INTERNAL AUDIT

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Internal Audit and ESG criteria

The Institute of Internal Auditors

Instituto de Auditores Internos de España

THE INSTITUTE OF INTERNAL AUTIDORS OF SPAIN is a professional body founded in 1983, and its mission is to contribute to the success of businesses by promoting Internal Audits as a key aspect of good governance. In Spain it counts with around 3,500 members, internal auditors in the leading companies and institutions in all sectors of the country's economy.

LA FÁBRICA DE PENSAMIENTO is the think tank of the Institute of Internal Auditors of Spain for corporate governance, risk management, and Internal Audits, in which more than 150 members and professional experts participate.


INTERNAL AUDITS


GOOD PRACTICES IN RISK MANAGEMENT


SECTOR OBSERVATORY


GOOD GOVERNANCE PRACTICES

The laboratory operates with an essentially practical approach to the production of documents based on good practices that help to improve good governance and risk management systems in Spanish-speaking organizations. Besides creating content, it also promotes the exchange of information among its members.

FIND ALL THE DOCUMENTS OF THE FÁBRICA AT www.auditoresinternos.es

INTERNAL AUDIT

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Internal Audit and ESG criteria

November 2021 - Translation February 2022

MEMBERS OF THE TECHNICAL COMMITTEE

COORDINATION:

Gabriel Pérez Urrutia, MEMBER OF THE ICJCE, CIA, COSO-IC. IBERDROLA.

Sergio Adán Plaza. REPSOL.
Carmen Alcalá Cristino, FRM. CAIXABANK.
Estefanía Arribas Arroyo, COSO-IC, COSO-ERM. GLOBALVIA.
Montserrat Artigas Abelló. SAREB.
Pablo Bernabeu de Lope, ROAC, REC, COSO, CESCOM, IFCA. PRODIEL.
José Enrique Díaz Menaya, CÍA, CRM, COSO, ROAC. INDEPENDENT.
José Ignacio Díez Arocena, CIA, CISA, CFE, CESCOM, COSO-IC. INDRA.
Javier García Braojos. EBRO FOODS.
Sara González Gómez, CESGA, CIA, CRMA. ING.
José Antonio Jiménez Corpa. DELOITTE.
Marta Luaces Calpe, CIA. AXA.
Iciar Marquinez Beñarán. VELATIA.
Juan Luis Martín Ferrera. MANAGEMENT SOLUTIONS.
Mireya Martínez de San Martín, CIA; COSO-IC. REDEXIS.
Yolanda Pérez Pérez, CIA, CRMA, COSO-ERM, ROAC, EFFAS. KPMG.
Rodrigo Salvador Alonso. BBVA.
Elena Tejero Hernández, CIA, ROAC. FERROVIAL.
Ángela Valcarce Ruiz. CAPITAL ENERGY.
Pablo Valerio Sardón. MAZARS.

The Institute of Internal Auditors

Instituto de Auditores Internos de España

Companies' increasing awareness of their social responsibilities –also called sustainability– in relation to their performance in managing the environmental, social and governance (ESG) factors, requires them to include these aspects in their business models and investment strategies and to assess their impact on profitability, liquidity, reputation and relationship with wider society, among other factors.

Just as society demands greater transparency from businesses, internal auditors must seek to reassure our stakeholders by incorporating these specific ESG criteria into our risk analyses and acquiring the necessary skills to enhance our capacity in this area.

This document has been split into two parts. The first will develop the definitions and identify the fundamental aspects of each of the E, S and G factors in terms of strategy and governance, risk management and establishing the reporting framework. The second part will focus on the process of Internal Audit work on ESG criteria by considering the approaches, tests and indicators that can be used as reference.

Our proposed model will be very useful as a guide to managing the supervision of the ESG aspects, although each Internal Audit team will have to adapt, develop, and complete it with reference to the nature, circumstances and context of their organization.

In short, this is an essential publication prepared by a Technical Committee of experts who have put their experience and knowledge at the service of the whole profession and we would like to express our gratitude for their work and dedication.

Institute of Internal Auditors of Spain

Contents

Executive summary

The ESG aspects can condition business strategy and entail significant risks, but they can also provide new opportunities.

In recent years, there has been an increase in awareness of environmental, social and governance (ESG) issues among companies and their stakeholders. These aspects have become the center of attention of many management boards and regulators around the world, and they now, in many cases condition business strategy. Although ESG criteria come accompanied by significant risks, they also represent a gateway for new opportunities.

It is in this context that the role of Internal Auditing gains greater importance for adding value to the company, both in its role as provider of assurance as well as in its role as trusted advisor.

It is important for Internal Auditing to consider a series of key aspects that, not only guide its fieldwork, but also contribute to adequate planning. The mentioned aspects are:

Strategic management and supervision by the company's governance bodies and senior management are key actors to ensure the proper handling of ESG issues and their integration into the corporate strategy, in so much as the need for these to be aligned with the vision and purpose of the company, and the expectations of its stakeholders. It is therefore fundamental to count on the commitment and leadership of the Board of Directors and the support of its delegate committees who are in charge of handling this issue (Audit Committee and Sustainability Committee, where present) through defined responsibilities and mechanisms, such as an ESG policy or the integration of targets related to its remuneration model.

Identification, assessment and management of ESG risks and opportunities, which are based on a suitable analysis of materiality and allow identification of critical issues, risks and indicators.

Internal Control System for Non-Financial Information (ICNFR), which is essential to ensure the coverage of risks associated with ESG factors. Entity level controls and controls specifically directed towards handling ESG related risks are necessary, as well as training that focuses on these subjects. There also needs to be a policy for non-financial information and adequate reporting and communication resources.

An ESG reporting framework. As well as a formal and documented ESG reporting process, organizations must also assign specific roles and responsibilities where technical expertise is required irrespective of traditional reporting lines and organizational hierarchy. A review is essential at this point to ensure that the information is suitable, complete and correct, which means that there must be internal and external validations.

It is also fundamental that Internal Audits identify the specific risks for the material questions within each one of the three pillars of ESG, and establish a specific approach towards work. This document is intended to serve as a manual to guide internal auditors in this task. However, it does not claim to provide full coverage for each and every one of the risks that may arise. The importance of these will depend on factors such as the culture, analysis of materiality, the business model, the industry, the business context, etc.

PILLARS ON WHICH ESG APECTS ARE BASED

ENVIRONMENT
Environmental - E

It is fundamental to take into account aspects such as emissions, contamination, management of material and natural resources, biodiversity, ecosystem services, circular economy and waste management, as well as climate change.

SOCIAL
Social - S

These include respect for Human Rights, diversity, equality, contribution to society, hiring and management of human resources, safety, the health and wellbeing of employees and training.

GOVERNANCE
Governance - G

The structure, governance and responsibilities of the governing bodies of companies are important here, along with the expectations of stakeholders, strategies, risk management and investments, the remuneration system, the internal regulatory framework information systems, transparency, supervision and reporting, ethics and integrity, measures to tackle corruption and bribery and tax affairs.

Specific types of risks of different categories have been identified for each of these pillars: strategic, compliance, financial and operational; approaches are suggested to internal auditors about how to address those, along with possible indicators.

This guide can be used by internal auditors of organizations with more a mature ESG culture and those that are just taking their first steps.

In essence, for an Internal Audit to provide value for companies and to fulfill its role of compliance with ESG factors, it has to consider both general and specific aspects of each of these pillars.

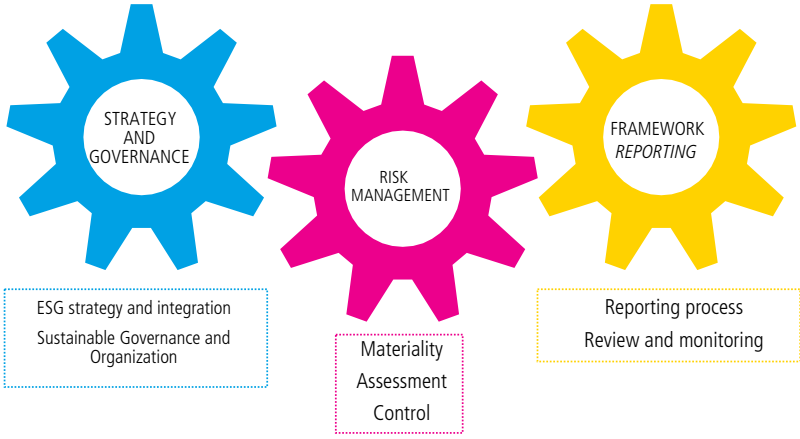
Chapter One: Fundamental features of the ESG criteria

This chapter will cover, first of all, the fundamental information that will allow Internal Auditors to put the specific characteristics and situations of each company into the right context, and how they might focus their work on the ESG aspects.

Performing benchmarking exercises against accepted standards and best practices is a perfectly valid approach for Internal Auditors.

Starting from the basic definitions of what is meant by ESG criteria, we will move forward to an overview of general aspects of interest grouped into three main sections.

- Strategy and governance.
- Risk management and opportunities
- Reporting framework.



Preliminary considerations about ESG factors. SOURCE: author (2021)

DEFINITION AND IMPACT FOR COMPANIES

Definitions

E - ***Environment.*** Identifies and assesses the relation between business practices and the environment. Climate change has become the most urging factor for most companies, although the focus is on different priorities. Some key indicators are emission of greenhouse gases, the deployment of natural resources, the loss of biodiversity in ecosystems, deforestation or the transition to a circular economy.[1]

1. EU Technical Expert Group on Sustainable Finance. *Taxonomy: Final report of the Technical Expert Group on Sustainable Finance,*

· S - *Social.* This gathers the effects generated on human resources and the other stakeholders of companies: respect for Human Rights, investment in human capital, working practices, occupational health and safety, supply chain management, training, and relations with local communities, among others.

· G - *Governance*. This includes indicators related to the internal structures of companies, policies and decision-making in the processes, and how these factors affect the different stakeholders; the structures of management and leadership, working relations, the policies established by the principles of independence, transparency and accountability, the promotion of good practices and the fight against bribery, fraud and money laundering ...

ENVIRONMENT
Environmental - E

The environmental impact of the business, such as pollution, the use of resources, or the adaptation to, and mitigation of climate change.

The main objectives in the environmental sphere (in accordance with the Taxonomy of the EU) are:

· **Climate Change:**
  - Mitigation of climate change.
  - Adaptation to climate change.
· **Environmental Challenges:**
  - Sustainable use and protection of water and other marine resources.
  - Transition towards a circular economy
  - Prevention and monitoring of pollution.
  - Protection and restoration of biodiversity and ecosystems.

SOCIAL
Social - S

Impact on society, the community, the economy and stakeholders in general.

Some of the main objectives in the social area (in accordance with the *Global Reporting Initiative* (GRI) international standard of reference, are:

· Eradication of social inequalities.
· Social inclusion.
· Improved working relations.
· Investment in human capital.
· Protection of local and indigenous communities.
· Preservation of cultural heritage.

GOVERNANCE
Governance - G

The inclusion of good governance practices in institutions, in recognition of its fundamental role among shareholders, clients, employees and all the parties involved in business decisions.

Some of the main objectives in the good governance area (in accordance with the Global Reporting Initiative (GRI) international standard of reference, are:

· Development of solid internal structures for management, leadership and relations.
· Encouragement of independent decision making.
· Support for transparency and accountability.
· Promotion of good practices.
· Fight against corruption and fraud.

Framework of ESG principles SOURCE: Management Solutions (2020)

General regulatory framework

There has been an exponential transformation of regulations in relation to ESG in recent decades.

Beginning with the Montreal protocol of 1987, and moving on to the indicators of the World Economic Forum of Davos in 2020, regulation has resulted in significant milestones over the last 30 years: the Kyoto Protocol;

the *ISO 2600 Standard - Guidance on Social Responsibility* (2010); the OECD Directives (2011); the United Nations Guiding Principles for Businesses and Human Rights (2011); the Performance Standards of the *International Finance Corporation* (2011); the Sustainable Development Goals (SDG) or Paris Agreement (both from 2015) and, more recently, the OECD *Due Diligence Guidance for Responsible Business Conduct* (2018) are the most outstanding examples of this topic.

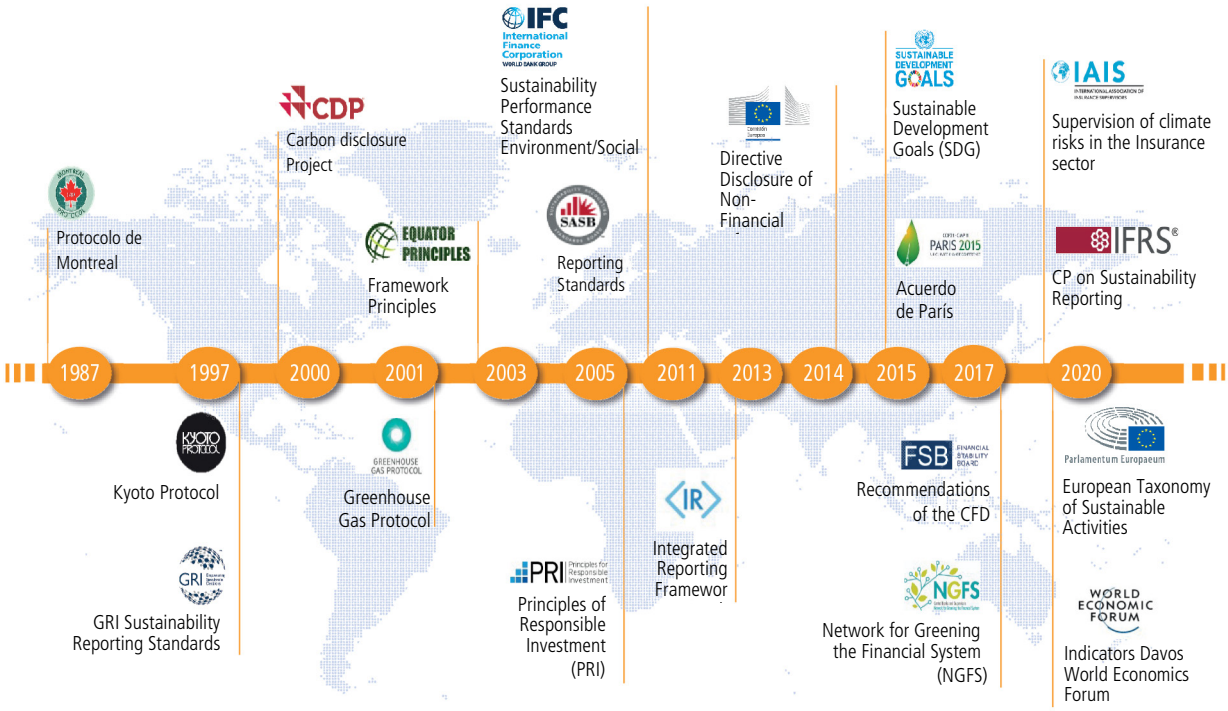


Figure 3: Growth of regulations on ESG matters. SOURCE: Management Solutions (2021)

The type of company involved will determine the scope of the internal auditor's work, not only because of the specific characteristics of the sector or company, but also because of the different regulatory demands that may apply. For example, Law 11/2018 requires the submission (and approval by the AGM) of a Statement of Non-Financial Information by companies with more than 500[2] employees, and they are to be considered as large companies under the terms of Directive 2013/34/EU of the European Parliament and Council. This means that they meet two of the following three requirements in two successive years:

2. It is lowered to 250 employees three years after the law comes into effect, which will therefore apply to the Statement of Non-Financial Information for 2021.

Total assets worth more than 20 million euro, annual net turnover of more than 40 million euro, and an average workforce of more than 250 employees. This includes companies of public interest with consolidated accounts where the business groups are in excess of the above and, therefore, companies that issue listed securities.

In addition, they will have to consider the specific nature of the sector in which the company operates, focusing the attention on those which are subject to specific legal requirements. For example, on February 18, 2021, the CNMV (Comisión Nacional del Mercado de Valores) published a *Note on the forthcoming application of Regulation 2019/2088 on the reporting of information about sustainability in the financial sector.*

This document, directed to fund and asset management companies, venture capital companies and financial advisors, sets out the obligations for disclosure of sustainability information, in accordance with the content of EU Regulation 2019/2088, of the European Parliament and Council, of November 27, 2019, on this subject.

Internal Auditors must therefore - when planning work related with ESG risks - consider very carefully the sector where the company operates and the legal obligations which it is subject to.

Sustainability governance plays a crucial role, because the setting of objectives for ESG matters will condition the corporate social responsibility strategy that the company intends to follow.

STRATEGY AND GOVERNANCE

The importance of governance and defining strategy in ESG areas.

When addressing ESG matters, sustainability governance plays a very significant role, because the objectives defined for these areas will condition the corporate social responsibility strategy that the company wants to apply.

There are two main components: strategic control and supervision. Senior management is responsible for the strategic leadership in the implementation of objectives in ESG matters. It defines the actions to be taken and appoints the people in charge of carrying them out. The Board of Directors is responsible for the supervision.

The CNMV recommendations for listed companies, the Law on Corporations and Law 11/2018 on non-financial information and diversity are all in alignment: boards have to guide, oversee and monitor their companies' approach to sustainability.

Moreover, the current Code of Good Governance of Listed Companies of Spain (hereinafter CBGSC) explicitly assigns to the Audit Committee the task of supervising and evaluating the process of preparation and integrity of the financial and non-financial information, as well as the responsibility for supervising the systems for controlling and managing financial and non-financial risks, which include operational, technological, legal, social, environmental, political,

reputational and bribery risks. The latter are mentioned explicitly in the identification of the control and risk management policy, along with assurance provided by Internal Auditors. This is intended to ensure coherence of the financial and non-financial aspects, both with regard to their management and risk assessment, and with the annual reporting of information. This is also aligned with the direction of regulation in Europe, as we can see in the European Union's current plan to revise its directive on non-financial information[3].

Sustainability must be included in the company's process of strategic planning to estimate its relevance for achieving its purpose and getting closer to its vision.

Integration with corporate strategy: vision and purpose of management

Given the potential impact of ESG risks, it is inevitable that they be incorporated into the business strategy and processes, in order to ensure the long-term financial resilience of the company. By guiding the business in a more responsible direction that is consistent with the expected social and environmental transition, it is more likely that the companies plan ahead and ensure they are better prepared to prevent and mitigate the long-term negative impacts of ESG risks and to take advantage of any associated opportunities that may arise.

Sustainability must also be included in the company's process of strategic planning to estimate the extent to which it is relevant for achieving its purpose and getting closer to its vision.

Sustainability or Corporate Social Responsibility has often been linked with the long-term competitiveness of companies. Companies that handle these aspects in accordance with their main activity and purpose will achieve better outcomes. Not only will they identify new opportunities in the market and create innovative products, improve their interaction with their stakeholders and converge in the medium term towards more inclusive and sustainable business models, but they will also become more competitive and improve their reputation.

The role of regulators is equally significant. As an example, the Sustainable Finance Disclosure Regulation (SFDR) - in force since March 10, 2021 - which requires all financial entities that sell products in the European Union to be more transparent on the sustainability of their investment products.

Expectations of the stakeholders

The most common internal and external stakeholders are: shareholders, employees, investors, financial institutions, suppliers, clients, partners, competitors, authorities, regulators, public bodies, social groups, local communities and *proxy advisors*.

It is absolutely vital to manage these relations when a company is developing its sustainability strategy. The ability to respond to all their needs and expectations and remunerate them according to the value attributed to the company is the starting

3. Under review during the period when this document was being prepared.

point to ensure that the ESG aspects are being managed competently, to achieve sustainable profits in the long run. It means that the company is better adapted to its situation, avoids risks and reduces uncertainty, and is capable of grasping opportunities arising from returning value to the society in which it operates.

In sum, it should be underlined that ESG is an issue that cuts across areas and needs to permeate the whole company, not only the units which are traditionally client/investor facing, but also others that are commonly engaged in supervision, such as Internal Control, Risk, Compliance and Internal Audit.

Administration and sustainability committees

The most senior governance body is involved in the approval of policies and objectives related with ESG matters and is responsible for encouraging the development of their companies through the following **key initiatives**, among others (according to the recommendations of the *European Banking Authority*, the EBA):

- Integrate ESG matters into the corporate culture.
- Consider ESG risks in the risk committees or create specific committees.
- Implement a training program for specific ESG knowledge and skills within the company, and incorporate board members with knowledge and expertise on the subject.
- Define and supervise a clear structure for assuming responsibilities in this area. Include ESG risks within the risk appetite framework and in risk models.
- Guarantee that Internal Audits include ESG risks in their reviews.
- Consider a remuneration policy that ties variable salary components to the achievement of ESG objectives.

Provided that ESG aspects must be incorporated into the company strategy and are a source of value creation, these should be supervised and managed from the main organs of governance and direction of the company. For example, the CBGSC indicates, in its recommendation number 53, that among its other responsibilities, the Board should supervise questions related with ESG matters.

A distinction is also needed between the functions of the Audit Committee - based on assurance - and the functions of the delegate committee responsible for sustainability, which guides the strategy.

Policy on ESG matters and the incorporation of ESG goals into the remuneration model

A defined sustainability or ESG policy in the company must include:

- The principles, commitments, objectives and strategy related to the company's relation with stakeholders.
- Systems for monitoring compliance with policies, the associated risks and their management.
- The risk supervision mechanisms for ESG matters.

The concept of ESG must permeate the whole company, including units which have traditionally been engaged in supervision, such as Internal Control, Risk, Compliance and Internal Auditing.

- The communication channels, participation and dialogue with stakeholders and responsible communication (*reporting)*.

It is important that there is a solid mechanism of incentives to nurture an appropriate risk culture. It is important that employee conduct is aligned with the organization´s outlook on ESG risks.

IDENTIFICATION, EVALUATION AND MANAGEMENT OF RISKS AND OPPORTUNITIES INESG

The next step is establishing the priority or materiality of the significant issues that have been identified for the company, which means that it is crucial to determine which risks are associated or derived from those issues, the impact on the company and alignment with the overall strategy.

It is fundamental to consider the impact of exposure to traditional risks across all areas - not just in terms of its reputation - and to consider the temporal horizon as a relevant dimension. Some factors can be dealt with in the short and medium term, especially the ones determined by regulatory changes. Others may be extended over the course of several years, with the related strategies[4].

In ESG terms, materiality can be defined as the threshold from which certain social, ethical and environmental topics can be considered significant for the company and its stakeholders.

Materiality analysis: concept and application to define ESG risks, methodologies and relations to strategy

In terms of ESG, materiality could be defined as the threshold beyond which certain Social, ethical or environmental topics are considered relevant and meaningful for the company and its stakeholders. ESG issues should not be viewed only under the perspective of their importance for the internal affairs of the company, but also for the importance they have for external stakeholders. This represents an incisive difference from the traditional view of financial materiality; indeed, the concept of "double materiality[5]" for ESG issues is starting to be used.

According to the *Sustainability Reporting Standards* of the *Global Reporting Initiative* (GRI): "Companies should focus in their reporting on the issues that: a) have significant negative financial, environmental and social impacts on their business and/or their objectives, and b) have a significant influence on the evaluations and decisions of their stakeholders".

One common standard when defining the materiality of ESG issues is to draw a materiality matrix, which is intended to show which ESG issues are a priority for the company, taking internal and external impacts

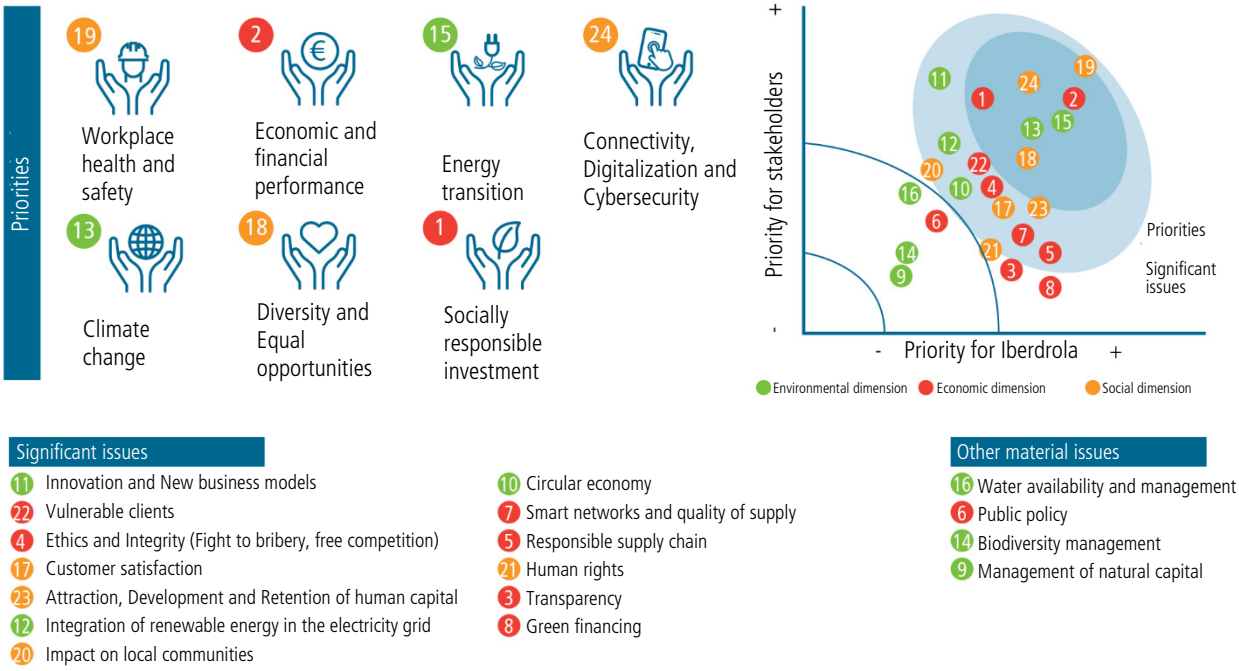
4. Central European Bank. *Guide on climate-related and environmental risks,* 2020.

5. European Commission. *Interim study on the development of tools and mechanisms for the integration of environmental, social and governance (ESG) factors into the EU banking prudential framework and into banks' business strategies and investment policies,* 2020.

into account, and which need to be updated on a regular basis.

The result of this analysis of materiality indicates what is "material" for the company and what guides and reinforces the sustainability strategy and, therefore, its overall strategy[6].

Materiality analysis is a tool that helps a company understanding which ESG factors are the most significant, establishing a new dialog with management, and raising new questions. The underlying ESG risks will then be defined from these factors, allowing the creation of ESG risk maps.



Example of a materiality matrix. SOURCE: Iberdrola. *Statement of non-financial information - Sustainability report* (2020)

Risk identification and assessment

Companies can implement different approaches to identify the ESG risks: analysis of major trends, materiality assessments and company SWOT analysis. These risks, in turn, should be associated with the strategic objectives.

In order to use these tools, it is advisable to collaborate with the risk management area along with specialists in sustainability. This will ensure that the list of risks is drawn up correctly and that it will be consistent with the materiality analysis carried out.

6. VIVES, A. *Materialidad: 12 principios básicos y una metodología para la estrategia de RSE.* Ágora. February 2015.

The following mechanisms should be considered to ensure correct implementation:

- The Board of Directors or Steering Committee must set specific and measurable non-financial targets that are aligned with the business strategy.
- Identification of the non-financial questions that are significant for the company and its stakeholders through a process of materiality assessment.
- Establishment of a risk management framework that enables companies to identify and manage their non-financial risks in the short, medium and long term as an essential part of their risk management process.
- Regular assessment of the risk of non-financial information being unreliable (by accident or design) and that this assessment should be part of the risk reports to be presented to the Board.
- Implementation of a process to identify internal and external changes that may affect non-financial information and the way to deal with these changes.

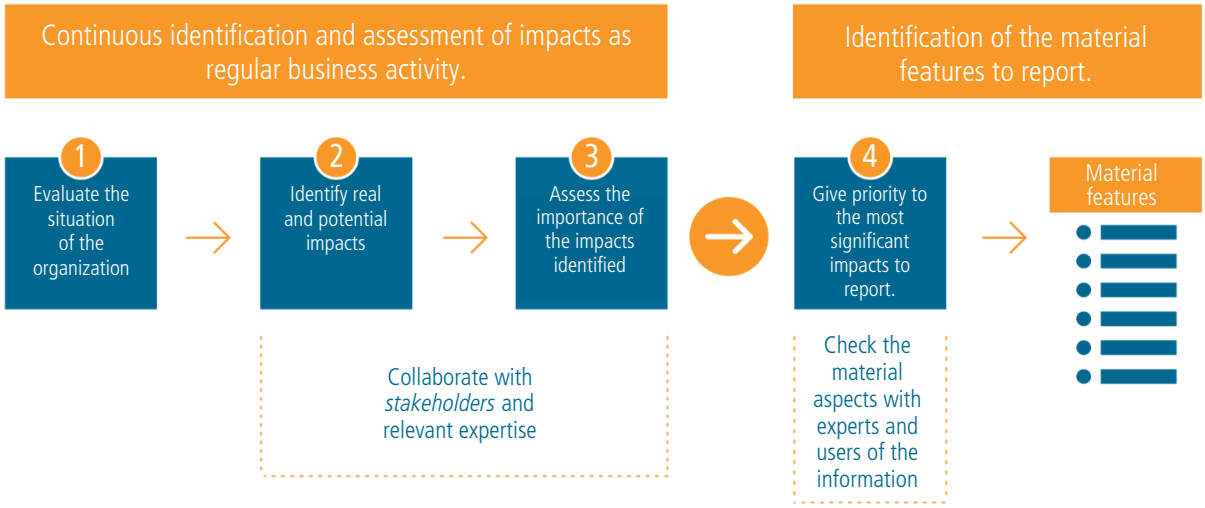


Figure 6: Process of identifying material issues. SOURCE: GRI[7] (2020)

The process of assessment starts after the risks are identified. The method will depend on the maturity of the organization´s risk functions and the nature of the ESG risk to be addressed.

For example:

- Many organizations require an assessment of the risks and opportunities associated with climate change in order to assess how resilient

7. Global Sustainability Standards Board. *GRI Universal Standards: GRI 101, GRI 102, and GRI 103 – Exposure draft.* Amsterdam: GSSB, 2020.

the company's strategy is in climate scenarios.

- In view of the criteria for eligibility for Next Gen funding, there is a growing demand for methods for assessing social impact risk, whether for social impact or the positive effects of company operations. The aforementioned methods may combine either quantitative elements (such as the propagation effect) or qualitative elements (such as the effects on vulnerable groups).
- Determining financial impact is not enough to assess certain impacts, such as those affecting the environment. These cases usually involve the use of qualitative scales to account for issues which are significant for the company, *per se*, but which are not properly reflected in financial terms.

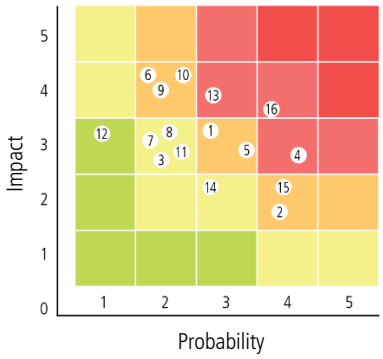
The best practice is to quantify risks through the use of modeling, both of frequency and impact, to enable the subsequent insertion of those risks through correlation matrices.

When assessing risks, the value or losses that each risk could cause is compared with the maximum loss or value that the company is willing to accept (risk appetite). This can be done by considering the company's mission and values, its SWOT and materiality analyses and its strategy. ESG concepts must be embedded in these sections, for these to be correctly registered in our risk matrix.

The comparison between the real and desired values of the losses incurred since the last risk analysis will allow the company to identify its priorities in mitigating risks: higher priority will be given to those where there is a greater disparity between the value obtained and what was anticipated for that specific risk. The mitigation can be achieved by adopting controls that are aligned to the nature and characteristics of the risks. Society itself is setting more demanding thresholds every year for ESG risks, which is forcing companies to continually review their risk appetite or to plan ahead so that they are not left behind.

Usually, for ESG risks there is zero tolerance towards non compliance with governance and social aspects, and more stringent requirements in relation to the environment, either due to regulatory restrictions, the spectrum of which is expanding, or due to the negative effects of reputation or financial impacts (worse conditions for loan financing, for example).

The company's governance bodies and senior management will be kept informed through the reports created from the risk register and the corresponding risk map (heat maps in which the axis of the matrix indicate impact and probability).



The best practice is obtaining a quantification of risks by modeling their frequency and impact, and aggregating it through correlation matrixes.

With the aim of continuously supervising risks and monitoring how they change, there are several examples of Key Risk Indicators (KRIs) for each of the selected risks.

EXAMPLES OF KRIs WITH DIFFERENT METHODOLOGIES (QUANTITATIVE OR QUALITATIVE)

		METHODOLOGY	KRI
 ENVIRONMENT	Climate change	Quantitative	Carbon footprint/carbon emissions
		Quantitative	Annual average temperature/rainfall
	Natural resources	Quantitative	Water balance
		Qualitative/quantitative	Environmental biodiversity
		Quantitative	Raw materials production
	Contamination and waste	Quantitative	Toxic emissions.
		Quantitative	Waste.
 SOCIAL	Human capital	Quantitative	Staff turnover/absenteeism.
		Quantitative	Staff security/incidents.
		Qualitative	Working environment based on employee interviews (scores).
		Quantitative	Non-compliances of international SDG standards (Zero Tolerance)
		Quantitative	Percentage of men/women and salaries - labor gap.
 GOVERNANCE	Governance	Quantitative	Non-compliances in policies (Zero Tolerance)
		Qualitative	Level of supplier concentration complying with policies.
		Quantitative	Score obtained in ESG organisms.
	Ethics	Quantitative	No. of channels for complaints
		Quantitative	Accumulated call center reportings by type
		Qualitative	Employee surveys (score).
		Qualitative	Exterior surveys - image.

Control of Non-Financial Information - ICNFR

Non-financial information is a particularly important disclosure published by companies regarding ESG aspects. It discloses all the data collected in the Non-Financial Information Statement (hereinafter NFIS) in accordance with the requirements of Law 11/2018 of Spain. This is where the concept of Internal Control Systems for Non-Financial Information (ICNFR) is introduced.

ICNFR is one part of the internal control and it is the group of processes that the Board of Administration, the Audit Committee and all the personnel involved in the company carry

out to provide assurance over non-financial information.

In accordance with the COSO integrated framework for internal control (2013) - main international reference for internal control frameworks - the components and main mechanisms that must be designed, implemented and operational to ensure an effective ICNFR are:

· Control environment

This refers the awareness and importance afforded to control and supervision of the non-financial reporting process by senior management. The *tone at the top* will favor an appropriate definition of standards of conduct and policies, and determine the structures, the supervisors and assign supervisory responsibilities

The main mechanisms to ensure that this component has been well designed, implemented and is functioning would be:

- Preparing a policy that defines the responsibilities related to the existence, implementation and supervision of the ICNFR. Here it is important to highlight a recent and highly significant regulatory milestone: the partial modification of the CBGSC in June 2020, which assigns the supervision and assessment of the elaboration process and integrity of non-financial information to the Audit Committee. This result of this means that a system of ICNFR becomes critical to governance.
- Drafting of a manual that describes the ICNFR, similar to that of the Internal Control of Financial Information (ICFR), with the review of organization charts, job descriptions etc. to incorporate the responsibility in the ICNFR. The coordination of the different control functions is essential to guarantee effective and efficient coverage, and the plan to develop or evolve the ICNFR to a level of maturity suited to the specific circumstances and context.
- Review codes of conduct and whistleblowing provisions and documentation to ensure coverage of non-financial information.
- Establish a training program with specific material for the persons involved in the preparation and review of the non-financial information that covers aspects associated with internal control and risk management. The CBGSC reinforces this requirement, making the evaluation of experience and specific knowledge of non-financial risk management as one additional criteria when appointing members to the Audit Committee.

the *tone at the top* will favor an appropriate definition of standards of conduct and policies, and determine the structures and assign supervisory responsibilities

· Risk assessment

This has already been covered when describing materiality and risk management.

· Control activities

These shape the necessary instruments to carry out the most important supervision activities in accordance with the risk assessment. The following mechanisms should be considered to ensure correct implementation:

- Identify and define the processes and implementation of control activities, based on on the analysis of materiality,

identifying the most important risks on which to build the list of indicators and the control model.

- Select and implement IT General Control for systems involved in constructing non-financial information, making sure we are able to confirm our assertions.
- Review ICFR policies and procedures an evaluate need for including specific NFI provisions.
- Use of significant information: identify key, necessary information for the correct definition of control activities. Does materiality analysis and relevant indicators provide relevant information on control activities?

Internal Auditing must supervise the design and effectiveness of the controls included in the scope of the ICNFR audit review.

· Information and communication

Mechanisms must be in place to provide relevant, accurate, timely, effective and precise information on performance of the organization in non-financial matters.

This component is singularly important given the distribution of ownership of ESG risks throughout the organization. (environment, HR, corruption etc.). Correct definition of reporting lines is key to the system of ICNFR being efficient.

Software solutions are often employed to construct the Statement of NFI. It is important to consider the requirements for aggregation and consolidation from different systems.

· Supervision

As previously mentioned, the latest update of the CBGSC clearly attributes the supervision and assessment of the elaboration process and integrity of the non-financial information to the Audit Committee.

The supervision of the design and effectiveness of controls covered by the scope of the ICNFR audit is an important part of the overall process of assurance and supervision that Internal Audit performs for the Audit Committee.

ESG REPORTING FRAMEWORK

Information about a company's performance in relation to ESG matters is an indicator that is increasingly being linked to the creation of value in the long term. This has accelerated the demand for more information from stakeholders.

National and EU regulations, mentioned previously in this document, have established the mandatory nature of incorporating information on ESG matters in the management report for large companies and those considered of public interest.

In general, the frameworks for disclosing ESG information are less mature than those used for financial information. Nonetheless, there are certain frameworks that have become consolidated as references: these include the *Global Reporting Initiative* (GRI), the *Sustainability Accounting Standards* (SASB), the *International Integrated Reporting Council* (IIRC), *Value Reporting Foundation* (from the merger of IIRC and SASB), the Commitments of the United Nations Global Compact (UNGC), the *Carbon Disclosure Project* (CDP), the *Task Force on Climate-related Financial Disclosures* (TCFD) or the *Climate Disclosure Standards Board* (CDSB).

Governance roles and model

ESG *reporting* is a process whose size, location and even definition and recognition as a function within the company depends largely on the type of company, its size, and its maturity.

While the structure, processes and resources employed are important, it is a key common requirement that all NFI should be integrated.

Frameworks for preparing and disclosing ESG reporting do not generally assign responsibility to any one area. Responsibility and roles are cross-functional, but closely aligned to other stakeholder reporting roles.

The roles in the reporting process are:

- Review and maintenance of the reporting framework.
- Data collection.
- Data validation.
- Data consolidation.
- External verification.

Internal Audit provides assurance over the whole process.

To manage the *reporting* function, some companies have chosen to set up a sustainability committee that is usually drawn from operational or reporting functions of the company whose activities are related with ESG aspects. For example the committee may be made up with representatives from HR, Investor Relations, Customer Relations etc.

Whoever fills the ESG reporting role, they must have full access to tools and accurate information.

ESG reporting must integrate all the non-financial information that should be reported, as it is of supreme value for the *stakeholders*

Responsibility for accuracy must be borne by the area that produces it.

The *reporting* process

Like processes for Financial Reporting, NFI reporting must have clear and defined process, with internal controls built in to assure integrity and accuracy.

Reporting ESG aspects must be a clear process with internal controls to ensure integrity and accuracy.

Once the information required for internal and external reporting has been defined, the function responsible for coordinating the process must consider the following factors:

- Calendars.
- Scope.
- Allocation of responsibilities.
- Definition of indicators and reporting manual.
- Tools.
- Training.
- Consolidation.

Review and monitoring

· **Frequency and monitoring of the relevant non-financial indicators**

This section provides a list of the different sources of information from where the non-financial data has been extracted, and its characteristics in terms of integrity, automation and type of reports that can be generated, and the levels of control established, whether automated or validated manually, according to the case.

Once the company has listed this information, requirements of reporting non-financial information must be considered - both in terms of type of indicator and the timing - in order to define, as required, any additional needs that might be relevant.

Compiling non-financial information involves a variable number of indicators that must be selected so that their content is adapted to the demands of each company department and their characteristics, and the frequency in response to the needs.

· **Year on year comparison**

The principles related to defining the quality of the INF must enable the establishment of solid and reasonable evaluations by the company in view of the following:

- Clarity: the information must be presented in a way that is comprehensible and accessible for the stakeholders.
- Accuracy: it must be precise and detailed enough to allow the stakeholders to assess the company's performance.
- Balance: it must report both positive and negative aspects of the company's performance to allow a reasonable non-biased assessment.
- Comparability: the company must choose, compile, and report information that is coherent and comparable.

- Reliability: it must bring together, register, compile, analyze and report the information and processes implemented to prepare the information for review, and this can confirm its quality and materiality.
- Timeliness: reports must be prepared according to a regular schedule to ensure that the information is available on time.

Third-party verification

The requirements for external validation of NFI should be identified. Regulatory Non-financial Statements and/or CSR Reporting must be verified independently under the following standards.

- *International Standard on Assurance Engagement* 3000 (ISAE-3000) of the *International Auditing and Assurance Standard Board* (IAASB).
- The Action *Guide* of the Institute of Certified Auditors of Spain.

Regulatory Non-financial Statements and/or CSR Reporting must be verified independently under the following standards.

Chapter Two: Internal Audit of ESG matters

When planning audits, Internal Audit should consider what ESG aspects need to be covered in the scope of work.

The following pages contain tables suggesting the aspects and potential risks that the internal auditor may consider, and references to the reporting standards.

FUNDAMENTAL ATTRIBUTES FOR INTERNAL AUDITING TO CONSIDER WHEN DOING ESG WORK

The participation of Internal Audit in ESG related work will vary depending on many factors.

Internal Audit should benchmark its own capabilities and resources with those required to execute work, which in itself will depend on the actual nature of the business, the complexity of information, the maturity of ESG reporting roles and the dependence on third parties for information and expertise.

It is important to have a framework for action defining the role that the Third Line will have with regard to ESG aspects.

Factors that might be considered:

- **POSITION OF INTERNAL AUDITING.** There should be a framework that delimits the role of the Third Line in ESG matters, as this will determine the scope of work that Internal Audit Provides to the Audit Committee and Senior Management. This framework must specify the roles that Internal Auditing will cover and how it will carry them out.

  · **Assurance Role**: providing the necessary guarantees over the main concerns of the Audit Committee and senior management in the following situations, for example:

  - Ensuring that ESG aspects are integrated into the company's strategic and investment initiatives.
  - Guaranteeing that executive remuneration is aligned with sustainability-related goals (ESG aspects).
  - Guaranteeing coherent and transparent communication of these aspects to all interested parties
  - Ensuring the effectiveness of the approach to integrate the consideration of ESG aspects in the organizational structure and governance of the company.

  · **Trusted Advisor Role:** develop more of a "consultative" role, adding value to special or critical project or initiatives, such as:

  - Assessing the company's maturity in relation to ESG aspects: when a company is prepared, compliant and is proactive or a leader in its sector, it will be able to provide its senior management and Board of Directors with valuable information.
  - Offering advice on how ESG aspects can affect the demand for the company's products and services. For example: how climate change will affect its operations along its supply chain, and the impact of its strategy on the environment and society.
  - Assisting in building ESG criteria into the organization's risk appetite.
  - Carrying out scenario analysis to assure the viability of strategies and plans.
  - Consider the upside or opportunities of ESG risks. This may facilitate uptake by senior management and the Board.

- **RISK ASSESSMENT AND PRIORITIZATION.** Make sure ESG aspects are contemplated in internal audit´s risk assessment methodology.
- **SKILLS AND NECESSARY CAPABILITIES.** Internal audit needs different skill sets and knowledge for ESG aspects. Internal Audit could consider adding new talent to its teams (engineers, climate experts, social workers, etc.), updating its training and skills programs in response to its needs or even adopting guest auditor programs and the rotation of specialist personnel.
- **ORGANIZATION OF WORK.** Efficient internal audit work may require different approaches. Centralized or decentralized teams, specific ESG projects or incorporation of ESG aspects into other assignments.
- **REPORTING TECHNIQUES.** Consider the best way of reporting the audit of ESG aspects. This may be standalone reporting or integrated reporting.

AUDITING ENVIRONMENTAL ASPECTS

Environmental management
- Different emissions of greenhouse gases and pollution.
- Management of natural resources, biodiversity and ecosystem services.
- Circular economy and waste management.

Climate change
- Governance.
- Risk management process.
- Strategy.
- Objectives.

Environmental risks.
- Environmental analysis.

Climate risk
- Governance.
- Risk management process.
- Strategy.
- *Reporting.*

AUDITING SOCIAL ASPECTS

- Diversity and equality.
- Providing value to society.
- Subsidies.
- Innovation.
- Human resources management.
- Health, safety and wellbeing of employees.
- Training.

AUDITING GOVERNANCE ASPECTS

- Governance and accountability structures.
- Stakeholder expectations.
- Strategy, Risk Management and Investment.
- Remuneration framework.
- Internal regulatory framework and Information systems.
- Transparency, Supervision and Reporting.

Ethics and Integrity.
- Corruption and bribery.
- Tax.

AUDITING ENVIRONMENTAL RISKS

There are international reporting standards such as the recommendations issued by the TCFD and CDP organizations.

The main environmental challenge society is facing at this time is undoubtedly climate change.

Bearing in mind the concern and the urgency with which the issue must be addressed, regulators, supervisors and international institutions have all adopted regulations in this area.

Many organizations are obliged to disclose specific decarbonization targets among the earliest legislative work, along with the requirement to submit annual reports which assess the financial impact of climate change risks on the organization. They must include the risks associated with the transition to a sustainable economy and the measures taken to deal with these risks[8].

There are also several international *reporting* standards to be used as reference, especially those recommended by the TCFD (disclosure of climate risks) and more general ones like the CDP.

It is necessary to distinguish the issue of **climate change**, which is a global phenomenon, from the problem of **air quality**, which is local and affected by the concentration of pollutants caused by combustion processes in the local area. This is determined by a company's energy mix, size and density of populations, weather etc.

Due to the significance of these risks, the assessments made by Internal Audit must consider greenhouse gases and pollution emissions separately.

Another important chapter is the **protection of natural resources and biodiversity**. Organizations must have management systems that enable them to implement specific actions to prevent and reduce the impact of their activities. Responsible management will allow organizations to mitigate risks, from the most basic, such as small fines, to more significant ones that may have an impact on the organization's reputation and business operations, such as the loss of operating licenses or the impossibility of resourcing finance.

Finally, **circular economy** offers a framework for solutions in economic development, addressing the deeper causes of the global challenges mentioned previously (climate change, loss of biodiversity, increased generation of waste and pollution, etc.) as well as revealing major growth opportunities.

8. For example, Law 7/2021 on Climate Change and Energy Transition, in force since May 2021.

ENVIRONMENTAL

Distinguishing between greenhouse gases and pollution emissions

RISKS	AUDIT APPROACH	INDICATORS
Absence of a long-term strategy aligned with the company business.	• Verify the existence of an approved strategy communicated to senior management, which includes the scope of the objectives, the mitigation strategy and the timeframe for achieving these objectives.	--
Absence of a specific deployment plan that is integrated in the activity.	• Verify that the strategy is included in the road map and in the company's action plans and that the objectives set are specific and measurable. • Confirm that there are intermediate targets that enable any deviations to be detected.	--
Inadequate measurement that impedes measurement of performance.	Assure periodic performance reviews of emissions reduction plans. Verify indicators exist for emissions and verify the exactness of calculations.	KPIs for fuel consumption (e.g, kilometers covered/total liters). KPIs for electricity consumption (e.g, total consumption/production volumes; energy consumed/number of employees; energy consumed/hours worked).
	Confirm the existence of Carbon Footprint certificates for products or by company; verify that they are updated and still valid.	--
	Substances that deplete the ozone layer (ODS) Where relevant: Confirm that the calculated ODS emissions are within the set limits and in compliance with the regulations.	Emissions of substances that deplete the ozone layer (GRI 305- 6). KPIs in relation with the production of ODS (e.g, difference between the amount of ODS produced minus the amount destroyed by approved technologies, and minus the amount used as raw material for the manufacture of other chemical substances).
	Nitrogen oxide NOx (excluding N2O), SOx, volatile organic compounds (VOC) and particles (PM10), H2S, HAP Confirm that the method for calculating emissions (direct measurements, based on data centers, estimates…) is correct and properly backed up.	EM-EP-120A.1 EM-RM-120 A.1 RT-CH-120A.1 (SASB). Air emissions for each category (GRI 305-7).
Non-compliance of the standard	Confirm that the company complies with the regulations for emissions that may apply.	No. of penalties. Amount of penalties (€).

Management of natural resources, biodiversity and ecosystem services

RISKS	AUDIT APPROACH	INDICATORS
Management of natural resources **General risk:** Not having business license to operate and access to financing. **Risks by vector** Ground - raw materials (RM) and water. - Regulatory risk: Limits for RM capture, or areas with water shortages. - Operational risk: environmental and/or safety risk, spillage or leaks, production stoppages, fines or penalties, repair costs. Limited capacity in areas with water shortages - future water demand. - Increased future demand for RM. - Reputational risk: as a result of the potential adverse effect of the activities of the company. Operations in areas with water shortages. - Social risk: use of the land for operations that differs from the community, movement of population, areas of water shortage.	**Management of natural resources** Land - RM and water. - Ensure that an assessment of the environmental and social impact has been made, and that action plans to prevent and mitigate the impacts identified exist. - Confirm that there is an economic assessment of the risk and its impacts. - In the event of an operating incident, ensure that there is a register of impacts, remediation and follow-up actions to return to acceptable or agreed levels of quality. - Guarantee compliance with the quality control measurements stated in environmental law/regulation/authorization. * Specifically for water: - Ensure the data quality (measuring instruments, registers, calculations, tools, etc.) concerning volumes of water used, released, reused and how much is within the acceptable range of quality. - Ensure that the business operating centers comply with laws and provide quality parameters. - Confirm that the targets for reducing capture and use of water are being met, especially in operations with intensive consumption.	- No. of risk assessments pending completion, totally or partially. - No. of actions pending implementation and no. of days delay, by criticality. - No. of penalties/ fines/ complaints and their financial cost. No. of penalties appealed against. Non-payment. - Level of compliance with quality plans. - Level of compliance with maintenance plans, including calibrations, to guarantee data quality. - Level of preparation of emergency plans. - Level of compliance with plans for emergency drills. - No. of collaborations/studies with organizations that protect biodiversity.
Biodiversity and ecosystem services: - Regulatory risk: restrictive new legislation. - Operating risk: adverse effect on biodiversity: spillages, fires, invasive species, etc. Fines or penalties. - Reputational risk: as a result of the potential adverse impacts of the activities of the company. Loss of species and severe impact in vulnerable, protected areas rich in biodiversity. - Social risk in vulnerable areas where there are indigenous people, fishing, cattle and farmers. Whatever has an impact on the use of land or water, whether the seas or rivers.	**Biodiversity and ecosystem services:** - Ensure the presence of underlying studies. - Ensure that an assessment of environmental and social impacts has been made. - Ensure that the impacts have been identified and action plans defined to prevent potential impacts. - Ensure that the actions defined in the plan are registered and monitored. - Ensure that there are no pending remedial actions. - In the event of an operating incident, ensure that there is a register of impacts, remedial and follow-up actions to return to levels of quality. - Ensure that there is a system that enables an assessment of the water bodies which receive discharges, including their volumes, their quality and other associated ecosystems. - Opportunity for collaboration with organizations that protect biodiversity and ecosystem services.	

Circular economy and waste management

RISKS

Regulatory and operative risks:

- General non-compliance with laws that regulate the production, possession and management of waste.
- Non-compliance with the obligations of selling waste-generating products.
- Absence of communication with the corresponding authorities when starting waste-generating activities.
- Incorrect separation and packaging of materials and waste.
- Partial, incorrect or missing labels for containers with hazardous and non-hazardous waste.
- Inappropriate storage or non-compliance of time limits for storage.
- Incorrect management of a waste product (abandon, discharge or uncontrolled disposal) instead of removal through an authorized agent.
- The delivery, sale or transfer of hazardous waste to unauthorized people or organizations.
- Absence of preparation and sending of studies to minimize hazardous waste for producers of such material.
- Absence or non-renewal of financial deposits or guarantees when these are required by law.
- Contamination of land or water through incorrect waste management.

Reporting risks:

- Absence of procedures to collect and maintain records from waste management agents.
- Incorrect reporting of quantities of material consumed and the amount of waste generated

Reputational risks:

- Absence of a strategy for improving material consumption, waste minimization and promotion of recycling and reuse. No consideration of the analysis of product or service life-cycle.

AUDIT APPROACH

- Review of applicable legislation (national, regional and local) on waste management.
- Review of obligations of selling waste generating products on the market (packaging, oils, vehicles, tires, batteries, electrical and electronic devices, etc.)
- For waste producing activities, request evidence of prior communications with correspondent authority before starting activities.
- Request list of waste generated and review of the classification of waste by type in relation with its hazardous nature according to applicable legislation.
- Verify the correct packaging and labeling of materials and waste.
- Verify the measures established to ensure correct storage of raw materials, chemicals and waste.
- Request study on minimizing waste and assess the level of compliance with the proposed measures.
- Assess the initiatives set in motion to improve efficiency throughout the product or service life-cycle.
- Request, where relevant, any financial guarantees which are demanded.
- Request file with the chronological record of the amount, nature, source, destination and method of waste treatment.
- Request the documents provided by the agent (delivery notes, DCS, etc.) to ensure the traceability of the reported information.
- Review forecast v actual for waste generation.
- Verify the accounting records of purchases and withdrawals of waste against the information in the records.

INDICATORS

Materials used by weight or volume (GRI, 301-1).

Recycled inputs (GRI 301-2).

Recycled products or packaging materials (GRI 301-3).

Waste generated (GRI 306-3).

Waste not sent for elimination (GRI 306-4).

Waste sent for elimination (GRI 306-5).

CLIMATE CHANGE

Governance

RISKS	AUDIT APPROACH	INDICATORS
Insufficient involvement of the Board of Directors (BD)/Steering Committee (SC) in considering climate risks.	- Existence of communication channels on climate-related issues to the BD and SC (review of procedures) and characteristics of the communications (regular presentations, dashboards, sporadic communications, etc.). - Formal and recurring review of climate related matters by the BD, and review of procedures related to BD business. - Existence of specific governing bodies to review climate-related matters (e.g. Sustainability Committee). Discussion in other governing bodies of climate-related matters (e.g. Audit Committee). - Give effective consideration to climate-related issues in decision making processes (review of minutes of meetings).	- No. of annual reports dedicated to climate change that reach the BD/SC. - Time dedicated by board members (in BD or delegate committees) to review risks or other aspects related to climate.
Non-compliance with the organization's agreed on governance model.	- Review of the company's public commitments in relation to governance (e.g. Sustainability Report, information reported to CDP, information sent to other rating agencies (e.g. DJSI, FTSE). - Comparison with elements of governance (previous risk) and definition of senior and intermediate management positions (in areas like Sustainability, Risk, Strategy, etc.).	- The company's sustainability rating. - Number of jobs in the company with specific responsibilities in managing climate risk

Risk management process

RISKS	AUDIT APPROACH	INDICATORS
Unsuitable method for quantifying risks.	- Review of the results of quantification. i) they are directly related with climate scenarios and the physical variables and transition that they define, ii) they include different time horizons (short/medium/long term), iii) and combine risks and opportunities associated with climate change using robust methods, iv); there is sufficient level of detail (by business unit and geographical area), v) and aggregation criteria that consider the correlation between the risks are used. - Review of the process for collecting physical variables (reliability of sources, sufficient detail in time horizons, variables and RCPP scenarios).	- Number of risks and opportunities identified. - Number of business unit and geography combinations evaluated.
Misalignment between the reported risk management process and the process used internally.	- Review of the information shared by the company in relation to the risk management process (e.g. Sustainability Report, information reported to CDP, information sent to rating agencies (e.g. DJSI, FTSE). - Review of the risk policy and process of risk management (or, where relevant, risk manual). - Where relevant, review of the latest process to identify and assess risks ("risk workshop") with a focus on climate risks: basic documents, input information, insights generated. - Review of the process of identifying mitigation plans for climate risks.	N/A

Strategy

RISKS	AUDIT APPROACH	INDICATORS
Incorrect definition of climate scenarios and use of heterogeneous scenarios.	- Identify long-term scenarios used by the company and their potential climate implications (i.e., in strategy, energy planning, investment or sustainability and risks areas). - Assess divergences between scenarios and impulse to adopt certain common climatic scenarios. - Identify inconsistencies in climate scenarios (i.e., unaligned physical and transition scenarios) - Ensure the use of an adequate number of climate scenarios (between 2 and 4) and that at least one of them is compatible with an aggressive transition scenario (an increase in temperature of <2°C by the end of the century).	- Number of climate scenarios used. - Number of physical climate variables compiled. - Number of transition variables.
Dissemination of messages not aligned with the outcome of climate risk quantification exercises.	- Analysis of information shared with stakeholders (i.e., frequent reports, information sent to investment funds or raters and messages to investors in roadshows) in showing a resilient strategy to the climate change scenario. - Review of the outcomes of internal climate risk quantification exercises (Net risk/opportunity impact) by climate scenario.	- *Climate value at risk* by scenario - CVaR breakdown by business and geographical area
Investor flight or restricted access to finance due to: - Not providing detailed risk information to investors. - Not providing information on the organization's resilience strategy for climate scenarios.	- Assure that the company pursues a short, medium, and long-term energy transition and decarbonization strategy, and that goals for its implementation have been set and are being followed up. - Assure that a short, medium, and long-term risk assessment of the company's climate change mitigation activities has been carried out. Ensure this is completed with an action plan. - Assure existence of policies and regulations regarding the management of greenhouse gas (GHG) emissions, inventory measuring and its verification. - Ensure the quality of data (measuring instruments, calculations, tools, etc.) measuring GHG emissions, as well as reduction of such emissions and offsetting measures. - Verify that the company has a governance model, defining roles and responsibilities.	- Reviewing the strategy plan and the degree of compliance with goals. - Number of fully or partially completed risk assessments. - Number of outstanding items on action plans, length of delay, criticality of the item. - Verification of emissions and strength of registration and reporting processes. - Verifying reports issued by third parties for their validation in accordance with international standards (ISO 14064). - Degree of implementation of the control model. - Number of climate change goals which have an impact on the remuneration systems for senior management and employees.

Goals		
RISKS	**AUDIT APPROACH**	**INDICATORS**
Objective setting process not documented with potential misalignment with risk appetite.	- Review of the process to define goals linked to indicators (procedures, minutes of meetings from decision-making bodies, ensuring traceability between input used and decision). - Review of the risk appetite framework, if any, regarding climate change commitments and alignment of the to specific goals and timeframe.	- Number of goals defined (including breakdown of indicators by business and geography). - Number of climate relevant indicators for which no goals are defined. - Number of risk appetite statements related to climate aspects.
Non-inclusion of sustainability indicators in remuneration.	- Review of existing remuneration policies, both for managers and for employees, identifying elements linked to sustainability. - Review of associated indicators and alignment with the company's overall goals.	- Percentage of staff whose variable remuneration is partially affected by sustainability indicators. - Average percentage of variable remuneration affected by sustainability elements.

Approach for the financial sector

Contrary to non-financial business, with operations often impacting directly on environment, financial sector organisations impact is most likely indirect. This refers to the impact on the environment derived from the operation of its clients (financed, insured) or by organisations the company is invested in. Therefore, when analyzing the environmental risks of the financial sector and the scope of Internal Audit, a different perspective should be adopted.

The *Guide on Climate-Related and Environmental Risks*, published by the ECB, sets expectations for risk management frameworks for financial institutions. The approach is to be implemented gradually.

As a consequence, internal audit should also adjust its work gradually in line with the risk management framework.

The European Commission presented on April 21, 2021 an ambitious and comprehensive set of measures to channel funding to sustainable activities across the European Union. By allowing investors to re-orientate their investments towards technology and more sustainable companies, these measures will be essential to achieve a more carbon neutral Europe by 2050 and will make the EU a worldwide leader in the establishment of sustainable finance. The package consists of the EU Taxonomy Climate Delegated Acts, a proposal for the Corporate Sustainability Reporting Directive (CSRD) and six Delegated acts.

Additional voluntary benchmarking standards in the financial sector are the *Principles for Responsible Banking* and the *Principles for Responsible Investment*, backed by the United Nations, establishing the general principles for banking and investment, as well as transparency and reporting obligations for companies adhered and the UN's *Principles for Sustainable Insurance* (PSI).

The proposed approach would split auditing in to two areas:

- Environmental risk assessments performed on clients, transactions and vendors, assessing financial and reputational impact on the organization.
- A detailed review of the audit approach for climate risks.

AUDIT APPROACH FOR THE ANALYSIS OF ENVIRONMENTAL RISKS

Environmental analysis

RISKS	AUDIT APPROACH	INDICATORS
Client-driven environmental risks: Inadequate assessment of environmental risks associated with client transactions may damage reputation and include financial impacts.	**1. Environmental due diligence/screening of clients/transactions** a) Verify that a prior due diligence policy and process is in place that evaluates environmental risk associated with the financing of clients. Review that the policy details the following attributes: - Does the process and policy include at risk sectors (infrastructure, automotive, oil & gas, agriculture etc.)? - Risk-based approval and exclusion for customer transactions. - Review environmental risk mitigation action plans agreed with clients. b) Assure environmental risk assessment has been carried out on customers that operate in high environmental risk sectors. c) Verify that, for clients with a high risk of environmental impact, the transaction has been approved at the appropriate level within the company and that action plans have been established to reduce risks with those clients. Reviewing, for such clients, that a follow-up process of the action plans agreed with clients exists and, if they are not being carrying out adequately, there is a process to escalate and report them to the corresponding governance bodies (i.e. Committees).	Percentage of customers in the credit portfolio that have been subject to an environmental analysis over the portfolio's total. Percentage of customers/transactions rejected due to unacceptable environmental risk over the total number of transactions requested.

Environmental analysis

RISKS	AUDIT APPROACH	INDICATORS
Vendor-driven environmental risks: Inadequate assessment of environmental risks associated with vendor/supplier transactions may damage reputation and include financial impacts.	**2. Environmental due diligence/screening of suppliers** **a)** Verify that a prior due diligence policy and process is in place that evaluates environmental risk associated with supplier transactions. Review that the policy details the following attributes: - Does the process and policy include at risk sectors (infrastructure, automotive, oil & gas, agriculture etc.)? - Risk-based approval and exclusion for supplier transactions. **b)** Verify, for a selection of suppliers with a higher potential environmental risk, that an environmental risk assessment has been carried out, applying those policies correctly prior to entering to a contractual relationship with the supplier.	Percentage of suppliers that have been subject to an environmental assessment over total suppliers.

CLIMATE RISK AUDIT APPROACH

Governance

RISKS	AUDIT APPROACH	INDICATORS
Governance structure: Inadequate governance of environmental risks affects decision making and may result in greenwashing.	**1.** Governance body: a) Verify if the company's governance bodies adequately monitor climate risks. b) Verify that climate risks are discussed by governing bodies when setting strategy, remuneration policy and rolling out the risk management process. **2.** Organizational structure: Assess whether responsibilities are attributed to the management of climate risk within the company's organizational structure, according to the Three Lines Model. 3. Risk management framework: a) Verify the company has included climate risks in its risk management framework. b) Verify that the company has a process to identify and quantify climate risks within its risk management process, including capital allocation decisions.	Number of committees that include climate risks on their agenda. Existence of specific KPIs/business goals in terms of climate risk in the company's strategy. % of employees with climate risk related objectives included in remuneration. % of employees qualified (trained) in this topic. % of risks of risks inventory the company includes in climate risks as an additional driver.

Risk management process

RISKS	AUDIT APPROACH	INDICATORS
Climate risk management: Methodologies used to identify, quantify and manage climate risks are inadequate. Exclusion of climate risks from existing risk categories.	**1. Risk appetite:** a) Verify that the entity has included climate risks in its risk appetite framework and has defined *Risk Appetite Statements* (RAS) covering climate risks over an adequate horizon of time. b) Verify that Key Risk Indicators (KRI) and limits have been defined to adequately manage risk and that qualitative and quantitative metrics exist for transition and physical risks. c) Verify that the company's remuneration/incentives policy is aligned with the climate risk appetite, at the different company levels. 2. Credit risk: a) Verify that climate risks are being considered in the relevant stage of the credit approval process (scoring, assessment of collateral, price strategy, etc.). b) Verify climate risks are monitored in credit portfolios. c) Determine whether the company's credit risk policies include provisions for climate risk (concession policies, rating policies, etc.). d) Verify the existence of data on credit exposure and collateral volumes by geography/country, where activities or collateral are located, stating whether said countries/geographies are highly exposed to physical risks. 3. Operating risk: a) Verify that an assessment is made of how climate risks may have an adverse impact on business continuity in all locations where the company operates. b) Review the climate risk assessment on the continuity of third parties (suppliers), on which the business highly depends, located in areas with higher exposure to physical risks. 4. Market risk: a) Review that the effects of climate risk are monitored in the market current positions, as well as in future investments. b) Verify that the stress testing processes include climate risks. c) Determine if the company's investment policies take into account climate risk, and if climate risk is integrated in investment processes. 5. Stress testing: Verify that the company's stress scenarios have been reviewed to spread climate risks over an adequate period of time (long-term). 6. Liquidity risk: Assess whether climate risks may cause cash outflows or a reduction in liquidity and, if positive, verifying that said factors are included in the company's liquidity management process and calibration of the company's liquidity buffer.	**Overview of financial sector:** 1. Group's financed emissions (Scope 3): - Quantity (in EUR million) of carbon-related assets in the portfolio or % over total portfolio. - Weighted average carbon intensity per portfolio - Volume of exposure by industry or counterpart, to show the concentration of exposures towards low/high carbon intensity industries. **Financing and Investment Activities:** 1. Volume of collateral related to assets or activities in sectors mitigating climate change. 2. Exposure to credit risks and collateral volumes by geography/countries where activities or the collateral are located, stating whether these countries/geographies are highly exposed to physical risks. 3. Full amount of fixed-interest portfolio invested in certified green bonds (according to approved frameworks, EU *Green Bond Standard*) at the end of the year, compared to the total value of assets in the fixed-interest portfolio. **Insurance and subscription activities:** 1. Breakdown of subscription exposure by business lines (life/non-life/reinsurance) in economic sectors/industries. 2. % of products including climate risks in subscription processes for individual contracts (life/non-life/reinsurance).

Risk management process

Asset management: Environmental and climate risks are not sufficiently considered in the investment process and may lead to financial loss and reputational risk.	Integration of climate risks in the investment process: - Verify end to end investment process (policies/investment guides, decision on asset selection, building the investment portfolio, portfolio management and monitoring, participation of shareholders and reporting). - Verifying that the investment policy provides proper guidance in the investment process, highlights investment goals and is aligned with the investment strategy in terms of climate risks. - Verify that, for an adequate selection of assets, climate factors are included (indicators, trends, ...) in the macroanalysis, based on the industry and country, and that an estimate is made of the potential financial impact of climate risks in each industry on cash flows, the balance sheet, income, and integrated in assessment models. - Verify that the environmental challenges in companies invested into are analyzed, with special focus on carbon footprint (scopes 1, 2 and 3) and GHG emissions volume compared to its competitors in the industry. - Verify that climate risks are integrated in the process of building the portfolio and of selecting the investment strategy to be followed to integrate said climate factors. - Verify climate-related performance monitoring is carried out for assets.	**3.** Maximum expected loss due to natural disasters caused by climate change (life/non-life/reinsurance). **4.** Total losses attributable to insurance payments due to (1) expected natural disasters, (2) unexpected natural disasters, by type of event and geographical area. **Asset management activities:** **1.** Breakdown of assets managed by each business area through the different types of assets (equity/bonds/infrastructure/real estate/structured products/MBS/derivatives). **2.** Rate of funds managed responsibly (Social Responsible Investment) over total assets managed.
Subscription restrictions: The entity may have not altered its subscription activities to comply with the restrictions and prohibitions set by the group. The entity may not comply with subscription restrictions set by the group.	a) Validate the application of the company and the group's subscription directives, including: - The existence of a list of banned activities. - Existing processes to ensure compliance with the subscription policy. - Appropriate communication of the strategy regarding the application of the subscription policy to the entity's employees. b) Validate that the company has defined a criterion to screen all the green projects and activities in its insurance portfolio, as well as a related control model, to monitor the degree of implementation of adopted policies, and to review the management process for additional existing risks related to climate change. c) Validate that locally defined criteria are aligned with the restrictions set by the group (i.e. Restriction to insure assets related to coal and oil sands, drilling in the Arctic Pole or illegal fishing boats). d) For exceptions, make sure that the entity involves relevant governance bodies and consults the Corporate Responsibility and Risk Management areas for advice.	
"Green" hazards: The entity may not comply with the group's regulations on green hazards.	Validate credentials of claims settlement process (repair v replace, sustainability of parts and materials etc.).	
Design of insurance products: The entity may have not included environmental aspects in the design of its insurance products.	Review product design process to validate compliance with responsible saving or insurance criteria.	

Strategy

RISKS	AUDIT APPROACH	INDICATORS
Measures for climate impact: Incorrect reporting of environmental operations from operations.	**Strategy to manage the organization's carbon footprint:** - Validate that the environmental policy is defined and consistent with (qualitative and quantitative) goals and action plans (i.e. Reducing CO_2 emissions by person by 25%, 15% water consumption, 95% of paper is recycled or proceeds from sustainable resources). - Validate that there are clear and precise action plans aimed at reducing the company's environmental footprint (i.e. CO_2 emissions, electricity consumption, business travel, vehicle fleets, paper, water consumption, waste management). - Verify the usage of actual and reliable data to report information (under the framework of Directive 2014/49/EU on non-financial reporting).	**1. Group's financed emissions (Scope 3):** - Quantity (in EUR million) of carbon-related assets in the portfolio or % over the total portfolio. - Weighted average carbon intensity per portfolio - Volume of exposure by industry or counterpart, to show the concentration of exposure towards low/high carbon intensity industries.
Business model: Climate risks are not considered in objective setting or decision making, thus potentially threatening continuity of business. There might be the risk that the company is not feasible in the future due to an inadequate strategy or green-washing risk.	**1. Business model:** Verify climate impact on business model is measured over different time frames. Assure that outcomes of analysis are considered in decision making.	**2.** Percentage of income from products or services that finance/invest in economic activities contributing to mitigating or adapting to climate change (according to EU taxonomy).
	2. Business strategy: a) Ensure the company has short, medium, and long-term energy transition and decarbonization strategy, that goals for its implementation have been set, and that they are being monitored (i.e. that there are goals aligned to the entity's customers' portfolio to comply with the Paris Agreement to keep global warming below an increase of <2ºC). b) Verify that the short, medium, and long-term analysis of climate risks has been accounted for when determining the company's strategy and setting new business goals. c) Verify that goals (KPIs) have been defined aligned with the company's climate risk strategy and that the latter have been adequately reported in the company and are monitored. d) Assess if the entity's product and services portfolio consists of products/services to finance or invest in assets promoting sustainable activities substantially contributing to mitigating or adapting to climate change.	**3.** Volume of financial assets financing sustainable economic activities which are a significant contribution to mitigating or adapting to climate change (compared to total assets) according to the EU taxonomy. Example of retail banking: % of loans for electric/hybrid vehicles, % of mortgages for more energy efficient housing, Example of wholesale banking: % of loans to improve energy efficiency in housing.
Responsible investment: Investment strategy may diverge from the organization's climate goals. Investment process does not comply with policy. The organization may not promote the development of greens bonds and transition bonds financing.	**1. Investment strategy:** Validate that an adequate action plan has been implemented in the company to achieve the goals of limiting "global warming" under 1.5ºC by 2050, including at least: - Verify the company's investment plan to achieve the group's *Green Bond* goals. - Analysis of the entity's plan to launch transition bonds assets. - Verify that blacklisted investment aligns to goals to full detachment from coal as set out in Paris Agreement or by the WEF.	**4.** Number and quota of subscription products offered in relation to climate (non-life/reinsurance) - (if the company has prepared a specific offer by geographical areas specially exposed to extreme climate events). **5.** No. of climate change goals included in remuneration systems for senior management and employees

	2. Investment choice process - Verifying if the entity has defined criteria to adequately assess "green" activities and if such criteria are aligned with local rules. - Validate that the assessment methodology for investments is appropriate (considering criteria such as sustainability over time, compliance with regulatory and group requirements, and comparative assessment with internal and external best practices). - Verify that the assumptions and parameters used are appropriate (considering criteria such as actual analysis vs. expectations, sustainability over time, compliance with regulatory and group requirements, and comparative assessment with internal and external best practices). 3. Development of *Green Bonds* and *Transition Bonds* Analyze the implication and effort made to develop new "transition" financial instruments according to the entity's ambition.	

Reporting

RISKS	AUDIT APPROACH	INDICATORS
External or internal reporting: Inadequate management of data related to climate risk, which may lead to an inconsistent management of data, not aligned with regulatory requirements, or to an inconsistent use thereof in the company during decision-making.	1. Public information: Verifying that relevant information and metrics regarding climate risk are published, in accordance with the EU's non-financial information reporting guide. (European Commission's Guidelines on non-financial reporting: Supplement on reporting climate-related information). 2. Management information: Verifying that enough internal information is generated, with integration of data regarding climate risk and showing the company's exposure to it, and that this information is used by the relevant management bodies and committees to make decisions.	No. of internal reports (management information) created during the year including climate risk data. No. of metrics reported on climate risk in annual reports or sustainability reports.

AUDITING SOCIAL RISKS

Social factors have become more relevant over time, especially from the perspective of sustainable investment and, even more so, due to the effects of the recent pandemic.

Society and investors demand organizations lead my example, demonstrating ethics committed to social issues.

Social risks need to be reviewed from a double perspective. Internally and basically linked to employee relations, and externally, related to corporate governance driven relations to society.

Social risks are driven by numerous factors. Diversity and equality in policies, training and development of employees, health and safety, care for and contribution to society and the promotions of positive impacts in stakeholder communities.

Initiatives such as GRI give a basis on which we can look at risks possible audit approaches for organizations.

SOCIAL AUDIT

Diversity and equality

RISKS	AUDIT APPROACH	INDICATORS
Discrimination leads to reputational damage and talent drain.	- Assure that an approved code of ethics that covers diversity issues is published. - Evidence the approval and publication of policies promoting work life balance. - Verify that an equality plan is approved, published and in force. - Verifying that there is a remuneration policy (salary ranges) - Verify existence of model for performance reviews. - Verify existence of defined career pathways. Evidencing the existence of a Human Rights policy. - Assure the existence of due diligence process for Human Rights: risk identification, assessment of impact (direct and indirect, including those resulting from business relationships), training, communication channels and reporting, action plans and mitigation measures. - Evidence the existence of a complaints mechanism at operational level (other than ethics channels) according to the description on the UN Guiding Principles on Business and Human Rights.	Percentage of employees by category, age group, gender and other diversity indicators (i.e., ethnic origin) (GRI 405-1b). Ratio of basic salary and remuneration for each employee category by significant locations of operation for equality priority areas. (GRI 405-2). Average basic salary gap and relevant full-time employees' remuneration based on gender (women vs. men) and diversity indicators. (GRI 102-38).
Weak vendor due diligence program or processes can lead to indirect criminal liability for organizations.	- Review onboarding process for new vendors or suppliers that include acceptance of ethics code covering social and environmental risks. - Review evidence for ethics training given to vendors.	Child labor, forced labor or mandatory labor risk. (GRI 408-1b, GRI 409- 1).

Diversity and equality

RISKS	AUDIT APPROACH	INDICATORS
Infringement of Human Rights and workers' rights causing financial loss (fines) and reputational loss.	- Review approval and publication of ant-harassment protocols. - Review equality, discrimination and diversity related cases reported on internal channels. - Review measures to prevent or mitigate impacts due to issues with child or forced labor, modern slavery or unionization in the supply chain.	Number of discrimination and harassment incidents and total amount of financial loss. (GRI 406-1). Number of discrimination and harassment incidents, status of incidents and adopted measures. Total amount of monetary losses resulting from legal procedures linked to: a) infringement of the Law, and B) discrimination at work.
	- Evaluate design of, and compliance with, policies related to freedom of association and collective bargaining provisions.	Freedom of association and right to collective bargaining at risk (%) (GRI 407-1). Percentage of working population covered by collective bargaining agreements.

Added value to society.

RISKS	HOW TO AUDIT IT	INDICATORS
Lack of monitoring and assessment of the impact of contributions to the community. Unreliable information on the economic value or impact of contributions.	- Review the aggregated economic value, achievements and impacts of company initiatives in the community (data audited in the financial statements or other guidance may be used).	Information that must be reported according to the GRI 201-01. London Benchmarking Group model. **i.** Direct economic value generated: income. **ii.** Distributed economic value: operational costs, salaries and employee benefits, payments to shareholders, payments to the government (by country) and investments in the community; **iii.** Retained economic value: "Directed economic value generated" less "distributed economic value"- (GRI 103 and GRI 201).
Long term strategy for adding value to society is not aligned with companies activities.	- Obtain the strategic plan and goals in the longer term related to ESG matters, as well as indicators associated to each of them, and verifying their degree of compliance, following up, if applicable, action plans that may arise because of deviations.	Criteria and indicators set in the company's strategy to favor the community at social level. (Deviations).

Contribution via subsidies

RISKS	AUDIT APPROACH	INDICATORS
Fraud in the management of subsidies.	- Verify match of grant /subsidy vs funds received. - Verify correct use of funds (purpose v real use). - Review value generated from correct use of funds. - Ensure that the necessary control mechanisms are in place to guarantee the performance of subsidies received.	Total sum of funds received over period of time including tax relief, subsidies, etc.

Innovation

RISKS	AUDIT APPROACH	INDICATORS
No clear strategy for innovation may limit growth and competitiveness.	- Verify that R&D+i projects are meeting the established deadlines and physical and financial goals.	Innovation *benchmark* between organizations and its competitors. Innovation indicators included in the strategy.
Technological advances are not deployed in line with competition.	- Review metrics and indicators. - Review internal controls over bot deployment.	Manual ordinary tasks vs automated tasks. Workers' free hours vs robots.

Hiring and management of human resources

RISKS	AUDIT APPROACH	INDICATORS
Non-compliance with data protection directives Weak securitization of confidential information. Cyber attacks Impersonation.	- Verify controls over algorithmic processes and machine learning. Assure anonymity.	Amount of sensitive data included in algorithm inputs and outputs.
Information used in machine learning processes is discriminatory.	- Review data populations for bias and discrimination.	--
Malpractice in employee management may lead to lower performance and incentivize occupational fraud.	- Review hiring policies. - Review diversity of workforce. - Review diversity of new hirings. - Review diversity of employee rotation. - Review exits, review for voluntary or disciplinary and verify root cause. - Review employee satisfaction surveys. - Verify implementation of action plans.	**i.** Segment new hires as % of total by age group, gender, etc. **ii.** Employee's rotation total number and rate over a period of time, by age group, gender, other diversity indicators and region. (GRI 401-1a&b).

Hiring and management of human resources

RISKS	AUDIT APPROACH	INDICATORS
Data breaches leak employee or organization private and confidential information.	- Review controls to prevent data breaches of sensitive employee data. - Review data systems and hardware used in HR processes. Test for extraction or illicit sharing vulnerabilities. - Inventorize sensitive employee data (current and past). - Review storage methods and hardware. - Identify interdepartmental personal data flows.	No. of reports based on privacy violation. (GRI 418 may serve as a guide, although this standard is based on the protection of consumer's data).

Employee's health and safety.

RISKS	AUDIT APPROACH	INDICATORS
Non compliance with health and safety regulations. Non-committance to employee wellbeing.	- Review health and safety governance and relevance: strategy and goal setting, reporting to the management proactive or reactive indicators. - Assess the company's occupational health and safety management system, rules, procedures, management plans, certifications, risk analysis, training and awareness, management of change, etc. - Review the robustness for Occupational Health and Safety program. Check for: • Risk assessments • Preventative measures • Incident investigation • Internal audits • Leadership visits • Health monitoring • Reporting quality • Workers' participation and consultation • Follow-up of internal inspections or external certifications • Other on-going improvement initiatives. - Review non-occupational health services offered to workers (i.e. private health insurance or physiotherapy service) and health and well-being promotion programs (i.e. healthy food, programs to stop smoking or managing stress, nutrition experts, agreements with sports centers) and their reach, to ensure needs are adequately met. Review the involvement of employees in the selection of programs and how success is measured. - Review scope of H&S program. Does the program cover all our liabilities, i.e. contractors, agents, vendors etc.? - Evaluate data protection measures for employee H&S data.	Reactive indicators. - Occupational hazards: no. of fatal victims, frequency rate, severity index, - Absenteeism rate (GRI: 2018 403-9). Proactive indicators: - Health and safety training hours: - Inspections done. - No. of reports on risk situations. - Assistance or health and well-being promotion services offered to employees. (GRI:2018 403-6).

Training		
RISKS	AUDIT APPROACH	INDICATORS
Employees do not receive required training.	- Assess governance when setting employee's training strategies and goals. - Evaluate controls over the recording of training hours and attendance. - Verify that learning objectives are achieved. - Review content of community development programs and performance against objectives.	% of employees that have received training. (GRI: 404- 2).
Discrimination in training.	- Verify that training is provided to all employees of the same rank. - Assure that there are no discriminatory practices. - Assessing the criteria to select employees for training. - Verify the consistency of the adopted approaches for training. - Review the percentage of training hours among the number of employees.	No. of yearly training hours per employee. (GRI: 404- 1.) % of employees receiving regular feedbacks on their performance and professional development. (GRI: 404-3).
Unmotivated employees affect talent retention and productivity.	- Review employee satisfaction with training programs. - Verify if actions are implemented based on survey results. - Investigate high employee rotation and root causes.	Training programs to upgrade employee's skills. (GRI: 404.2).
Lack of employee talent and employability in the medium/long-term.	- Assure whether training goals are included for future workers. - Verify the existence of training help programs to drive future employment.	Programs to help transition. (GRI: 404.2).

GOVERNANCE AUDIT

There is a consensus between markets, investors, society and employees that good corporate governance is critical. The supervision of ESG criteria in organizations is therefore gaining importance at board and management level.

Governance in this sense includes those aspects related to the organization's internal structures, policies, decision making processes and how these factors reverberate with stakeholders.

More specifically this covers management and leadership structures, labor relations, policies establishing independence, transparency, and accounting policies, promotion of good practices, or the fight against corruption, fraud, and money laundering, among other factors.

Internal Audit plays a key role in ensuring initiatives which promote responsibility, transparency, and that good corporate governance practices are adopted and implemented in their organizations.

Various benchmarking initiatives give a basis on which we can look at risks and possible audit approaches for organizations.

GOVERNANCE AUDIT

Governance structure and responsibilities

RISKS	AUDIT APPROACH	INDICATORS
The compositions of governing bodies do not hit targets for representation or length of mandate.	- Assure rules of procedure for the board include rules of procedure for supervising committees, and that these are consistent with legal requirements.	- % of female members of the board/Total members of the board. - % of independent members of the board/Total members of the board - % of foreign members of the board/Total members of the board - Average seniority of independent members of the board.
Sustainability and audit committees do not have sufficient scope to supervise ESG matters.	- Verify there is adequate monitoring of ESG matters from the Board of Directors and sustainability and auditing committees, through an annual schedule of matters to be dealt with aligned with their respective responsibilities, such as approval of the adequate sustainability policy in terms of environmental and social aspects, as a non-delegable power of the Board of Directors, transparently providing information about its development, application and results.	No. of meetings for each committee in the year discussing ESG matters.
Information on ESG risk management does not flow through the organization.	- Verify that management is involved in sustainable development and that this matter is regularly discussed in executive management committees.	- No. of meetings of each committee per year discussing ESG matters. - Sufficient time to prepare meetings. - Rules on the number of committees in which their members can be.
Lack of specific ESG knowledge at Director, C-Level and on the Board.	- Verify existence of specific ESG training programs. - Verify that selection of board members includes specialists.	ESG training hours/member of the governance body.
ESG risk management structures and responsibilities are inadequate.	- Verify that accountability and responsibility for ESG risks is clearly defined through policies and procedures, and that supervising committees are established.	No. of meetings for each committee per year in which ESG matters are discussed.

9. Such as OECD and G20's corporate governance principles, GRI 102 and ICGN (International Corporate Governance Network) principles.

Stakeholders' expectations

RISKS	AUDIT APPROACH	INDICATORS
Shareholder meetings do not abide by the principles of transparency and adequacy of information. This may breach shareholders' rights.	- Verify that there are general shareholder's meeting regulations governing, at least, the board's powers, the meeting requirements, shareholders' rights and, particularly, participation rights. - Verify the duration of the shareholders' meetings. - Verify documents and reports made available to shareholders' (prior to holding the meeting). - Verifying that there is a general policy for communications and contact with shareholders. - Verify that a specific communication channel or service is available to shareholders. - Verify the information made available to shareholders from the "Investor Relations" section of the organization's web.	- No. of general shareholders' meetings held. - Quorum in the general shareholders' meetings held. - No. of meetings in which the following people have taken part: CEO, CFO, Chairman of the Board and Chairman of the Board's Committees (auditing, remunerations, appointments, and other committees). - Disclosure of information prior to the meeting (reports, agenda, etc.). Number of days in advance relevant information is disclosed. - No. of questions, matters or requests submitted to the shareholders' office and number of matters settled satisfactorily, in accordance with the shareholder's assessment.
The general shareholders' meeting does not adequately manage minority shareholders' participation. Risk associated to power abuse by controlling shareholders.	- Verify the existence of regulations regarding the participation of minority shareholders, proxy voting, remote attendance, etc. - Evaluate the level of transparency of the proxy voting procedure. - Verify there is a policy promoting shareholders' participation, such as a share policy to attend shareholders' meetings.	- Information on the percentage of quorum participating in each meeting through "proxy voting". - No. of proxy voting requests accepted and rejected. - No. of questions included in the agenda under request of minority shareholders. - Disclosure of resolutions adopted and percentage of favorable and unfavorable votes.
Poor management of customer or consumer relations.	- Verify the existence of rules regarding costumer and consumer relations and management. - Verify the existence of a communications office or channel for clients and consumers (customer office, customer service, etc.).	- No. of complaints filed by customers/consumers. - Percentage of complaints settled appropriately (customer's assessment).
Poor management of supplier/vendor or supply chain relations.	- Verify the general procurement and supply policies including the assessment, approval and onboarding of suppliers. - Verify that environmental, social, corruption and bribery matters are included in suppliers' assessment and approval procedures. - Verifying the existence of a suppliers' code of ethics or similar documentation extending the entity's commitment to ESG goals to the supply chain - Verify there are provisions made for auditing and supervising suppliers.	- No. of suppliers analyzed for approval over the period (percentage of suppliers approved and suppliers rejected). - No. of suppliers rejected for ESG matters. - No. of suppliers adhered to the suppliers' code of ethics. - No. of complaints received regarding breaches related to the supply chain. - No. of audits of suppliers over the year (% of "apt" and "not apt" suppliers).

Strategy. Risk Management and Investment		
RISKS	**AUDIT APPROACH**	**INDICATORS**
ESG strategy and goals are not defined.	- Verify that specific and strategic ESG goals have been set and published, including Key Performance Indicators (KPIs), in line with the company's risk appetite.	- Company's positioning in benchmarking sustainability indexes (Dow Jones, GRESB, etc.). - No. of ESG KPIs/Total KPIs. - Degree of progress of ESG strategic plan.
	- Review design and effectiveness of KPIs.	- No. of ESG KPIs/Total KPIs.
ESG strategy is not aligned to global or other strategy.	- Verify that ESG strategy is consistent with other strategies.	- % of ESG related goals with employees' variable remuneration.
ESG risks are not considered when establishing the company's strategy.	- Verify assessment of new trends in sustainability to identify risks.	- % of ESG risks over total risks. - No. of KRIs (key risk indicators) defined in terms of ESG.
	- Review strategy and objective setting processes to assure ESG risks are considered, according to their relevance for the company's strategy in the long-term, its competitive position, its qualitative factors and, if possible, quantitative values driving financial value.	- No. of KRIs (key risk indicators) defined in ESG terms.
	- Verify that impact from new and emerging ESG topics are evaluated and incorporated into long term forecasts.	- % of sustainable finance KPIs vs financial KPIs - No. of KRIs (key risk indicators) defined in ESG terms.
	- Verify specific governance mechanisms have been established to manage ESG risks. - ESG risks discussed in risk committees. - Specific ESG risk working groups have been set up.	- No. of meetings of the ESG committee.
ESG strategy is not fluidly communicated.	- Verify disclosure of ESG strategy to stakeholders.	- No. of ESG training communications and/or actions.
ESG aspects are not part of the company's investment strategy.	- Verify that the company includes ESG aspects in its investment proposals and decisions, to contribute to improving profitability adjusted to risk.	- Sustainable investment criteria - % of sustainable finance KPIs vs financial KPIs

Remuneration system

RISKS	AUDIT APPROACH	INDICATORS
Lack of commitment in the achievement of ESG goals.	- Verify that variable remuneration policy is linked to ESG goals. Verify policy does not promote or allow excesive risk taking.	- % of variable remuneration linked to attaining ESG goals.

Internal regulatory framework and Information Systems

RISKS	AUDIT APPROACH	INDICATORS
Company does not keep abreast of corporate governance requirements due insufficient resources.	- Assure responsibilities for maintaining the corporate governance framework are clearly defined.	- People/areas/committees responsible for identifying and keeping up to date the corporate governance regulatory requirements.
	- Verify maintenance tasks have been carried out.	- Number of governance reviews carried out in year. - Number of actions implemented in response to corporate governance reviews.
Internal corporate governance regulations do not meet external requirements.	- Verify internal corporate governance regulations meet external requirements and disclosed voluntary commitments.	- Number of reviews of corporate governance framework carried out in the period.
	- Verify that the corporate governance regulatory framework is updated in line with regulatory updates and/or voluntary commitments undertaken by the company in the last year.	- Number of actions implemented in response to corporate governance reviews.
Corporate Governance framework is no adequately communicated.	- Assure mechanisms exist to communicate corporate governance framework. - Assure communications have been made.	- No. of platforms/corporate vehicles existing for the internal dissemination of the internal corporate governance regulatory framework. - Number of communications made regarding corporate governance framework.

Internal regulatory framework and Information Systems		
RISKS	**AUDIT APPROACH**	**INDICATORS**
Not having an adequate training plan to drive employee awareness and compliance with the internal corporate governance framework.	- Verify the existence of the company's training plan with regard to corporate governance.	- No. of training actions on corporate governance included in the annual training plan.
	- Verify the training courses/pills in the year regarding the internal corporate governance regulatory framework.	- Number of hours dedicated to corporate governance training in the period. - % of (key) staff trained on corporate governance in the period.
Insufficient resources to assure compliance with corporate governance framework.	- Assure responsibilities for maintaining the corporate governance framework are clearly defined.	- People/areas/committees responsible for ensuring compliance with the corporate governance regulatory requirements.
	- Verify actions taken correspond to responsibility framework.	- No of reviews of corporate governance framework carried out in the period. - Number of corporate governance non-compliant events recorded in the period. - Number of actions implemented in response to corporate governance non-compliance.
IT systems are not implemented or do not have the capacity to record non-financial information.	- Assure IT systems exist for recording ESG information and these are adequately maintained.	- Number of indicators for ESG risks embedded in IT systems.
IT systems have weak controls and cannot guarantee data integrity.	- Assure controls for data integrity are implemented and functioning according to design.	- Results of the review done on corporate IT systems handling information/indicators related to ESG risks and the internal corporate governance framework. - Number of remediation measures implemented in IT systems over the period.

Transparency, Supervision and Reporting		
RISKS	**AUDIT APPROACH**	**INDICATORS**
Supervision framework not adequately designed or implemented.	- Verify that a risk management exists and defines supervisory roles and responsibilities adequately for each of the three lines. - Assure this approved and communicated.	Last policy update and level of approval.
	- Review design of risk and control matrices. - Verify ESG risks are covered. - Verify approach for risk assessment. - Verify adequacy of internal controls.	No. of risks and controls per taxonomy and organizational levels.
	- Evaluate effectiveness of internal controls.	No. of controls with incidents and sorted by owner.
	- Assure efficient issue tracking and remediation.	Average age of issues.
	- Assure issues are escalated to senior management and Directors.	Number and frequency of reports to senior management and governance bodies.
Internal and external communication and reporting plan is not documented or is inconsistent with principles and commitments.	- Verify existence of approved communication and reporting plan. - Verify that this is shared with stakeholders. - Assure mechanisms in place for assuring transparency in ESG risk reporting. - Assure compliance with ESG commitments. - Verify KPIs are implemented, monitored and acted on.	Last plan update and level of approval. -- Internal and external reports ESG KPIs performance and trends.
Opportunities arising from transparency, supervision and reporting initiatives are not identified.	- Assure mechanisms exist to identify and process opportunities arising from ESG reporting and supervision.	No. of potential opportunities and % implemented.

Ethics and integrity

RISKS	AUDIT APPROACH	INDICATORS
Organization does not consider the promotion of ethical behavior culture as a strategic matter.	- Verify that the organization's principles, values, and behavioral rules are communicated in a Code of Ethics or similar document.	No. of employees that sign the code of ethics/total number of employees.
Organization does not have a formalized compliance system. or, compliance system does no offer employee guidance and training.	- Obtain evidence of its communication to employees and suppliers and confirmation they understand and accept them when entering the company and, on an annual basis, take into account their potential adaptations.	Initiatives to spread the organization's code of ethics.
Not following up ethical issues and performance using an effective system to measure progress.	- Obtain and review joint authorization and approval delegation matrices, order approval flows, approval flow for invoices integrated in ERP, granted powers, traceability of each approval and signature. Governance responsibility and segregation of duties is always taken into account.	- Powers delegation matrix. - Implemented approval flows. - Analysis of level of segregation of duties.
Remuneration system does not contemplate employee performance related to corporate values. There is no provision for disciplinary action for non-compliance with corporate values.	- Defining the company's mission and vision and verifying whether it includes ethical principles and conducts.	- Presence and publication of ethical values. - No. and frequency of ethical audits and level of dissemination of results.
	- Obtain evidence on the application of ethical principles in employee recruiting processes.	No. of candidates assessed based on ethical criteria per process/number of candidates hired.
	- Review remuneration system for inclusion of realizable and quantifiable objectives for performance and behavior.	Analysis of salary bands in the company and market benchmarking.

Corruption and bribery

RISKS	AUDIT APPROACH	INDICATORS
Contributions and donations to foundations and non-profit entities are not aligned with the company's strategy and goals.	- Review evidence on the criteria for approval of contributions to non-profit organizations.	Number of contributions made in the period, total volume of contributions, average volume of contributions.

Corruption and bribery

RISKS	AUDIT APPROACH	INDICATORS
Non-compliance with AML, Anti-Corruption and Bribery laws and commitments.	- Verify that the Board of Directors shows commitment to AML and anti-corruption and bribery efforts.	- No. and % of members of the governance body to whom the company's anti corruption policies and procedures have been reported, broken down by region. - No. and % of members of the governance body who have been trained against corruption, broken down by region.
	- Review adequacy of risk assessment, by sector, business, geography, etc.	- No. and % of transactions assessed related to corruption risks. - No. of significant risks related to corruption identified by means of a risk assessment.
	- Verify mechanisms for monitoring and supervising (AML- or Anticorruption) programs.	- No. of existing controls and frequency to verify they work adequately.
	- Verify the organization has a clear, updated, visible and accessible policy banning corruption and money laundering.	- Last update and approval by adequate level and consistency with the risks assessment.
	- Verify the organization has detailed AML and anti-corruption policies by specific risk areas.	- Existence of a risk map related to existing policies and/or procedures (Yes/No).
	- Verify that the anti-corruption and money laundering program is applied to business partners.	- Number and % of business partners that recognize organizations anti-corruption policies and procedures, broken down by type of partner, business and region. Describing whether the company's anti corruption policies and procedures have been reported to another person or organization. - No. of cases in which contracts with business partners have been terminated or have not been renewed due to corruption related issues.
	- Review of design and effectiveness of internal controls.	- No. of controls implemented, executed and verified.
	- Review training programs.	- Nº and % of employees that have received organization's anti-corruption policies and procedures.
	- Review plans and programs for the promotions of ethical behavior and compliance.	- Number and % of employees that have been trained on the organization's anti-corruption policies and procedures.

Corruption and bribery

RISKS	AUDIT APPROACH	INDICATORS
	- Review provisions for whistleblowing and internal reporting of ethics violations.	- No. and nature of confirmed corruption cases. - No. of confirmed cases in which an employee has been fired due to corruption or against which disciplinary measures have been adopted in this regard.
	- Review adequacy of investigations protocols for breach of ethics codes.	- Public legal cases filed against the company or its employees regarding corruption in the reporting year and outcome.
	- Assure anti-corruption and AML policies are reviewed and updated.	- Number and frequency of compliance management audits. - Number of recommendations and severity etc.

Tax

RISKS	AUDIT APPROACH	INDICATORS
Inadequate or inconsistent tax strategy.	- Obtain evidence there is a tax strategy.	Strategy approved by the Board of Directors. (Yes/No).
	- Review to assure tax strategy is designed, approved and reviewed by persons with sufficient accountability and adequate knowledge.	There are governance rules or statutes (Yes/No).
	- Review for adequate tax compliance provisions in all jurisdictions.	There are third-party reports evidencing compliance levels (Yes/No).
	- Review documents related to fiscal planning.	- Review tax risk mapping.
Insufficient controls over tax processes.	- Obtain evidence that the body responsible for the company's tax strategy can describe the degree of responsibility of governance bodies and the responsibility delegation procedures within the company.	A tax decision matrix exists.
	- Obtain evidence of the processes, projects, and initiatives to back up effective tax compliance within the company.	No. of controls implemented, executed and verified.
	- Review training programs that tie fiscal strategy to corporate development.	No. and % of employees trained on fiscal matters.
	- Review effectiveness of internal controls for tax compliance.	No. and nature of cases confirmed.
	- Obtain evidence of the level of commitment with tax authorities and public fiscal policies, as well as the progress on gathering opinions from stakeholders.	No. and type of agreements with third parties.

Conclusions

ESG matters entail a series of risks and opportunities that challenge internal audit to provide concrete assurance to senior management and the Board.

Internal audit should therefore understand and analyze certain questions:

- Senior management and the Board´s role in monitoring sustainability issues.
- The process for identification, assessment and management of ESG risks.
- The framework used for non-financial reporting.
- The internal control system for non-financial reporting.

Furthermore, it is essential for Internal Auditing to identify specific risks for each material matter, within each of the three ESG pillars, and to establish a specific approach towards carrying out its work.

Environmental (E) aspects are very diverse and often require subject matter experts. Two large blocks stand out: environmental management and climate change, which may entail reputational, regulatory, operational or financial risks. In this case, audit tests may mostly be substantive due to the abundant existing information on non-financial data, such as tons of CO^2 or other energy consumption. However, especially when it comes to climate change risks, the internal auditor may combine control tests with compliance tests and review and verification of information and indicators. The auditor may check for inconsistencies or deviations and then recommend actions be taken.

Regarding social (S) aspects, the main matters to be approached by Internal Audit are related to diversity and equality, contributing value to society, recruitment and human resources management, health, safety and well-being of employees, and training. Adverse impact from risks may be seen on the organization's reputation, its capacity to attract and retain talent, the violation of human and workers' rights, loss of competitiveness and obviously on its bottom line. The internal auditor may use substantive testing or internal controls assessments. Review of quantitative indicators is also a useful tool.

The main risks related to the Governance pillar cover:

- Corporate governance compliance.
- Not satisfying stakeholder´s expectations.
- Non-alignment of sustainability strategy and overall objectives.
- Non-transparent internal and external reporting
- Non-alignment of remuneration policy with ESG policy.
- Undefined tax strategy.
- Undefined ethics culture.
- Non-compliance with anti-bribery laws.

It is essential that Internal Auditing identifies the specific risks of each ESG pillar and establishes a specific approach towards work.

The internal auditor may wish to evaluate the organization's compliance model and procedures, and review internal controls.

Internal Audit is key to providing the Audit Committee, senior management and other stakeholders, with the assurance they require on the impact of ESG risks.

Bibliographical references

MONOGRAPHS

- BONIME-BLANC, A. *Gloom to Boom: How Leaders Transform Risk into Resilience and Value.* London: Routledge, October 2019. ISBN 978-1783538157.

REPORTS AND STUDIES

- ACCIONA. Sustainability Report 2019, 2020.
- EUROPEAN CENTRAL BANK. *Guide on climate-related and environmental risks,* 2020.
- BASEL COMMITTEE ON BANKING SUPERVISION. *Climate-related financial risks - measurement methodologies*, 2021.
- BASEL COMMITTEE ON BANKING SUPERVISION. *Climate-related risk drivers and their transmission channels,* 2021.
- CARBON DISCLOSURE PROJECT. *Global Climate Change Analysis 2018,* 2018.
- SOCIAL IMPACT CHAIR COMMILLAS -ICADE. *Principios ESG y cadena de valor: del reporting al impacto social,* 2021.
- CENTER FOR AUDIT QUALITY. *The Role of Auditors in Company - Prepared ESG Information: Present and Future,* 2020.
- CHARTERED INSTITUTE OF INTERNAL AUDITORS. *The role of internal audit in non-financial and integrated reporting,* 2015.
- CLIMATE DISCLOSURE STANDARDS BOARD. *Application guidance for climate-related disclosures,* 2020.
- EUROPEAN COMMISSION. *Interim study on the development of tools and mechanisms for the integration of environmental, social and governance (ESG) factors into the EU banking prudential framework and into banks' business strategies and investment policies,* 2020.
- CONSEJO GENERAL DE ECONOMISTAS DE ESPAÑA. *Trabajo preparatorio sobre las normas de información no financiera de la UE: Un tour europeo - El enfoque español,* 2021.
- CORPORATE HUMAN RIGHTS BENCHMARK. *2019 Key findings,* 2019.

- CORPORATE REPORTING DIALOGUE. *The Sustainable Development Goals and the future of corporate reporting,* 2019.
- ENAGÁS. Annual report 2019, 2020.
- EU TECHNICAL EXPERT GROUP ON SUSTAINABLE FINANCE. *Taxonomy: Final report of the Technical Expert Group on Sustainable Finance,* 2020.
- EUROPEAN CONFEDERATION OF INSTITUTES OF INTERNAL AUDITING. *Non-Financial Reporting: Building trust with internal audit,* 2015.
- EUROPEAN CONFEDERATION OF INSTITUTES OF INTERNAL AUDITING. *Practical guidance on climate change and environmental sustainability,* 2021.
- EY. *Barómetro de Divulgación del Riesgo Climático 2020,* 2020.
- FERROVIAL. *Integrated annual report 2020,* 2021.
- FORÉTICA. *El futuro de la sostenibilidad en las empresas - Resiliencia y 'nueva normalidad' Post COVID-19,* 2020.
- IBERDROLA. Non-financial information report - Sustainability report 2020, 2021.
- KPMG. *La importancia de los asuntos ESG,* 2020.
- KPMG. *Reporting en información no financiera: Recorriendo el camino,* 2020.
- KPMG. *The time has come - The KPMG Survey of Sustainability Reporting 2020,* 2020.
- MANAGEMENT SOLUTIONS. *La gestión de riesgos asociados al cambio climático,* 2020.
- SUSTAINABILITY ACCOUNTING STANDARDS BOARD. *ESG Integration Insights - 2020 Edition,* 2020.
- PRINCIPLES FOR RESPONSIBLE INVESTMENT. *Principles for Responsible Investment,* 2019.
- PRINCIPLES FOR SUSTAINABLE INSURANCE. *Underwriting environmental, social and governance risks in non-life insurance business,* 2019.
- SCIENCE BASED TARGETS. *Foundations for science-based net-zero target setting in the corporate sector,* 2020.
- TASK FORCE ON CLIMATE-RELATED FINANCIAL DISCLOSURES. *Recommendations of the Task Force on Climate-related Financial Disclosures,* 2017.
- THE INSTITUTE OF INTERNAL AUDITORS. *Internal Audit's Role in ESG reporting - White Paper,* 2021.
- THE INSTITUTE OF INTERNAL AUDITORS - AUSTRALIA. *The 20 Critical Questions Series: What Directors should ask about ESG,* 2020.
- UNITED NATIONS. *Sustainable Development Goals,* 2015.
- UNITED NATIONS DEVELOPMENT GROUP. *Guidelines to Support Country Reporting on the Sustainable Development Goals,* 2017.
- UNITED NATIONS GLOBAL COMPACT. *Integrating the Sustainable Development Goals into Corporate Reporting: A Practical Guide,* 2018.
- UNITED NATIONS HUMAN RIGHTS. *Guiding Principles on Business and Human Rights,* 2011.
- WORLD BUSINESS COUNCIL FOR SUSTAINABLE DEVELOPMENT. *Controlling Non-Financial Reporting,* 2013.
- WORLD ECONOMIC FORUM. *Measuring Stakeholder Capitalism - Towards Common Metrics and Consistent Reporting of Sustainable Value Creation,* 2020.
- WORLD ECONOMIC FORUM. *The Global Risks Report 2021*. 16th Edition, 2021

LA FÁBRICA

- INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA. LA FÁBRICA DE PENSAMIENTO. *Auditoría Interna y la Información no Financiera,* 2018.
- INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA. LA FÁBRICA DE PENSAMIENTO. *Auditoría Interna del proceso de inversión en tecnologías emergentes,* 2020.

RULES

- EUROPEAN CENTRAL BANK. *Guide on climate-related and environmental risks.* Frankfurt: ECB, 2020
- EUROPEAN COMMISSION. *Commission Delegated regulation supplementing Regulation (EU) 2020/852 of the European Parliament and of the Council by establishing the technical screening criteria for determining the conditions under which an economic activity qualifies as contributing substantially to climate change mitigation or climate change adaptation and for determining whether that economic activity causes no significant harm to any of the other environmental objectives.* Brussels: EC, 2021.
- EUROPEAN COMMISSION. *Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC.* Brussels, EC, 2013.
- EUROPEAN COMMISSION. *Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups.* Brussels, EC, 2014.
- EUROPEAN COMMISSION. *Guidelines on non-financial reporting (methodology for reporting non-financial information).* Brussels: EC, 2017
- EUROPEAN COMMISSION. *Guidelines on non-financial reporting: Guidelines on reporting climate-related information* Brussels: EC, 2019
- EUROPEAN COMMISSION. *Proposal for a Directive of the European Parliament and of the Council amending Directive 2013/34/EU, Directive 2004/109/EC, Directive 2006/43/EC and Regulation (EU) No 537/2014, as regards corporate sustainability reporting*. Brussels: EC, 2021
- EUROPEAN COMMISSION. *Regulation (EU) 2019/2088 of the European Parliament and of the Council of 27 November 2019 on sustainability-related disclosures in the financial services sector (Text with EEA relevance)* Brussels: EC, 2019
- COMISIÓN NACIONAL DEL MERCADO DE VALORES. *Código de buen gobierno de las sociedades cotizadas.* Madrid: CNMV, 2020.
- COMISIÓN NACIONAL DEL MERCADO DE VALORES. *Comunicado sobre la próxima aplicación del Reglamento 2019/2088 sobre divulgación de información relativa a sostenibilidad en el sector financiero.* Madrid: CNMV, 2021
- INTERNATIONAL FINANCIAL CORPORATION. *Norma de Desempeño 6 - Conservación de la biodiversidad y gestión sostenible de recursos naturales vivos.* Washington: IFC, 2012.
- EUROPEAN BANKING AUTHORITY. *EBA Discussion paper - on management and supervision of ESG risks for credit institutions and investment firms.* París: EBA, 2020.
- GLOBAL SUSTAINABILITY STANDARDS BOARD. *GRI Universal Standards.* Amsterdam: GSSB, 2020.
- GLOBAL SUSTAINABILITY STANDARDS BOARD. *GRI Universal Standards: GRI 101, GRI 102, and GRI 103 - Exposure draft.* Amsterdam: GSSB, 2020.

- *GOVERNMENT OF SPAIN. Ley 11/2018, de 28 de diciembre, por la que se modifica el Código de Comercio, el texto refundido de la Ley de Sociedades de Capital aprobado por el Real Decreto Legislativo 1/2010, de 2 de julio, y la Ley 22/2015, de 20 de julio, de Auditoría de Cuentas, en materia de información no financiera y diversidad.* Madrid: BOE, 2018.
- INSTITUTO DE CENSORES JURADOS DE CUENTAS DE ESPAÑA. *Guía de actuación sobre encargos de verificación del Estado de Información No Financiera.* Madrid: ICJCE, 2019.
- INTERNATIONAL AUDITING AND ASSURANCE STANDARDS BOARD. *NIEA 3000 (revisada) - Encargos de aseguramiento distintos de la auditoría o de la revisión de información financiera histórica, marco internacional de encargos de aseguramiento y las modificaciones de concordancia de otras NIEA.* New York: IAASB, 2018.
- INTERNATIONAL CORPORATE GOVERNANCE NETWORK. *ICGN Global Stewardship Principles.* London: ICGN, 2016.
- INTERNATIONAL INTEGRATED REPORTING COUNCIL. *International <IR> framework.* London: IIRC, 2021.
- ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS. *Líneas Directrices de la OCDE para Empresas Multinacionales.* París: OECD, 2011.
- ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS. *Principios de Gobierno Corporativo de la OCDE y del G20.* París: OECD, 2016.
- SUSTAINABILITY ACCOUNTING STANDARDS BOARD. *SASB Standards.* San Francisco: SASB, 2021.

JOURNAL ARTICLES

- PORTER, M.E. and KRAMER, M.R. «The Big Idea: Creating Shared Value. How to Reinvent Capitalism-and Unleash a Wave of Innovation and Growth». *Harvard Business Review.* January-February 2011, no, 89, p. 62- 77.
- SOH, D.S.B and MARTINOV-BENNIE, N. «Internal auditors' perceptions of their role in environmental, social and governance assurance and consulting». *Managerial Auditing Journal.* January 2015, Volume 30 – Book 1, p. 80-111.

ARTICLES IN NEWS BULLETINS, BLOGS AND OTHER SOURCES

- BONIME-BLANC, A. «It's time we added a letter to ESG. Here's why». *World Economic Forum* website. October 2020.
- BUSINESS ROUNDTABLE. «Statement on the Purpose of a Corporation». *Business Roundtable website.* August 2019
- CEINSA. «Hacia la integración de los ESG en las políticas de retribución». *Compensation lab* website. January 2021.
- CHAMBERS, R. U.S. SEC: «Environmental, Social, and Governance Risks Better Be on Your Radar». Internal Auditor's Blog. March 2021.
- FINK, L.D. «Propósito y Rentabilidad». *BlackRock* website. January 2019.
- FINK, L.D. «Un cambio estructural de las finanzas». *BlackRock* website. January 2020.
- GARRIDO, X. «La presencia de las métricas ESG en los salarios». *Social Investor* website. February 2021.
- GÓMEZ, M. «La supervisión de los asuntos ESG desde el consejo y sus comisiones». Website *KPMG Tendencias.* 2020.
- HERNÁNDEZ GUIJARRO, L. «Qué es un *proxy advisor* y su impacto en las sociedades cotizadas españolas». *Funds Society* website. January 2016.

- IONOS. «*Stakeholders* - ¿Conoces a los grupos de interés de tu empresa? *Ionos* website. February 2019.
- MONTECELOS, M. and CERVERA, M. «Métricas ESG: ¿es posible mejorar los resultados financieros de las compañías incluyéndolos en los sistemas retributivos?» *Willis Tower Watson* website. July 2020.
- PALÁ LAGUNA, R. «Nuevas obligaciones de transparencia para determinadas entidades financieras en materia de sostenibilidad: exigibilidad a partir del 10 de marzo de 2021». *Gómez-Acebo & Pombo* website. February 2021.
- PWC. «Integrar los criterios ESG y el propósito en la estrategia, principal reto de los Consejos de las empresas españolas en el mundo post-COVID». *Auditoría & CO* website. May 2020
- SCHRODERS. «Breve historia de la inversión responsable». *Schroders* website. November 2016.
- SCHWAB, K. «Manifiesto de Davos 2020: El propósito universal de las empresas en la Cuarta Revolución Industrial». *World Economic Forum* website. December 2019.
- THE DANISH INSTITUTE FOR HUMAN RIGHTS. «Sustainable Development through Human Rights Due Diligence (Road-testing version)». *The Danish Institute for Human Rights* website. 2018.
- UNITED NATIONS ENVIRONMENT PROGRAM. «About ecosystems» UNEP website. 2020.
- UNITED NATIONS ENVIRONMENT PROGRAM. «Water». UNEP website. 2020.
- VAÑÓ, P. «¿Están preparadas las entidades financieras para integrar los factores ESG en la toma de decisiones?» *KPMG Tendencias* website. 2020.
- VIVES, A. «Materialidad: 12 principios básicos y una metodología para la estrategia de RSE». *Ágora*. February 2015.

Instituto de Auditores Internos de España

Santa Cruz de Marcenado, 33 · 28015 Madrid · Tel.: 91 593 23 45 · Fax: 91 593 29 32 · www.auditoresinternos.es

Copyright: M-31844-2021
ISBN: 978-84-122588-7-5

Design and layout: desde cero, estudio gráfico

OTHER WORKS FROM LA FÁBRICA DE PENSAMIENTO

BUSINESS STRATEGY INTERNAL AUDIT

This document compiles the work of Internal Auditing in the definition and follow up of the company's strategy, It describes possible roles in business strategy, and provides a practical view of how to execute said roles in the different stages of the strategy process.

INTERNAL AUDIT AND RISK MANAGEMENT

Implementing a comprehensive management system that allows to adopt decisions in an agile and better informed way is key for company's success. This guide develops a mature model approach and unveils good practices for Internal Auditing to achieve a more active role in managing risks and ensuring correct segregation of its assurance and consulting activities.

OUTSOURCES INFORMATION INTERNAL AUDIT

Companies must ensure proper risk management resulting from access to outsourced information by third parties. This document compiles the main regulatory aspects to be considered, and recommendations regarding the role Internal Auditing must play in the outsourcing process, from the stage prior to hiring to the completion of services provision.

DATA GOVERNANCE INTERNAL AUDIT

It tackles existing problems and practical upgrades to solve them in terms of definition of good governance of data. Several aspects are thoroughly analyzed, from the data life cycle, including traceability and quality, to methodologies and regulations applicable to data governance. All the above form an Internal Audit standpoint.

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

This reference guide defines and develops fundamental concepts of each ESG (Environmental, Social, Governance) pillar in terms of strategy and governance, risk management, and reporting.

Furthermore, it addresses the auditing of ESG approaches, tests and indicators, resulting in a highly useful outline proposed to internal audits to shift the focus towards monitoring.

Instituto de Auditores Internos de España
The Institute of Internal Auditors