risks that Bureau Veritas does not consider to be specific to its businesses as they generally also concern other issuers in varying degrees, regardless of their activities, such as risks related to the climate, international economic sanctions or exchange rate fluctuations, could also have an adverse impact on the Group, its businesses, its financial position, its earnings and/or its outlook. Other risks may exist or may come to exist that are not known by Bureau Veritas at the date of this Universal Registration Document or that are presented in other sections of the Universal Registration Document and considered at that date unlikely to have a significant adverse impact on the Group, its businesses, its financial position, its earnings and/or its outlook should they materialize.

In 2020, as part of the work to update the Group's risk map, all Group-wide processes for preparing the map were reviewed. This task involved all Operating Groups and support functions (see section 4.2.1 – Organization and general approach to internal control and risk management, of this Universal Registration Document). A total of 40 key risks were identified, including risks specific to the Group's businesses.

As a result of the update to the Group's 2020 risk map:

- cybersecurity risk is now included in the risk factors, in the "Risks related to the Group's operations and activities" category;
- the seven risks discussed in the 2019 Universal Registration Document published in March 2020 correspond to other risks specific to the Group and are described below.

In 2022, the Group's risk map was updated, with input from the members of the Executive Committee and the network of Risk Managers in each Operating Group. This update was reviewed in January 2023 by the Board of Directors' Audit & Risk Committee. The updated risk map takes into account the impact of the action plans implemented in 2021 and 2022, as well as changes in the Group's internal and external environment. This revision did not result in any changes to the risk factors or their net impact, as described below.

The risk factors shown below are sorted into the following three categories:

- risks related to the Group's operations and activities;
- risks related to human capital;
- risks related to acquisitions.

Risks are classified within their respective category in decreasing order of importance as determined by the Company based on the probability that the risks will materialize and the estimated extent of their impact on the Group, its businesses, its financial position, its earnings and/or its outlook, and after applying any risk mitigation measures. The order of importance as determined by Bureau Veritas could change at any time, in light of new external facts or circumstances, developments in the Group's businesses, or changes in the impact of measures to manage and mitigate risks.

For certain risks, references are made to specific chapters or sections of this Universal Registration Document in which they are discussed in more detail. Internal control and risk management procedures in place within the Group are described in section 4.2 – Internal control and risk management procedures, of this Universal Registration Document.

**Risk factors are assessed in terms of (i) frequency or probability of occurrence, (ii) gross impact (i.e., the impact if there were no risk prevention or mitigation measures), and (iii) the level of control of the organization. The table below shows the results of this net impact risk assessment. Each of the risk factors shown is ranked "low", "medium" or "high" on the risk scale.**

| | Low | Medium | High |
|---|---|---|---|
| **Net impact** | ● | ●● | ●●● |

| **4.1** | **Risk factors** | **Net impact** |
|---|---|---|
| **4.1.1** | **Risks related to the Group's operations and activities** | |
| | *Cybersecurity risk* | ●●● |
| | *Legal risk related to changing regulations* | ●● |
| | *Risk related to the non-renewal, suspension or loss of certain authorizations* | ●● |
| | *Ethics risk* | ●● |
| | *Risk related to litigation or pre-litigation proceedings* | ●● |
| | *Risk related to the production of forged certificates* | ● |
| **4.1.2** | **Human risks** | |
| | *Risks related to human capital* | ●● |
| **4.1.3** | **Risks related to acquisitions** | |
| | *Risk of impairment of intangible assets resulting from acquisitions* | ● |

In 2022, major geopolitical and economic events emerged, while Covid-19 continued to impact some parts of the world.

The effects of the Covid-19 pandemic and the increase in global geopolitical tensions were not considered to call into question the frequency, impact, nature or classification of Bureau Veritas' risks, as shown in the Group risk map. However, some risks are likely to be accelerated.

## 4.1.1 RISKS RELATED TO THE GROUP'S OPERATIONS AND ACTIVITIES



### Cybersecurity risk

**Description**

After two years of Covid-19 and the adaptations it required, 2022 was shaped by the lasting transformation in the use of IT systems. Remote rather than in-office working remained the norm to a large extent, and led to the use of new digital tools and solutions. The war in Ukraine also changed the risk landscape along with the behavior and modus operandi of cyber criminals.

User exposure to a hybrid workspace – company intranet and Internet – continually raises cybersecurity risk over the long term.

In this context, the Group constantly reviews cybersecurity risk to ensure a swift response and is further accelerating its transformation by stepping up measures to protect its business-critical systems and infrastructures:

- the expectations and requirements of the Group's clients in terms of IT security are also constantly growing. Maturity and leadership in cybersecurity and in data protection are therefore directly correlated with clients' trust in the Group and its growth trajectory;
- the Group's activities and processes increasingly rely on technical infrastructure and IT applications to deliver services;
- the Group's international presence requires multiple, interconnected information systems able to process increasing volumes of data. Malfunctions or shutdowns related to external threats (viruses, hacking) or internal threats (malicious acts, violation of data protection) could lead to an inability to ensure continuity of service for the critical information systems that host operating, financial and strategic information, to lost or leaked information, delays and/or additional costs representing a risk for Bureau Veritas' strategy and business continuity. If these databases and the related back-ups were destroyed or damaged for any reason whatsoever, the Group's business could be disrupted.

As part of its business, the Group collects and processes personal data. Within the European Economic Area (EEA), the Group is subject to Regulation (EU) No. 2016/679 of the European Parliament and of the Council on data protection (hereafter the "Regulation"). The Regulation requires a high level of transparency, particularly with regard to data subjects, and increases corporate accountability (elimination of upstream controls of processing tasks, obligation to document any decision made with regard to processing [accountability principle], obligation to report any breach to the competent supervisory authorities, etc.) and the amount of criminal penalties applicable in cases of non-compliance. Similar regulations protecting data privacy also apply in other regions (e.g., Canada, Singapore and Australia) and concern all Bureau Veritas Operating Groups.

**Risk control and mitigation measures**

The risk control and mitigation measures implemented by Bureau Veritas with respect to cybersecurity include the following:

- protection against malicious acts: central security systems have been devised and put in place, offering protection against software attacks (viruses, phishing, etc.), and against attempts to hack into the Group's systems. These security measures and policy are audited every year by a specialized independent company, which simulates intrusion attempts in addition to its audit work;
- new technologies have been introduced to improve Bureau Veritas' protection, detection and response capabilities, in particular PCs, servers and mobile devices;
- a Security Operations Center (SOC) was set up in 2020, covering the Bureau Veritas network, critical infrastructures, back-up systems and the cloud. The SOC has advanced capabilities for managing threats or responding to incidents;
- leading-edge, secure solutions for identity authentication, management and governance were deployed in 2022; two-factor authentication was set up for each user;
- a partnership has been put in place with an application security specialist to perform vulnerability scans and penetration testing, including via ongoing cooperation with the Operating Groups and the central IT teams;
- a Disaster Recovery Plan (DRP) has been developed for the Group's main data centers and its cloud, enabling them to migrate their critical software and infrastructure to an alternative data center in the event of a major disaster, with minimal loss of data;
- a charter defining the rights and responsibilities of Group information system users in terms of cybersecurity has been introduced;
- training and awareness-raising sessions have been organized for all Group users (employees, partners and suppliers) since 2019, helping to reduce vulnerability to hacking and the risk that viruses and other threats will spread;
- collaborative messaging and advanced security solutions designed to reinforce multi-factor authentication and increase protection against phishing have been rolled out across the Group;
- efforts have been made to avoid technologies and solutions becoming obsolete, leading to the large-scale introduction of cloud-based solutions (SaaS as a priority), alongside more timely upgrades and security updates.

Data confidentiality and security, particularly in terms of personal data, is one of the issues taken up in the Group's Compliance Program. This program puts in place the measures needed to enhance the Group's procedures and organization in terms of personal data protection. Data protection risk control and mitigation measures implemented by Bureau Veritas include:

- training and awareness-raising sessions are organized for the Group's employees (senior management, headquarters staff, IT and HR teams, etc.);
- legal and technical measures have been put in place to serve as a framework for ensuring that all processing of personal data within Bureau Veritas complies with the applicable laws and regulations;
- all employees and all external users are briefed on the Group's applicable data protection policies;
- procedures are in place to allow individuals to exercise their rights to privacy and to enable a record of processing activities to be kept and any data breaches to be reported and notified to the competent supervisory authority;
- contracts with external service providers now include stricter requirements: in addition to the provisions regarding the processor's obligations under the Regulation, the Group's contracts now also contain the security measures that must be implemented by the service provider.

**Potential impacts on the Group**

Cybersecurity risk could have:

- financial consequences (loss of client contracts, operating losses, penalties, etc.);
- consequences on the Group's reputation (unlawful disclosure of confidential and personal data, loss of accreditations and/or approvals to provide certain services); and/or
- legal consequences (liability with regard to legal entities and/or individuals on which the Group holds information).

Failure to comply with such regulations could result in criminal and/or financial penalties for the Group and harm its reputation.

**Changes in the risk in 2022**

The measures approved in the wake of the ransomware attack on Bureau Veritas at the end of 2021 were implemented in 2022.

Three key initiatives were launched and rolled out:

- deployment of an EDR solution to protect all Group servers and PCs. Implementation of XDR, an advanced threat detection technology;
- deployment and configuration of new market-leading solutions for identity and access management for all Group users;
- implementation of a “Zero Tolerance” policy for PC equipment, server and network compliance. This program has significantly improved compliance in these areas.

In 2023, the focus will be on strengthening and systematizing user, client and data protection, compliance and resilience by:

- continuing the identity and access management (IAM) program for enhanced data protection and integrating the IAM with EDR/XDR and SASE network technologies;
- pursuing zero-tolerance policies for non-compliant IT equipment and IT stakeholder awareness initiatives to ensure the ongoing compliance of “Security and Privacy by Default” applications and infrastructure and maintaining the security enhancement program for privileged accounts;
- adopting new technologies for network security and cloud access and implementing “Zero Trust” architecture by integrating and combining technologies and processes for managing identity and access, IT equipment and networks.

Despite the measures in place, there is no such thing as zero risk. The Group will continue to strengthen its preparedness to deal with cyber incidents and attacks.

## Legal risk related to changing regulations

**Description**

The Group conducts its business in a heavily regulated environment, with regulations sometimes differing widely from one country to the next. Most of Bureau Veritas' business activities involve inspecting, testing or certifying its clients' compliance with all types of benchmarks and standards (derived from regulations or contracts), and this often requires it to obtain the necessary licenses and authorizations from the relevant public or private bodies.

These regulatory frameworks are therefore at the heart of most of the Group's operating activities and directly determine its capacity to exercise its TIC activities (see section 4.1.2 – Human risks) as well as the operating conditions in which it conducts them.

Amid the economic downturn, clients affected by a possible reversal in their business cycle could be inclined to encourage, advocate (through lobbying efforts) or even demand a relaxation in controls or a reduction in the number of required inspections, tests or certifications performed by their TIC services provider. In this regard, private regulatory frameworks (not resulting from legislation but from contractual standards imposed by clients on their suppliers), such as in the oil and gas sector or retail industry for example, would be the first to be affected by a reduction in the number of tests and/or inspections.

Furthermore, increased competitive pressure on testing, inspection and certification activities could drive an acceleration in efforts to harmonize international or cross-industry benchmarks and standards with which Bureau Veritas clients regularly need to demonstrate their compliance in order to act in accordance with applicable laws and regulations. This would lead to the trivialization and commoditization of the services sold by the Group.

If the trend were to swing the opposite way, it would lead to fragmentation owing to a decoupling of the Chinese, US and European economies. Certain countries could also choose not to allow private or foreign companies to engage in the local TIC market, or may decide to change the rules for conducting business such that the Group can no longer operate in those countries.

**Risk control and mitigation measures**

The Group endeavors to monitor all of these changes through its regulatory intelligence in order to anticipate, monitor and give its input to the competent authorities when new regulations are being drafted.

As a member of national and international associations of the TIC profession, including the TIC Council (formerly the International Federation of Inspection Agencies – IFIA) and the International Association of Classification Societies (IACS), Bureau Veritas is able to keep informed of any such regulatory changes.

**Potential impacts on the Group**

It follows that changes in regulations applicable to the Group's businesses may be either favorable or unfavorable. Stricter regulations or stricter enforcement of existing regulations, while creating new business opportunities in some cases, may also result in new conditions for the Group's activities that increase its operating costs, limit the scope of its businesses (for example, in connection with real or perceived conflicts of interest) or more generally slow Bureau Veritas' development.

In particular, important changes in regulations or legislation applicable to the Group's businesses in the principal countries where it operates may lead to frequent, or even systematic, claims involving the professional liability of employees, the Company or its subsidiaries. The Group could face multiple lawsuits and may be ordered to pay substantial damages, despite the fact its services were provided in the jurisdiction prior to any regulatory changes. In extreme cases, such changes in the regulatory environment could lead Bureau Veritas to exit certain markets where it considers the level of regulation to be overly restrictive.

A relaxation in requirements or harmonization of laws, regulations, benchmarks and standards which form the basis of Bureau Veritas' testing, inspection and certification services, would potentially have a negative impact on revenue. This would also be the case if its clients relaxed the requirements imposed on their supply chains (standards, regulations and contractual requirements controlled by the Group). A decoupling of the Chinese, US or European economies would impact operating profit due to a potential increase in compliance costs or in the costs incurred to adapt Group facilities in different countries for certain laboratories.

**Changes in the risk in 2022**

On the whole, the analysis of this type of risk inherent to the Group's TIC activities in 2020 and 2021 remained relevant in 2022, leading Bureau Veritas to consider:

(i) the impact of deteriorating economic conditions on the financial health of its clients, potentially leading to pressure on the regulator to:
- relax or push back the introduction of new mandatory standards and regulations,
- reduce the number of tests, inspections and certifications usually carried out by the Group on behalf of its clients (when they are not required by law or regulations);

(ii) the impact of increased competitive pressure (via the trivialization and commoditization of the services sold by the Group) resulting from an acceleration in efforts to harmonize international or cross-industry standards, rules and regulations with which its clients have to comply;

(iii) changes in the geopolitical situation leading to increased protectionism and a decoupling of the Chinese, US and European economies, with a resulting reduction in international trade between these regions and countries.

## Risk related to the non-renewal, suspension or loss of certain authorizations

**Description**

Much of the Group's business requires it to obtain and maintain accreditations, approvals, permits, delegations of authority, official recognition and authorizations more generally (hereafter referred to as "Authorizations") at local, regional or global level, issued by public authorities or by professional organizations following long and often complex review procedures.

Most Authorizations are granted for limited periods of time and are subject to periodic renewal by the authority concerned. For some of its businesses (in particular Government Services in the Agri-Food & Commodities business and Marine & Offshore), the Group (or division concerned) must be an active member of certain professional organizations in order to be eligible for certain projects.

Although the Group closely monitors the quality of services provided under these Authorizations, as well as the renewal and stability of its Authorizations portfolio, any failure to meet its professional obligations or conflicts of interest (real or perceived as such), could cause Bureau Veritas to lose one or more of its Authorizations either temporarily or on a permanent basis. A public authority or professional organization which has granted one or more Authorizations to the Group could also unilaterally decide to withdraw such Authorizations.

Government Services (included within the Agri-Food & Commodities business), and in particular Destination Inspection or Technical Assistance to Customs, Verification of Conformity (VOC) and Single Window (SW) solutions, involve a relatively limited number of programs, contracts and accreditations (hereafter referred to as "Contracts") signed with or granted by governments or public authorities ("Authorities").

These Contracts, awarded within the scope of international calls for tender, have terms of between three and five years (sometimes ten years for Single Windows). Since the ultimate purpose of these Contracts is to transfer expertise to the Authorities, they are often not renewed and the related operations are often discontinued once the expertise has been transferred to said Authorities. This could cause revenues in the country concerned to suddenly dry up.

However, certain Contracts that are not renewed may be supported by local teams in the form of technical assistance provided to the Authorities, allowing operations to continue in that country.

**Risk control and mitigation measures**

For each of its businesses, Bureau Veritas has put in place a specific organization for managing and monitoring Authorizations. The management of Authorizations used in several countries was reinforced in 2017, particularly in the Agri-Food & Commodities, Certification, Industry and Marine & Offshore businesses, through optimum organization and implementation of control tools (especially employee qualification management and supervision, Internal Audit management, shared service centers to monitor execution, and Commitment Committees to analyze and prevent conflicts of interest). These tools and systems are regularly reviewed and enhanced by the Group.

Centralized management of international Authorizations has been stepped up and their geographic footprint streamlined in order to limit the Group's exposure to the risk of losses. Internal initiatives aimed at raising awareness of potential conflicts of interest and accreditation requirements have also been rolled out so that the risks associated with Authorizations can be better understood and addressed.

To reduce its exposure, Bureau Veritas endeavors to diversify the geographic footprint of its portfolio of Government Services businesses and to structure its programs so that services are paid for by the operators and not by the relevant governments. By engaging in ongoing intensive diplomatic and commercial efforts, the Group is also better able to anticipate crises and manage such risks if they were to arise.

Lastly, Bureau Veritas seeks to secure its Contracts as far as possible with the help of its internal and external counsel. Additional information on these Authorizations and their management is provided in section 1.6 – Accreditations, approvals and authorizations and section 4.2 – Internal control and risk management procedures, of this Universal Registration Document.

**Potential impacts on the Group**

The non-renewal, suspension or loss of any of these Authorizations and Contracts, or of its position as member of certain professional organizations, could have a significant adverse effect on the Group's business, financial position, earnings or outlook.

For example, in Government Services, the Group has around 30 Contracts of the type described above, most of which involve services for countries in Africa, the Middle East and Asia. These Contracts, which represent aggregate revenue of around €180 million, are generally for a period of one to three years (or ten years for Single Window). Many of them are subject to local administrative law and may be unilaterally terminated at short notice at the discretion of the government or authority concerned. They are also subject to the uncertainties inherent in conducting business in emerging countries, some of which have been or could be subject to political or economic instability, sudden and frequent changes in regulations, civil war, violent conflict, social unrest or actions of terrorist groups. The suspension, cancellation or non-renewal of even a small number of these Contracts could have a significant adverse effect on the Group's business, financial position, earnings or outlook.

In addition, in performing the Contracts entered into with governments or public authorities, the Group may face difficulties in collecting amounts receivable, and the collection process could prove long and complex. The non-payment or late or partial payment of substantial sums owed under these Contracts could also have a significant adverse effect on Bureau Veritas' business, financial position, earnings or outlook.

**Changes in the risk in 2022**

The risk related to the non-renewal, suspension or loss of certain Authorizations is still declining thanks to prevention measures rolled out by the Group.

## Ethics risk

**Description**

The Bureau Veritas brand is that of a recognized world leader operating with unparalleled know-how, independence, objectivity and integrity for almost two centuries. Independence, objectivity and integrity are the foundation of trust, and trust is at the heart of Bureau Veritas' relations with its clients. The Group's communications are a tangible demonstration of its commitment to "Shaping a World of Trust". Ethics has long been an "absolute" for Bureau Veritas, which strives to enforce strict ethical values and principles in conducting its business (principles of transparency, honesty and integrity, fight against corruption, fair employment, health and safety). However, the risk of isolated acts in breach of these values and principles by Group employees, agents or partners cannot be ruled out. These may include employee actions or failures to act in the face of corruption in order to secure personal gain, facilitate business development, avoid or settle disputes or fast track administrative decisions, as well as fraudulent acts, conflicts of interest, anti-competitive practices, violation of international economic sanctions, and more.

In terms of ethical conduct, Bureau Veritas believes its main risk exposure to be the passive corruption of a Group employee during an audit carried out at a client's premises or at the premises of one of the client's suppliers on behalf of that client. This risk increases when (i) the client or company audited is located in a jurisdiction where corruption is considered to be endemic, culturally accepted or commonly attempted, or (ii) the audited entity's business or the development of that business depends on the delivery of a favorable report by a Group employee. Failure to comply with independence or objectivity rules (which may or may not result from an act of passive corruption) is also considered a major risk for the Group.

In addition, in performing the Contracts entered into with governments or public authorities, the Group may face difficulties in collecting amounts receivable, and the collection process could prove long and complex. The non-payment or late or partial payment of substantial sums owed under these Contracts could also have a significant adverse effect on Bureau Veritas' business, financial position, earnings or outlook.

**Risk control and mitigation measures**

Thanks to the deep-seated and broadly publicized commitment of its Executive Management team, the Group has set up a Compliance Program. This includes a Code of Ethics and a manual of internal rules and procedures applicable to all employees, a dedicated central and regional internal organization, a whistleblowing hotline, specific training courses, and a corruption risk map, as well as third-party due diligence and audit procedures, which fall under the responsibility of the Group's Ethics Committee. Any incidents of identified non-compliance with the Group's ethical standards are subject to disciplinary measures. These risk management procedures are audited every year.

The Group's Compliance Program is described in further detail in section 4.2 – Internal control and risk management procedures and in section 2.5.1 – Ethics, of this Universal Registration Document.

**Potential impacts on the Group**

Group employees, executives or companies may be held liable for any failure to comply with ethical principles and standards. This risk is heightened by the number and variety of the commercial partners working with Bureau Veritas (intermediaries, partners and subcontractors) and by the fact that the Group does business in certain countries that are particularly well known for corruption risk. This situation could therefore lead to penalties – particularly financial penalties – and/or affect Bureau Veritas' reputation and image, and adversely impact its businesses, financial position, earnings and/or outlook.

As well as legal and administrative penalties and reputational harm, failure to comply with the Group's ethical principles and standards could render stakeholders liable as well as result in the loss of accreditations, approvals, delegations of authority, official recognition and more generally, of authorizations issued by public authorities or professional organizations.

**Changes in the risk in 2022**

The ethics risk remains intrinsically the same from one year to the next. The degree of management improves as new and ever stricter procedures and controls are put in place.

## Risk related to the production of forged certificates

**Description**

The Group's main mission is to ensure that products, assets and systems comply with a given framework (mainly standards and regulations in terms of quality, safety, environmental protection and social responsibility). Bureau Veritas acts as an independent body and issues reports and certificates stating that products, assets and systems conform to applicable standards and regulations. Certification enables companies to conduct their business activities (e.g., place products on the market), access new markets or strengthen their reputation.

Since obtaining certification is often vital for companies, Bureau Veritas is exposed to the risk that its reports or certificates are falsified or tampered with, or that counterfeit reports or certificates are issued, infringing Bureau Veritas' trademarks and/or copyright. The production of forged or counterfeit reports can result from employee conduct or, more commonly, external sources (fraudulent behavior by a client or third party in order to meet regulatory requirements).

**Risk control and mitigation measures**

A policy aimed at preventing counterfeit certificates and reports has been in place in the Group since 2015. Whenever there is a suspected case of forged or counterfeit certificates, the Group conducts an investigation to rapidly identify the source and authors of the forgeries/counterfeits. Where applicable, it informs clients, accreditation bodies and, if necessary, government and customs authorities in accordance with applicable legal and regulatory requirements. Legal and criminal proceedings are also initiated to put a stop to the fraud and seek damages for the harm suffered by the Group. Penalties may be adopted against those responsible.

For example, an employee was suspended and subsequently dismissed after it was discovered he had tampered with the results of analyses. Clients and the relevant legal authorities were immediately notified of the discovery.

The Group's Compliance Program, described in further detail in section 4.2 – Internal control and risk management procedures and in section 2.5.1 – Ethics, of this Universal Registration Document, helps to prevent and, where necessary, detect any fraud resulting from inappropriate employee conduct.

To address external counterfeit risks, the Group has developed technologies using timestamping, electronic signatures and QR codes for certificates or reports in a bid to reduce the risk of forged or counterfeit certificates and improve the traceability of the reports and certificates issued by Bureau Veritas.

**Potential impacts on the Group**

This situation could lead to legal proceedings (civil and criminal), jeopardize the Group's ability to maintain or renew the Authorizations it needs to pursue certain activities, result in the withdrawal of certain products from the market and/or damage the reputation of the Group and the TIC industry in general. It could also adversely and significantly impact Bureau Veritas' businesses, reputation, image, financial position, earnings and/or outlook.

**Changes in the risk in 2022**

The risk of forged certificates or reports remains stable, even though developments in information technologies could make such counterfeits either easier to produce and/or harder to detect or identify, despite the Group's efforts in this regard.

Accordingly, the Group stepped up very significantly the deployment of technologies aimed at protecting against forgery and improving the traceability of reports and certificates in order to provide protection for all of its businesses. These technologies notably allow end users to verify document authenticity and content accuracy online.

## Risk related to litigation or pre-litigation proceedings

### Description

As for any TIC company, the nature of Bureau Veritas' testing, inspection and certification activities is such that there is an inherent risk of the quality and pertinence of its work and findings being called into question in the event that flaws are subsequently identified or should major incidents occur.

What makes these types of claims different is that inspection companies can be held liable for sums that are often disproportionate in light of the amounts actually paid for the services provided.

In the normal course of business, the Group is therefore involved in a large number of litigation or pre-litigation proceedings seeking to establish its professional liability on a contractual or extra-contractual basis in connection with services provided.

Bureau Veritas is particularly exposed in terms of (i) frequency of occurrence: due to France's Spinetta law of January 4, 1978, which establishes a presumption of joint and several liability for technical inspectors, the Group's Construction business in France sees significant, recurring claims and the Group's creditworthiness could also encourage third parties to make claims against it; (ii) timing: there may be a substantial delay between the date services are provided and the date a legal claim is filed or a legal decision is handed down (certain proceedings can last between 10 and 20 years); (iii) financial penalties: services provided for hundreds or thousands of euros can give rise to claims seeking several millions of euros in damages; and (iv) geographic presence: the Group operates in almost 140 countries, including countries whose legal and political systems can be unpredictable.

To put pressure on Bureau Veritas, in addition to litigation, some claimants readily initiate administrative or even criminal proceedings that are unfounded but can harm the Group's image, for example proceedings seeking to call into question licenses granted to the Group.

Accordingly, we cannot rule out that new claims may be made against a Group company in the future, leading to substantial liability for the Group and thus having a significant adverse effect on the Group's business, financial position, reputation, earnings or outlook. A detailed description of major legal proceedings to which the Group is a party is provided in section 4.4 – Legal, administrative and arbitration procedures and investigations, of this Universal Registration Document.

### Risk control and mitigation measures

Bureau Veritas has implemented procedures aimed at preventing, monitoring and managing litigation. These procedures are described in section 4.2 – Internal control and risk management procedures, of this Universal Registration Document.

The Group's legal experts work closely alongside its lawyers across the globe to manage these risks as effectively as possible. The Group also seeks to significantly insure itself against all financial consequences of claims asserting professional liability.

Provisions may be set aside to cover expenses resulting from such proceedings. The amount recognized as a provision is the best estimate of the expenditure required to settle the present obligation at the end of the reporting period. Details of total provisions for contract-related disputes are provided in section 6.6 – Notes to the consolidated financial statements, Note 27 – Provisions for liabilities and charges, of this Universal Registration Document.

### Potential impacts on the Group

Substantial fines or damages handed down by a court in respect of an incident not insured by a pertinent insurance policy and not adequately provisioned for could have a significant adverse impact on the Group's consolidated financial statements.

Moreover, multiple awards leading to substantial payouts from insurers under the Group's insurance policies could result in a sharp rise in insurance premiums due to the negative claims history.

### Changes in the risk in 2022

The Group's efforts to manage this risk as effectively as possible by fine-tuning internal processes and extending insurance coverage are paying off. The Group's civil liability claims history remained stable, although there is no guarantee this trend will continue owing to the global economic, commercial, political and legal environment in which the Group operates.

## 4.1.2 HUMAN RISKS

### Risks related to human capital

**Description**

The Group employs more than 82,000 people, the majority of whom work in areas requiring a high level of technical and specialist skills. On account of its global reach, Bureau Veritas has to attract and retain these highly-skilled and/or high-potential employees in virtually all of the countries in which it does business. Risks related to human capital concern talent management and, in particular, the Group's ability to attract, retain, develop and engage its staff, particularly its highly-skilled employees.

- an unsatisfactory staff attrition rate;
- longer recruitment times to fill vacancies with qualified candidates;
- insufficient workforce diversity;
- unknown or low levels of employee engagement;
- an inadequate sense of well-being among employees.

**Risk control and mitigation measures**

Bureau Veritas has formally set down a Human Resources (HR) strategy that focuses on three key elements of talent management to attract, engage and develop its employees. The HR strategy designs and implements initiatives to attract the best talent to Bureau Veritas and to offer an employee experience that fuels the Group's sustainable growth, while enabling employees to realize their developmental goals. Bureau Veritas' HR strategy also aims to provide an inclusive development and performance-driven culture, in which the well-being of its employees is essential to its business. In addition, the HR strategy is designed to reward and recognize employees' contributions in a fair, consistent and transparent manner.

Key HR strategy initiatives that manage and mitigate risks related to human capital include:

- employer brand image: continued improvement of the LEAVE YOUR MARK employer brand, including greater emphasis on the Group's Green Line of services and solutions; career possibilities with Bureau Veritas; the Group's inclusive culture; and better profiling of the demographic diversity of employees, including those who work in "non-traditional" departments, and those with highly sought-after expertise, such as data scientists and software developers;
- recruitment of high-potential employees: leveraging new channels to identify potential recruits, including search platforms using enhanced artificial intelligence; continuous improvement of internal recruitment processes and technologies; and reviews of the organizational design of recruitment;
- attrition: evaluation of employee engagement through the "BVocal" survey; development of strategy; and implementation of initiatives at Group, divisional and individual team levels, all tailored to feedback collected from the questionnaires;
- diversity: monitoring of and reporting on a series of diversity measures, some of which are used as key performance indicators (KPIs) linked to management's variable compensation, including those related to improving the representation of women on executive bodies; ongoing development of the capabilities of all managers and team leaders in building more diverse teams and an inclusive culture, notably illustrated by the "Leading Inclusive Teams@BV" program; and leadership programs for high-potential women employees aimed at fast-tracking their career development;
- talent development: robust and regular talent assessment and development processes at Group and divisional levels to ensure an adequate and diverse pool of talent for key positions in the future. Emphasis is placed on approaches to develop high-potential employees' versatility, enabling them to work across all Group areas;
- employee well-being: mandatory employee training on workplace safety; and provision of educational materials, resources and guidance on relevant topics within the Group's well-being policy (emotional, financial, physical and "purpose & community engagement"). The Group also reviews and provides ongoing information on select policies and approaches related to employee well-being, including for those affected by situations such as the conflict in Ukraine and the Covid-19-related lockdowns in China.

**Potential impacts on the Group**

An unsatisfactory employee attrition rate and lengthy recruitment times to fill vacancies with qualified candidates could compromise the quality of the Group's services, affect its ability to meet client expectations and impact the ability to achieve the growth objectives set by the Company.

Insufficient diversity among employees and prospective employees could compromise the Group's ability to execute the aspects of its strategy based on growth and profitability through innovation, and could also make it more difficult to tangibly demonstrate workforce diversity and the inclusive culture that are part of the Bureau Veritas brand.

Inadequate employee engagement could prevent the Group from achieving a satisfactory and sustainable level of productivity and growth, and could harm its employer brand.

An inadequate sense of well-being among employees could lead to accidents, a rise in absenteeism, lower productivity and a decline in employee engagement. It could also harm the employer brand.

**Changes in the risk in 2022**

So far, Bureau Veritas has not been significantly impacted by the volatile economic environment in 2022 in terms of its ability to recruit and retain high-potential employees. Nevertheless, given the current global labor market, Bureau Veritas believes that, for certain specific roles in certain countries, there is a significant risk of increased attrition and longer recruitment times to fill vacancies with qualified candidates with diverse profiles.

In 2022, the Group significantly expanded the population covered by its employee engagement survey: A total of 49,500 employees were given the opportunity to complete the survey, compared to 39,000 in 2021. Thanks to this broad coverage coupled with a rigorous approach that uses the findings of the survey to determine what measures to take, the risk of a decline in employee engagement is low.

Given public exposure to the Covid-19 virus, the travel restrictions put in place by the authorities in some countries, the geopolitical instability caused by the conflict in Ukraine, the impact of inflation on purchasing power, and increased uncertainty in terms of energy consumption, employee well-being is classified as a high risk, despite the relevant mitigation measures that are in place.

## 4.1.3 RISKS RELATED TO ACQUISITIONS

### Risk of impairment of intangible assets resulting from acquisitions

**Description**

A significant proportion of the assets recorded on the Company's statement of financial position corresponds to intangible assets resulting from business combinations. Goodwill as reported in the statement of financial position at December 31, 2022 amounts to €2,143.7 million, or 30.1% of total assets (€7,119.2 million).

**Risk control and mitigation measures**

In accordance with current IFRS standards, the Group tests the fair value of its indefinite-lived intangible assets each year, based on which it decides whether or not to recognize impairment against these assets.

The testing approach used is detailed in section 6.6 – Notes to the consolidated financial statements, Note 11 – Goodwill, of this Universal Registration Document.

**Potential impacts on the Group**

The value of intangible assets depends on the future operating profit of the companies acquired and the discount rates used, which themselves are dependent on the current and future economic and financial environment.

Changes in the assumptions underpinning their valuation can lead the Group to write down certain intangible assets. In accordance with current IFRS standards, impairment taken against certain intangible assets cannot be reversed.

Any such impairment would reduce attributable net profit and equity. However, there would be no impact on cash flow for the period.

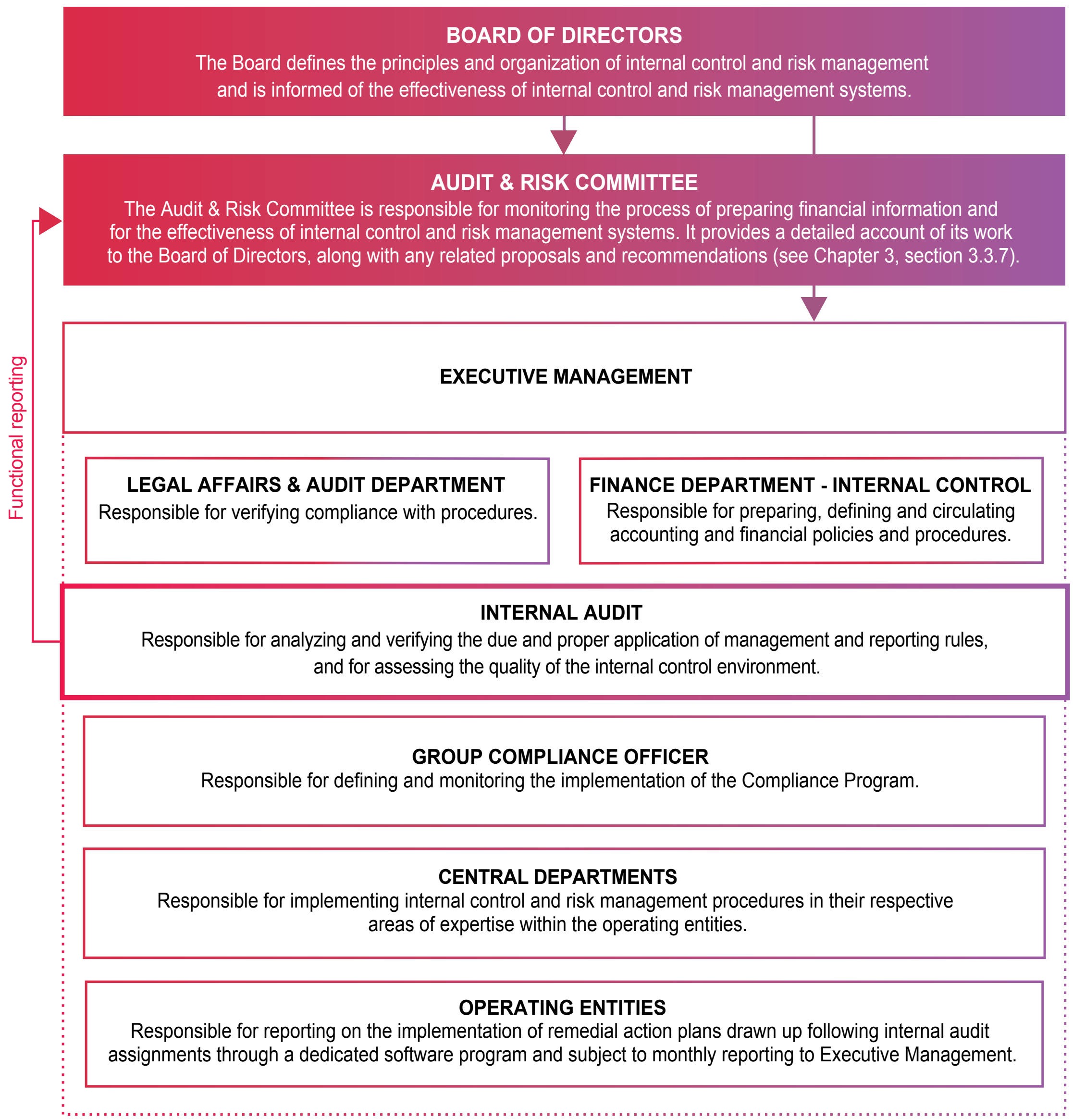
**Changes in the risk in 2022**

No significant changes in the risk were identified in 2022.

# 4.2 INTERNAL CONTROL AND RISK MANAGEMENT PROCEDURES

## 4.2.1 ORGANIZATION AND GENERAL APPROACH TO INTERNAL CONTROL AND RISK MANAGEMENT

**Main internal control and risk management stakeholders**



## Executive Management

Group Executive Management ensures that internal control objectives are set, particularly with respect to the control environment, risk assessment and management, internal control processes, reliable financial information and Group business management, based on the principles and organization previously defined by the Board of Directors.

Internal control as implemented within Group companies is based on the following principles:

- recognition of the full accountability of the management of Group companies;
- regular financial reporting;
- monitoring of relevant indicators by the different Group departments; and
- regular and occasional reviews of specific items as part of a formal or one-off process.

Where necessary, however, this general framework is adjusted for simplicity purposes so that the internal control process continues to be aligned with the size of the companies within the Group and so that the management teams of Group entities can duly discharge their responsibilities.

## Audit & Risk Committee

In accordance with article L. 823-19 of the French Commercial Code (*Code de commerce*), the Audit & Risk Committee is chiefly responsible for monitoring the process of preparing financial information, the effectiveness of internal control and risk management systems and, where applicable, those of Internal Audit, and the independence of the Statutory Auditors.

After each meeting, the Chairman of the Audit & Risk Committee prepares a detailed report of the Committee's work, proposals and recommendations for the Board of Directors.

Details of the work of the Audit & Risk Committee during 2022 are provided in section 3.3.7 – Committees of the Board of Directors, of this Universal Registration Document.

## Internal Audit

The Internal Audit department reports to the head of Legal Affairs & Audit. To reinforce the department's independence, it also reports functionally to the Chairman of the Audit & Risk Committee since the end of 2018.

The role of the Internal Audit department is to perform audits, principally financial audits, in the various entities of the Group. The entities to be audited are selected at the time of preparing the annual audit plan, which is discussed with Executive Management and validated by the Audit & Risk Committee. They are chosen primarily based on the risks identified, the resulting financial implications and previous internal or external audits. This formal, structured approach is designed to ensure adequate audit coverage for the Group's entities over several years. In addition, the Internal Audit department oversees the Group's recently acquired entities and regularly liaises with the Legal, Risk, Assurance and Compliance functions as part of its work.

In 2022, as the pandemic continued to affect several parts of the world, certain audit assignments were performed remotely by internal auditors. This enabled internal audit arrangements to be maintained, despite a deterioration in the conditions in which the assignments were performed.

These audits are aimed at analyzing and verifying that management and reporting rules are duly applied, as well as reviewing the quality of the internal control environment. The main procedures and cycles covered are:

- billing and revenues;
- purchasing, subcontracting and accounts payable;
- Human Resources;
- cash management;
- tax;
- financial statement closing procedures and reporting;
- the Group Compliance Program; and
- IT risks.

In addition, a review of the financial performance of the Group's businesses is conducted when each audit assignment is carried out to verify the consistency of all the financial information produced by the entity being audited. The Internal Audit team continued its audit procedures relating to the Group's Corporate Social Responsibility policy.

The audit reports are sent to the managers of the operating entities and to their superiors, the central operating departments and Group Executive Management. Audit reports set out remedial action plans for improving the control environment.

The Internal Audit department systematically monitors implementation of the action plans drawn up following Internal Audit assignments through a dedicated software program accessible to the audited departments, and gives Executive Management a monthly progress update on the implementation of recommendations.

In 2022, the implementation rate of recommendations issued by the Internal Audit department averaged just over 80%.

In addition to the annual audit program, the Internal Audit department heads up an internal control self-assessment campaign via the distribution of two questionnaires across the Group (see "Internal control framework and general principles").

## Group Compliance Officer

The Group Compliance Officer reports to Executive Management and draws on the resources of the Legal Affairs & Audit department.

The Group Compliance Officer is the head of the Bureau Veritas Compliance Program and a member of the Group's Ethics Committee, which also comprises the Group Chief Executive Officer, the Deputy Chief Executive Officer, the Group Chief Financial Officer, and the Group Chief Human Resources Officer. This Committee deals with compliance issues within Bureau Veritas and supervises the implementation of the Code of Ethics. The Group Compliance Officer also relies on a network of Compliance Officers, the department's liaisons in the Group's different Operating Groups. The head of each operating unit is responsible for implementing and managing the Code of Ethics and the Code of Ethics manual within his or her particular remit, overseen by his or her Executive Vice-President.

## Central departments

The implementation of internal control and risk management procedures is the responsibility of the central departments in their respective areas of expertise, i.e., Legal Affairs & Audit, Human Resources, Finance, Quality, Health & Safety, Security and Environment (QHSE), and Technical, Quality and Risk.

- The Legal Affairs & Audit department provides advice and assistance for any legal, insurance, risk and compliance issues affecting the Group. It helps review calls for tender, major contracts and mergers and acquisitions, and analyzes or supervises Group litigation and claims as necessary. In close cooperation with operational staff and the Group's Technical, Quality and Risk departments, the Legal Affairs & Audit department helps identify the main risks associated with the Group's activities, particularly by overseeing risk maps, and circulates the Group's risk management policies and procedures. It is responsible for taking out the Group's professional civil liability and property and casualty insurance policies. It also defines, implements and supervises the Group's Compliance Program, which includes the Code of Ethics and its internal application procedures, a risk map relating to corruption and international sanctions, an externally managed ethics alert procedure, specific training and regular internal and external audits.
- The Human Resources department circulates the evaluation and compensation policies applicable to Group managers and ensures that all Group employees are compensated and assessed on the basis of objective, predefined criteria.
- The Finance department consolidates all of the Group's financial information and manages the necessary reconciliations. It ensures that Group standards and frameworks are strictly applied, including the Group Management Manual (GMM). In this respect, it defines a series of procedures, tools and references intended to guarantee the quality and consistency of information provided (management reporting, financial statements). In particular, monthly reviews of results of operations, the net cash position and consolidation data allow financial and accounting information to be continually monitored and checked for consistency on a centralized basis.
- The Quality, Health & Safety, Security and Environment department defines and oversees the Group's quality, safety, security and environment management system. It ensures that the various Operating Groups implement management systems, leads the continuous improvement process and organizes the verification of compliance with procedures.
- The Technical, Quality and Risk departments across the Operating Groups are responsible for drawing up the technical risk management policy and verifying the technical quality of services provided, the technical qualification of organizations (overseeing operating rights and accreditations) and operators, and applying technical guidelines and methodologies rolled out by the Group. They rely on local networks to circulate procedures and verify that they are duly applied among operating entities. They are tasked with auditing the operating entities, defining any corrective actions required and ensuring that these actions are implemented.

# Internal control framework and general principles

Bureau Veritas has adopted the general principles of the AMF's Reference Framework and has put in place a system that covers all of the Group's subsidiaries. The aim is to provide them with a tool that they can use for internal control self-assessment and for identifying areas of improvement.

In accordance with the aforementioned Reference Framework, two annual self-assessment questionnaires are used at registered office level by the Internal Audit department: one covers the general principles of internal control, while the other concerns financial and accounting internal control more specifically, and, in particular, how the finance and accounting functions are organized at central level, intended for support functions (particularly Finance).

In 2022, internal control procedures were also modernized and strengthened by implementing periodic controls in all Group subsidiaries via a centralized system. This new system sets out the essential financial controls that can be implemented by each subsidiary, with teams authorized and empowered to document and validate them on a single platform.

At the time of each audit assignment, the Internal Audit department reviews the quality of the findings of the internal audit procedures. External auditors also review the internal control system as part of their work.

Like any system, internal control is dynamic and constantly improving, but it cannot provide absolute assurance that all risks have been eliminated.

# Risk management framework and general principles

## Organization

The Group's risk management policy is focused on ensuring that the operating entities fulfill their contractual obligations in a competent and professional manner and on preventing professional civil liability claims for damages relating to a product, system or facility in respect of which the Group's entities had provided services.

Risks are managed through a structured organization rolled out within the Group's different Operating Groups. This organization is based on two complementary cross-functional networks and their respective departments: the Legal Affairs & Audit and the Technical, Quality and Risk departments.

The broad range of local operations and the need to give managerial autonomy to operational staff have led to the introduction of a global risk prevention strategy, which has been formally set down and rolled out to each division and Operating Group.

### Mapping and managing risk

The Group regularly prepares and updates risk maps under the supervision of the Legal Affairs & Audit department, with help from all Operating Groups and support functions in order to identify and quantify the main risks and thereby improve risk management procedures. In 2021, following the comprehensive risk mapping process conducted in 2020, each priority risk, selected by the Executive Committee from among the 40 key risks identified, was the subject of working groups aimed at developing action plans to be deployed across the Group. A specific organization was defined for this purpose, including Risk Owners, appointed for each priority risk from among the Executive Committee members, and a network of Risk Managers appointed by the Executive Committee within each Operating Group. This process allows the necessary actions to be implemented. To manage these risks, specific action plans are being developed and will be subsequently rolled out by the operating teams under the responsibility of the Risk Officers designated by the Executive Committee. Cross-functional initiatives, mainly relating to technical standards, monitoring regulations and global insurance programs, are also defined and implemented across the Group.

In 2022, the Group's risk map was updated, with input from the members of the Executive Committee and the network of Risk Managers in each Operating Group. The updated risk map takes into account the impact of the action plans implemented under the responsibility of the Risk Owners (members of the Executive Committee) in 2021 and 2022, as well as changes in the Group's internal and external environment. Following the same approach as that used for the risk mapping in 2020, this revision resulted in the identification of new or existing priority risks, the appointment of Risk Owners within the Executive Committee, and the launch or continuation of action plans.

The operating departments also prepare targeted risk analyses when new business activities are launched or when the Group responds to calls for tender, assisted by the Technical, Quality and Risk departments and the Legal Affairs & Audit department.

Within its networks, the Group's operational risk management policy aims to increase the number and specialization of technical centers. The Group wishes to develop Bureau Veritas technical standards that can be applied throughout the world, while satisfying the requirements of countries that apply the most stringent regulations.

Application of the risk management policy and the continual changes in services that the Group is asked to provide requires the commitment of local networks and risk management officers on all fronts (technical, quality, legal and compliance), thereby ensuring that they work together to enhance the Bureau Veritas brand image and reduce the risks of professional civil liability claims against the Group. The goal is to share the risk management approach and its objectives with operating teams, along with the information needed to take decisions consistent with the objectives set by the Board of Directors.

### Preventing and monitoring litigation

The Legal Affairs & Audit department has put in place resources and procedures to enable twice-yearly assessments of disputes. A root cause analysis is also performed each year, in conjunction with Operating Groups for atypical disputes (after the fact).

The procedure for preventing and monitoring litigation is covered in the risk management policy. It describes the methods for managing litigation which require coordination between heads of operating entities, the Operating Groups, and the Legal Affairs & Audit department.

Each Operating Group defines the organization it has put in place to achieve the Group's objectives, in order to:

- identify disputes from the outset;
- make sure that the relevant insurers are informed of any litigation claims;
- organize an effective management approach regarding the defense of the Group's interests; and
- allow a centralized follow-up of significant litigation by the Legal Affairs & Audit department.

The Group's policy of centralizing its professional civil liability and property and casualty insurance through global programs also facilitates controls and reporting.

## Sustainability risks

Sustainability risks are analyzed through a process set by the Group's Risk department. The general principles, organization and framework for managing these risks are detailed in section 2.4 – Sustainability risks and opportunities, of this Universal Registration Document.

## 4.2.2 INTERNAL CONTROL PROCEDURES

### Financial and accounting information

In order to implement internal control procedures relating to the production of financial and accounting information, the Group refers to:

- **external standards** including all national accounting laws and regulations based on which Group entities prepare their financial statements. The Group prepares its consolidated financial statements according to International Financial Reporting Standards (IFRS); and
- **internal standards** consisting of the Group Management Manual (GMM), which covers all financial, accounting and tax procedures.

The role of the Finance department is to provide reliable information and pertinent analyses in a timely manner and to act as an expert with respect to financial and financing issues within the Group. The department is responsible for setting rules for applying standards, consolidating results, managing cash and particularly hedging and exchange rate risks, managing tax issues and supervising credit risks. It also acts as a motivating force in certain improvement initiatives, such as the development of shared service centers.

The Finance department is assisted by a network of Finance Officers across the Group. These report to the heads of operating departments and, from a functional standpoint, to the Group Chief Financial Officer.

Subsidiaries operating in different countries are responsible for implementing the policies, standards and procedures defined by the Group.

The budget process is structured in a way that enables objectives to be set at the level of the Operating Groups. The resulting budget is therefore a highly effective oversight tool that can be used to closely monitor monthly activity at the level of each country/business. This monthly control of results from operations, the net cash position and consolidation data enables Executive Management to effectively monitor the Group's financial performance.

The Group has also defined internal rules and procedures designed to safeguard assets, prevent and identify fraud, and ensure that accounting information is reliable and presents a true and fair view of the business.

### Acquisitions Services

The Internal Audit & Acquisitions Services department also provides integration assistance on acquisitions. This role is based on a series of procedures known as the Post Merger Integration Plan (PMIP), covering Finance, Human Resources, Communication, Legal Affairs & Audit (including Compliance), Information Systems & IT, and Quality, Health & Safety, Security and Environment (QHSE).

Where appropriate, the Internal Audit & Acquisitions Services department assists the Operating Groups responsible for integration and liaises with all registered office support functions as part of a continuous improvement approach.



## 4.2.3 RISK MANAGEMENT PROCEDURES

### Monitoring accreditations – role of Technical, Quality and Risk departments

Bureau Veritas holds a large number of "licenses to operate" (accreditations, authorizations, delegations of authority, etc.) which may be issued by national governments, public or private authorities, and national or international organizations as appropriate.

Each of the Group's businesses has put in place a dedicated organization for managing and monitoring these authorizations on a centralized or local basis, and the authorizations are subject to regular audits by the authorities concerned.

The aim of the Technical, Quality and Risk departments is to ensure that the services provided by each Group entity are carried out in compliance with Bureau Veritas procedures, particularly management of conflicts of interest, as regards the application of technical guidelines and methods defined by the Group, and in accordance with the regulatory or private terms of reference of the accrediting organization.

The Group has implemented an operating organization for which the degree of centralization depends on the business:

- in businesses that are managed globally and that offer similar services (Marine & Offshore, Certification, Consumer Products and Government Services, Industry), the Technical, Quality and Risk departments are centralized and provide the procedures and rules to be applied throughout the world;
- in businesses that are managed locally and provide their services based on local technical standards, local Technical, Quality and Risk Officers specify the methods to be applied in their country/region under the supervision of a central Technical department.

The various Technical, Quality and Risk departments use a structured network of officers in each Operating Group and each year perform a certain number of technical audits to ensure that procedures are complied with and that the rules defined by the Group and the methodologies defined locally are respected.

## Quality and ISO certification

The Quality, Health & Safety, Security and Environment department is responsible for implementing and managing a quality system that supports the operating and functional entities in their aim to continually improve the processes that these entities have put in place to meet their clients' needs. These procedures have been certified to ISO 9001 by an accredited international body.

To this end, the Quality, Health & Safety, Security and Environment department has a structured network of officers around the world and at central level.

## Human Resources

The Group's Human Resources (HR) department ensures that manager compensation and evaluation policies are consistent and fair, while taking into account any particular characteristics of the local environment. The process of managing the performance of managers is defined by the Group, which verifies that it is deployed across the network. This ensures that managers are evaluated and compensated according to known, objective criteria. The Group's HR department has put in place career management processes to foster the emergence of high-potential employees and support staff development in general. Data relating to these Group HR processes are managed in an integrated software package.

Changes in the total payroll are managed by the Group. These are analyzed every year as part of the budget process to ensure they are mitigated. Key indicators such as the attrition rate are monitored regularly by the Group HR department and action plans are implemented in conjunction with the network of HR managers.

## Compliance Program

The Group's active risk management policy is underpinned by a series of values and ethical principles that are shared by all employees. Bureau Veritas is a member of the International Federation of Inspection Agencies (IFIA), renamed the TIC Council in 2019. The Group's Code of Ethics was drawn up in 2003 and is applicable to all of its employees. In compliance with TIC Council requirements, the Code of Ethics sets forth the ethical values, principles and rules on which Bureau Veritas seeks to base its development and growth and build relationships of trust with its clients, staff, and business partners. The Code of Ethics is updated on a regular basis, mostly recently in 2020. This Code received an award at the 2021 and 2022 *Grands Prix de la Transparence* ceremonies, in the category of Ethics Charters published by SBF 120 and non-SBF 120 issuers.

Bureau Veritas supported the rollout of its Code of Ethics by putting in place the global compliance program, a special ethics-focused program ("Compliance Program"), of which it is an integral component. The Compliance Program aims to (i) fight against corruption, (ii) monitor the integrity of Bureau Veritas' services and its financial and accounting information, (iii) prevent conflicts of interest, (iv) comply with applicable antitrust and market regulations, (v) apply international economic sanctions and regulations on export controls, (vi) ensure confidential and personal data protection, and (vii) protect employee health and safety and promote fair employment principles. The Group ensures that the program is effectively deployed and monitored, and it is regularly adapted to take into account important legislative and regulatory changes.

The Compliance Program includes:

- a Code of Ethics (available in 25 languages);
- a manual of internal procedures;
- a compulsory training program for all staff worldwide (available primarily as an e-learning module in 14 languages and supplemented by local training and awareness-raising initiatives);
- a whistleblowing procedure for internal and external ethics violations;
- a corruption risk mapping process;
- internal and/or external assessment procedures for third parties coupled with an information database and sample contracts;
- accounting control procedures with the allocation of specific accounts for regulated transactions (gifts, donations, etc.), and regular control and assessment processes, which are mainly conducted via an annual self-assessment campaign and rounded out by internal and external audits.

The Compliance Program's e-learning module is rolled out by a dedicated network of Human Resources managers. A regular reporting system has been put in place under the supervision of this network, which monitors the number of employees trained in the Compliance Program each quarter. The aim is to cover 100% of new employees worldwide.

The Group's Ethics Committee comprises the Chief Executive Officer, the Deputy Chief Executive Officer, the Chief Financial Officer, the Group Chief Human Resources Officer and the Group Compliance Officer. The Committee oversees the implementation of the Compliance Program and deals with all of the Group's ethics issues.

The Group Compliance Officer uses a network of Compliance Officers who act as intermediaries in the Group's Operating Groups.

In the operating entities, each unit manager is responsible for the application of the Compliance Program by the staff under his/her authority, and is supervised and managed by the heads of the Operating Groups to which he/she reports. For this purpose, it is the responsibility of each Operating Group head to provide a copy of the Code of Ethics to his/her staff, to oversee their training and inform them of their duties in simple, practical and concrete terms, and to leave them with no doubt that any failure to comply with the Compliance Program will constitute a serious breach of their professional obligations.

Any alleged breach of the Code of Ethics must be brought to the attention of the Group Compliance Officer. An internal or external investigation is carried out and, depending on the findings, penalties may be imposed, including the possible dismissal of the employees in question and legal proceedings.

Internal and external audits are conducted each year on the application of and compliance with the principles of the Code of Ethics, and a report is issued by an independent audit firm and sent to the TIC Council's Compliance Committee. It is also presented to the Company's Audit & Risk Committee.

A detailed description of the Compliance Program appears in section 2.5.2 – Ethics, of this Universal Registration Document. These measures are designed to prevent any actions that are incompatible with the Group's ethical principles. Although it endeavors to be vigilant in this regard, no guarantee can be given that these measures are, or have been, complied with in all places and circumstances.

### Sustainability

Sustainability risks are managed through a process set by the Group's Risk department. The general principles, organization and framework for managing these risks are detailed in section 2.4 – Sustainability risks and opportunities, of this Universal Registration Document.

## 4.2.4 CHANGES IN INTERNAL CONTROL AND RISK MANAGEMENT PROCEDURES

In the next few years, the Group will aim for better coordination between different stakeholders, covering internal audits, external financial audits, internal quality audits, health and safety audits, audits by accreditation authorities, compliance audits and technical audits.

In terms of risk management, the Group will continue its efforts to regularly adapt the risk map methodology in line with changes in the Group's environment, businesses and organization.

# 4.3 INSURANCE

In an insurance market under pressure, with the climate, political and inflationary crisis amplifying market adjustments, particularly in terms of exclusions, limits and rate increases, Bureau Veritas succeeded in renewing all of its insurance policies.



## 4.3.1 GROUP POLICY ON INSURANCE

The Group's policy is to take out insurance policies that cover all its subsidiaries throughout the world. Insurance programs are centralized in order to achieve an appropriate match between the risks transferred and the coverage purchased, thereby maximizing economies of scale while taking into account the specific characteristics of the Group's businesses and contractual or legal constraints.

The optimization of coverage and risk transfer costs is also based on the results of the risk map, as well as on the guarantees and capacity available on the insurance market.

To this end, the Group has taken out various global and centralized insurance policies placed via specialized insurance brokers with leading insurers such as Allianz Global Corporate & Specialty (AGCS), MSIG Insurance Europe AG, Chubb, QBE, AIG, MSAmlin, Zurich, RSA and Berkshire. All insurers selected by the Group have a minimum S&P rating of A-.

The following presentation gives a summary of the Group's main insurance policies but does not describe the restrictions, exclusions and limits applicable thereto. Policies are negotiated for periods ranging from one to three years.

## 4.3.2 GROUP INSURANCE PROGRAMS

The main centralized programs are as follows:

- the Civil Liability policy, which covers professional civil liability for all the Group's activities, with the exception of Construction in France and Aeronautics (these are covered by specific insurance programs). This Civil Liability policy is complementary to the Civil Liability policies taken out in the countries in which Bureau Veritas operates, but with different limits and/or conditions. As in the past, this policy involves the traditional insurance and reinsurance market, as well as the Group's reinsurance subsidiary;
- the "Directors and Officers" (D&O) policy, which covers Corporate Officer civil liability at all Group subsidiaries;
- the Civil Liability Aeronautics policy, which mainly covers aircraft inspection activities leading to certificates of airworthiness;
- the cybersecurity policy, which mainly covers data breaches and cyber incidents, including those resulting from malicious acts;
- the Property Damage and Business Interruption policy, which covers the offices and laboratories rented, owned or otherwise made available to the Group. As in the past, this policy involves the traditional insurance and reinsurance market, as well as the Group's reinsurance subsidiary;

- the policy that covers employees on professional missions, including a medical assistance and personal accident program.

Specific or local coverage is obtained to comply with regulations in different countries and meet the individual requirements of certain activities. Examples of this are the insurance policies for vehicle fleets and workers' compensation or for the Construction business in France, which are taken out in compliance with local regulatory practices and mandatory guarantees.

## 4.3.3 SELF-INSURANCE SYSTEM

The Group's self-insurance system is centered on its reinsurance subsidiary, the inclusion of which in these Group insurance policies has enabled the Group to better manage risks and disputes and optimize coverage and the cost of transferring the risks insured. It provides:

- first-line coverage for the Civil Liability policy for all of the Group's businesses, where this is permitted by applicable legislation and regulations. The maximum annual amount payable by the reinsurance subsidiary for the Civil Liability policy has been stable for several years, at €9 million per annum, with a limit of €3 million per claim. These amounts apply worldwide except for the United States, where there is an annual per-claim limit of USD 10 million for Errors & Omissions coverage and of USD 2 million for General Liability coverage;
- as part of the Group's Property Damage and Business Interruption policy, per-claim coverage of €2 million, up to a maximum amount of €4 million per annum.

The Group believes that the coverage and limits of these central and local policies are broadly similar or even more extensive than those subscribed by global companies of a similar scale operating in the same sector.

The Group intends to continue its policy of taking out global insurance policies where possible, increasing coverage where necessary and reducing costs through self-insurance policies as appropriate. It will ensure that its main accidental or operational risks are transferred to the insurance market where such a market exists, and that such transfer can be justified financially. The insurance program described above will be adjusted in accordance with ongoing risk assessments (based mainly on risk maps), market conditions and available insurance capacity.

# 4.4 LEGAL, ADMINISTRATIVE AND ARBITRATION PROCEDURES AND INVESTIGATIONS

In the normal course of business, the Group is involved with respect to its activities in a large number of legal proceedings seeking to establish its professional liability. Although the Group pays careful attention to managing risks and the quality of the services it provides, some services may result in adverse financial penalties.

Provisions may be set aside to cover expenses resulting from such proceedings. The amount recognized as a provision is the best estimate of the expenditure required to settle the present obligation at the end of the reporting period. The costs the Group ultimately incurs may exceed the amounts set aside to such provisions due to a variety of factors such as the uncertain nature of the outcome of the disputes.

At the date of this Universal Registration Document, the Group is involved in the main proceedings described below:

## 4.4.1 DISPUTE CONCERNING THE CONSTRUCTION OF A HOTEL AND COMMERCIAL COMPLEX IN TURKEY

Bureau Veritas Gozetim Hizmetleri Ltd. Sirketi (BVG) and the Turkish company Aymet are parties to a dispute before the Commercial Court of Ankara relating to the construction of a hotel and business complex in respect of which the parties entered into a contract in 2003. In 2004, construction on the project was halted following the withdrawal of funding for the project by the Aareal Bank. Aymet filed an action against BVG in 2008, claiming damages for alleged failures in the performance of its project inspection and supervision duties and BVG's responsibility in the withdrawal of the project's financing.

Regarding the merits of the case, the documents presented to the court support the Company's position that Aymet's claims are without firm legal or contractual foundation. In a parallel proceeding between Aymet and Bank Aareal, the Turkish courts have now definitively ruled that Aareal Bank legitimately terminated its financing on account of a breach of contract by Aymet.

Under local law, Aymet's claim is capped at 87.4 million Turkish lira, plus interest charged at the statutory rate and court costs.

On December 5, 2018, the Court upheld Aymet's application in its entirety and ordered BVG to pay the amounts claimed. As BVG contests both the principle of its liability and the loss assessment, it has appealed this decision, filing a bank guarantee in order to oppose any attempt at enforcing it.

On May 26, 2022, the Pre-Appeal Court reversed that decision and remanded the case to the trial judge for further consideration. As a result of this favorable decision, the bank guarantee deposited by BVG was released as of June 14, 2022.

At the current stage of proceedings, the outcome of this dispute is uncertain, even though BVG's legal counsel are optimistic. Based on the provisions set aside by the Group, and on the information currently available, and after considering the opinion of its legal counsel, the Company considers that this claim will not have a material adverse impact on the Group's consolidated financial statements.

## 4.4.2 TAX CONTINGENCIES AND POSITIONS

Bureau Veritas SA and certain Group subsidiaries are currently being audited or have received proposed tax adjustments that have led to discussions with the competent local authorities. Talks are currently at the litigation or pre-litigation stage.

Given the current status of the pending matters and based on the information available to date, the Group believes that the tax contingencies and positions reported in its consolidated financial statements in respect of these risks, audits and adjustments are appropriate.

There are no other legal, administrative, government and arbitration procedures or investigations (including any proceedings of which the Company is aware that are pending or with which the Group is threatened) that could have, or have had over the last six months, a material impact on the Group's financial position or profitability. The provisions for claims and disputes booked by the Group are presented in section 6.6 – Notes to the consolidated financial statements, Note 27 of this Universal Registration Document. This note continues to be relevant regarding the disputes relating to taxes other than income taxes (IAS 12).