



"ENTERPRISE RISK MANAGEMENT" GUIDELINE

Document approved by the Board of Directors on 16 March 2022

INDEX

1	FUNDAMENTAL PRINCIPLES	3
2	SCOPE OF APPLICATION	4
3	RISK GOVERNANCE	4
4	ENTERPRISE RISK MANAGEMENT MODEL	6
4.1	Methodology and metrics	6
4.2	The Enterprise Risk Management process	8
4.3	Roles and responsibilities	9
5	RISK & CONTROL REGISTER	11
6	INFORMATION FLOWS AND REPORTING	11
6.1	Information flows	11
6.2	Reporting	12
7	COMMUNICATION AND TRAINING	13
8	RESPONSIBILITY FOR UPDATING	13

1 FUNDAMENTAL PRINCIPLES

Snam S.p.A. (hereinafter also the "**Company**") is one of the world's leading energy infrastructure companies and carries out its activities with the aim of promoting the energy transition towards the use of resources and energy sources compatible with environmental protection and progressive decarbonisation.

To this end, the Company conducts and organises its business with the aim of pursuing sustainable success through the creation of long-term value for the benefit of its shareholders (taking into account the interests of other relevant *stakeholders*) and considers the analysis, assessment and management of risks to be of primary importance for the achievement of its objectives.

Snam, therefore, undertakes to:

- promote and disseminate to all Snam people ethical values oriented towards a culture of correct and transparent risk management;
- ensure in all business processes, a proactive, effective and efficient risk management, as well as consistency with the strategies, group objectives and the *corporate governance* system;
- ensure, through adequate procedural, management and organisational systems, that risks and opportunities are effectively identified, assessed, managed, monitored and communicated through transparent reporting;
- conduct and manage all company activities with a view to risk prevention, in compliance with the law, the Code of Ethics, company regulations and national and international *best practices*;
- ensure that the identified risks, which are different in nature, are assessed using a homogeneous and transversal model that allows a complete, synthetic and unique representation of the whole;
- define the nature and level of risk compatible with the strategic objectives, taking into account all the elements that may be relevant for sustainable success;
- promote continuous improvement in line with the evolution of strategies, the external and internal context and the interests of its internal and external *stakeholders*.

In this context, this "*Enterprise Risk Management Guideline*" (the "**ERM Guideline**"), approved by the Board of Directors, describes the *enterprise risk management* model adopted by Snam (the "**ERM Model**") in line with the values set out above and is drafted in compliance with the architecture of Snam's Internal Control and Risk Management System ("**SCIGR**"), i.e. the set of rules, procedures and organisational structures aimed at effective and efficient risk management identification, measurement and monitoring of the main risks.

2 SCOPE OF APPLICATION

The ERM Guideline applies to Snam S.p.A. and to controlled companies as part of the management and coordination activity exercised by Snam itself, whether they operate in Italy or abroad. The

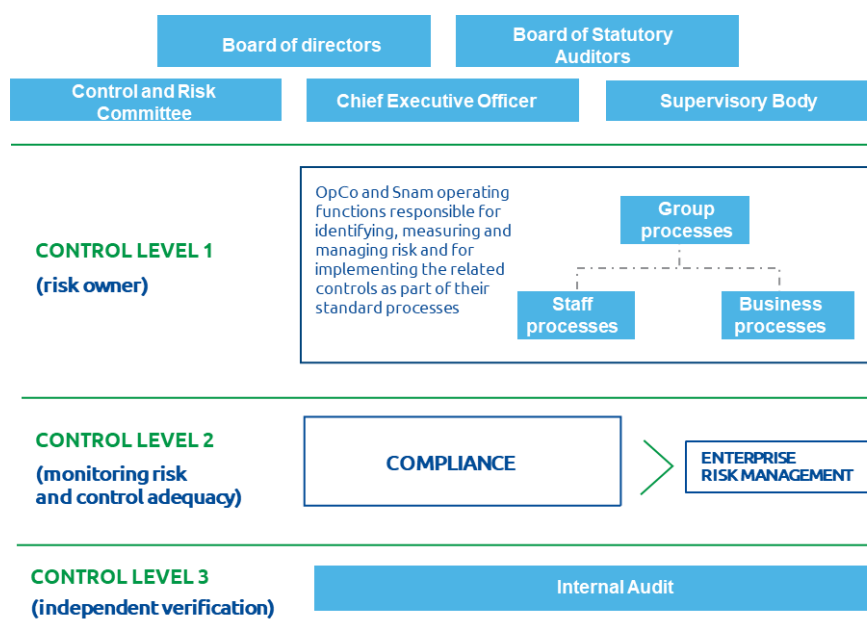
application is also intended to be extended to all corporate functions of all subsidiaries.

Snam shall use its influence, in a reasonable manner according to the circumstances, to ensure that Italian or foreign companies in which Snam's subsidiaries have a non-controlling interest meet the standards set out in this ERM Guideline.

3 RISK GOVERNANCE

The *governance* system outlined by the Board of Directors is based on cardinal principles such as the correct and transparent management of business activities ensured, amongst others, through (i) the definition of information flows between corporate bodies; (ii) an adequate and efficient SCIGR; (iii) the adoption - as part of the SCIGR and in accordance with the recommendations of the Corporate Governance Code - of an ERM Model that provides structured and uniform methodologies for identifying, assessing, managing and monitoring the main risks that could affect the achievement of Snam's strategic objectives.

The SCIGR provides for three levels of control and involves both corporate bodies and the entire organisational structure according to the scheme below.



In particular, without prejudice to the responsibilities of the 1st and 2nd level control functions described with specific reference to the ERM Model in paragraph 4.3 below:

- (i) the Board of Directors:
- within the framework of the preparation of the Snam Group's Strategic Plan, defines the nature and level of risk compatible with Snam's strategic objectives¹, including in its assessments all risks that may become relevant in the pursuit of the medium- to long-term sustainability of Snam's business;
 - defines, subject to the opinion of the Control and Risk and Related Party Transactions Committee, the guidelines of the SCIGR, so as to ensure the identification, measurement, management and

¹ This is also based on the risk mapping carried out within the framework of the ERM model and the risk *analysis* carried out on risks with an impact on the plan (the "**Strategic Plan Risks**").

monitoring of the main risks of Snam and its subsidiaries, also determining the degree of compatibility of these risks with the management of the Company and the Group in line with the identified strategic objectives, also including in its assessments all elements that may be relevant to the sustainable success of the Company;

- assesses, at least once a year, after the opinion of the Control and Risk and Related Party Transactions Committee, the adequacy of the SCIGR with respect to the characteristics of the Company and the Group and the risk profile assumed, as well as its effectiveness;
 - approves, at least once a year, the Audit Plan - prepared by the Head of the Internal Audit Function, also on the basis of the risk mapping provided by the ERM Function - subject to the opinion of the Control and Risk Committee and Transactions with Related Parties and after the opinion of the Chairman of the Board of Directors, the CEO and the Board of Statutory Auditors;
- (ii) the CEO acts as a director in charge of the SCIGR ("**Appointed Director**");
- (iii) the Control and Risk and Related Party Transactions Committee:
- supports the evaluations and decisions of the Board of Directors concerning the SCIGR;
 - supports the Board of Directors in defining the guidelines of the internal control and risk management system in line with the Company's strategies - including, in coordination with the ESG Committee, the risks that are important from a sustainability point of view, also for the purpose of non-financial reporting, concerning the Company and its subsidiaries in such a way that they are correctly identified, as well as adequately measured, managed and monitored, and in determining the compatibility of such risks with a management that is consistent with the identified strategic objectives;
 - examines the content of periodic non-financial information relevant to the SCIGR;
 - expresses opinions on specific aspects relating to the identification of the main corporate risks and supports the Board of Directors' evaluations and decisions relating to the management of risks arising from prejudicial events of which the Board of Directors has become aware;
- (iv) the Board of Statutory Auditors, also in its capacity as the "*internal control and audit committee*" pursuant to Legislative Decree no. 231/2001. 39/2010, monitors the effectiveness of the SCIGR;
- (v) the Head of the *Internal Audit* Function verifies, both on an ongoing basis and in relation to specific needs, the operation and suitability of the SCIGR, through the Audit Plan based on a structured process of analysis and prioritisation of the main risks.

The SCIGR will be subject, over time, to checks and updates to ensure that it shall always remain suitable to monitor the main areas of risk of the company's activities. In this context, and in order to fully implement the provisions of the Corporate Governance Code, Snam has adopted the ERM Model.

4 ENTERPRISE RISK MANAGEMENT MODEL

Snam has defined its ERM Model in accordance with corporate values and in line with reference models and international *best practices on risk management* (i.e. the international standard ISO 31000 "*Risk Management Guidelines*", the "*CoSO Enterprise Risk Management Framework - Integrating with Strategy and Performance*" and, with reference to ESG-related risks, the "*CoSO ERM WBCSD* -

Applying enterprise risk management to environmental, social and governance-related risks") and with the recommendations of the Corporate Governance Code.

The ERM model provides for an integrated, transversal and dynamic assessment of risks and opportunities that enhances the management systems already in place in individual business processes, and that will be subject to periodic updates in order to guarantee the continuity of an efficient and effective model.

The ERM Function, which is provided with adequate professionalism and resources necessary for the performance of its tasks, ensures the definition and updating of the ERM Model.

4.1 Methodology and metrics

Risk is defined as the possibility that an event occurs carrying a negative (threat) or positive (opportunity) impact on the achievement of the company's objectives; whereas the event is defined as a fact or change in a set of circumstances, resulting from one or more causes, with positive or negative repercussions on the organisation.

Risks and opportunities are assessed as a result of:

- **probability:** representing the possibility of an event occurring or the frequency with which an event may occur in a given time frame, and
- **impact:** representing the overall *magnitude* of the event in relation to the pursuit of corporate objectives.

In particular, probability is assessed according to two alternative metrics, articulated on four levels:

- a 'qualitative' one, using percentage thresholds of occurrence of the event
- a "quantitative" one, that measures the recurrence of the event over the plan period.

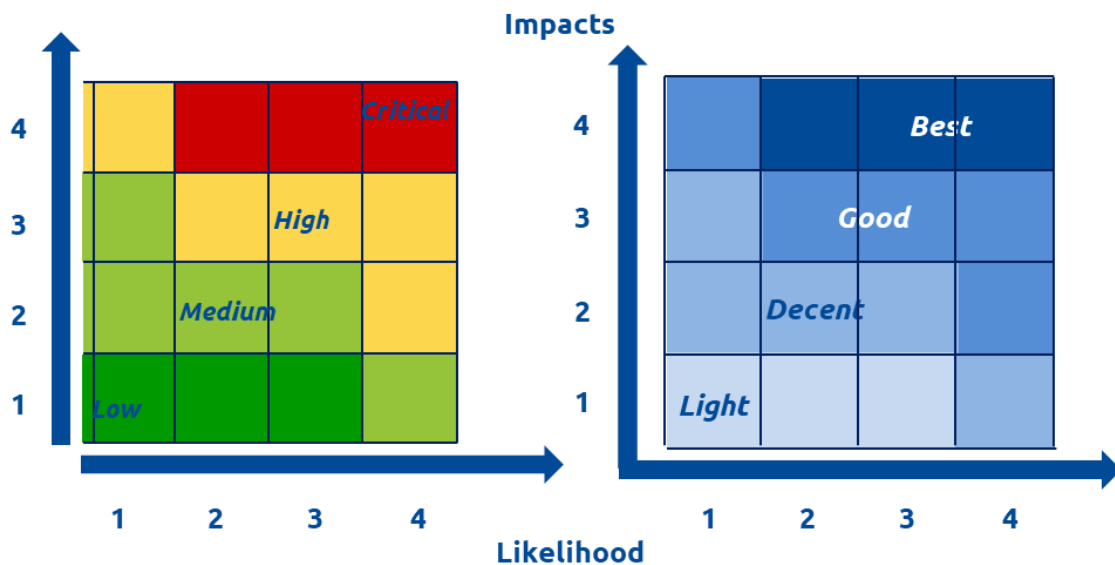
The valorisation of the impact of events takes place according to differentiated technical measurements with respect to the type of effect/consequence of the event. Specifically, various impacts are measured using metrics that are also divided into 4 levels:

- **operational:** Industrial/Business; Economic/Financial and Assets
- **specialists:** Legal; *Health & Safety*; Reputational; Market; *Environment*; *Social and Governance*².

The combination of the level of probability and the greatest impact among those measured defines the level of relevance of the risk/opportunity itself (so-called priority) as represented in the matrices below³.

² In particular, the "*Environment*" metric considers environmental and climate change impacts; the "*Social*" metric considers possible impacts on human and workers' rights, as well as on local communities; the "*Governance*" metric intercepts possible consequences on governance capacity, on the pursuit of sustainable success and on *corporate behaviour* (e.g. *Business Ethics*, *Anti-corruption*, *Tax Transparency*).

³ With particular reference to "non-regulated businesses", the ERM model provides *ad hoc* assessment metrics for risks and opportunities at the level of individual companies or business lines, with qualitative and quantitative parameters that are more in line with the specific characteristics of these businesses. Appropriate criteria for converting valuations allow those risks/opportunities identified at the level of individual entities/business lines that are relevant to the achievement of Snam's objectives to be brought back to group level.



A further third dimension emphasised is that of '*velocity*', namely the speed with which the impact of risk or opportunity can show up. *Velocity* allows, with particular reference to risks with **ESG** relevance ("**ESG risks**"), to take into account events with impacts that may emerge over e three different time horizons – short, medium and long term – and to prioritise specific analyses and monitoring activities.

Metrics for measuring the probability, impact and *velocity* of events can be found in the document "*ERM Operating Model and Tools*". The ERM Function updates the metrics with the relevant structures in line with Snam's *risk appetite*⁴ and makes an extract of the document "*ERM Operating Model and Tools*" available in a special section of the corporate intranet. The update of the document is submitted to the CEO⁵ and the General Counsel.

4.2 The Enterprise Risk Management process

The ERM Model is part of Snam's *Integrated Risk Assurance & Compliance* ("**RACI**") system, which is based on the coordination and collaboration of the various so-called second-level control models of the SCIGR, aimed at maximising the availability of skills and resources, reducing inefficiencies and overlaps, and providing uniform and complete information to support decision-making processes.

The synergies between the various control models adopted by Snam are achieved operationally through the "*Integrated Risk Assurance & Compliance*" IT platform (the "**RACI Platform**")⁶ used for the coordinated performance of risk identification and assessment and control activities within periodic time windows, known as *assessment* and/or *monitoring* "**campaigns**".

In this context, the ERM process represents the set of activities aimed at fostering the identification of risks, in a dynamic, effective and complete manner with respect to all business processes and at guaranteeing the homogeneity of risk identification and prioritisation through a uniform methodology for the group that takes into account the specificities and complexities of the various businesses.

⁴ Roles, responsibilities and methodology for defining *risk appetite* are described in the document "*ERM Operating Model and Tools*".

⁵ As Administrator in Charge

⁶ The RACI platform is implemented in order to coordinate the risk assessment and management activities carried out as part of the SCIGR 2nd level control models within the RACI system described in the "*Risk Assurance and Integrated Compliance*" Guideline approved by the Snam Board of Directors.

The ERM process consists of the following steps:



1. **Risk Identification:** identification of risks and opportunities starting from business processes, from an analysis of the external and internal context and from the objectives outlined in the company's strategic plan;
2. **Risk Measurement & Treatment:** assessment of risks and opportunities, in terms of probability of occurrence and impact, and consequent definition of related management strategies;
3. **Monitoring:** periodic monitoring of the risk/opportunity management measures to be approved or implemented through, where applicable, some identified indicators;
4. **Reporting:** release of differentiated reports according to the recipients (*top management*, corporate bodies, etc.).

The assessment of all risks and opportunities must be undertaken at least annually (*annual risk profile assessment*). Critical and high priority risks are to be assessed at least every six months (*interim top risk assessment*). Specific monitoring activities are also envisaged for top risks and opportunities.

Finally, *ad hoc risk assessments* may be carried out on particular risks or risk categories (e.g., new emerging risks), on the basis of indications from Snam's control and supervisory bodies or on reports from RS/ROs.

4.3 Roles and responsibilities

The ERM process provides for a clear identification and accountability of the persons involved in the above mentioned activities with a corresponding segregation of duties and formalisation of responsibilities.

In particular, the various heads of corporate functions/units are involved in their capacity as Risk Owner ("RO"), Risk Specialist ("RS") and Risk Impact Specialist ("RIS") and the Risk Model Owner ("RMO"); all perform the respective activities indicated below by accessing the appropriate sections of the RACI Platform with a dedicated profile.

Normally, RS are the 2nd level reports for Snam and the 1st level reports for subsidiaries, RIS are the representatives of the specialised function that measures the impact of risks/opportunities according to the aspects under their responsibility, and RO are the 1st level managers for Snam and the *Managing Directors* of the subsidiaries.

The role of RMO is performed by the ERM function, which plans, coordinates and prepares the activities to be carried out during the "campaigns"; provides specialist methodological support to RS and RO in identifying and assessing risks and opportunities; and ensures the coordination of the process as a whole.

Below is a detail of the activities foreseen for each of the phases of the Risk Management Process.

4.3.1 Risk Identification and Risk Measurement & Treatment

In coordination with the Strategic Planning and ESG functions, the ERM function carries out a cyclical context analysis in preparation for the *Risk Identification* phase. In particular, *the main drivers of change* in the external context (e.g. macroeconomic factors, regulatory developments, *business* development, *stakeholder* expectations, *mega-trends*) and in the internal context (Strategic Plan objectives, materiality analysis and stakeholder engagement, ESG objectives, new significant events in Snam's management) that could affect Snam's risk profile in the medium and long term (including beyond the plan horizon) are analysed from a *risk-based* perspective. The analysis is carried out by integrating external views and internal views collected also through specific meetings with Snam management.

The results of this analysis are made available to RS and ROs to support *Risk Identification*. During the *Risk Identification and Risk Measurement & Treatment* phases:

- the RS (i) identifies the risks/opportunities within the scope of the processes for which it is responsible, (ii) proposes, for the events identified, the measurement of the probability of occurrence and the 3 so-called impacts. "operational" (industrial/business, economic/financial and *asset*); (iii) identifies/integrates the strategy and the risk/opportunity management measures (the latter divided into "actions/controls in place" and "specific interventions") and any implementation plans and (iv) defines and updates the **key indicators** for risk *monitoring* activities;
- the RIS (i) assesses the relevant specialist impacts (e.g. legal, HS, *social*, reputational and market) for all identified risks/opportunities;
- the RO verifies and validates (i) the identification of the risks identified by the RS of its area, (ii) the proposed actions, and (iii) the assessment of likelihood and impacts carried out by the RS and RIS.

4.3.2 Monitoring

The risk and opportunity monitoring activity aims at providing dynamic information on the trend of the main events through the updating of management measures (i.e. progress/completion of specific interventions and/or confirmation/update of actions/controls in place) and the *trend* analysis of *key indicators* (where applicable)⁷.

⁷ *Key Indicators* can be related to: risk/opportunity events, causes or impacts (*Key Risk/Opportunity Indicator*); objectives related to risk/opportunity events (*Key Performance Indicator*); actions/controls to treat/mitigate risk events (*Key Control Indicator*). In order to enhance synergies at all levels of the organisation and between the businesses, the definition of *Key*

As part of the 'campaigns', RS update *key indicators* (noting their value) and management measures while RO verify and validate the updates made by RS.

4.3.3 Reporting

The ERM Function guarantees, at the end of each *assessment or monitoring* campaign, the preparation of reports addressed to the various *stakeholders* (see paragraph 6.2 below) extracting data and information available in the RACI platform (*i.e.* *assessment* results, analysis of the *trend of risks* and *key indicators*, progress of the management action plan, etc.).

The results of the ERM process also contribute to financial reporting.

5 RISK & CONTROL REGISTER

The RACI platform enables the creation and updating of an integrated database in which the ERM model and the other 2nd level control models share a single catalogue of risks and controls. ("**Risk & Control Register**").

The ERM function is responsible for recording and updating the data necessary for carrying out *risk assessment and/or monitoring activities* and verifies the upload of the data and results of these activities onto the RACI platform.

6 INFORMATION FLOWS AND REPORTING

The ERM function handles the following information and reporting flows.

6.1 Information flows

Strategic Plan Risks

As part of the process of defining the Strategic Plan, the ERM, Strategic Planning and P&C functions (through the controllers of the various business lines) compare risks with an impact on the plan ("Strategic Plan Risks") and ERM risks and their respective assessments/analyses in order to represent risks in a consistent manner with respect to the strategic objectives.

The Strategic Planning Function performs a quantitative analysis of the Strategic Plan Risks (each of which is associated with an ERM risk) through Monte Carlo simulations and "*What if*" scenarios and the ERM Function assesses the consistency between the outcomes of the Strategic Planning assessments and the risk prioritisation carried out by the RS and RO.

Strategic Plan Risk data, associated with the respective ERM risks, are made available to RO on the RACI platform to support ERM risk assessments.

The Strategic Plan Risks are included in the *Risk & Control Register*.

Financial risks

The ERM Function receives periodic information from the Finance Function on the management and assessment of financial risks, including in the context of the periodic *assessments* provided for in the

Indicators is carried out by resorting, where possible, to the selection of indicators already used in the context of RO/RS activities.

ERM Model on the same risks.

ESG risks

In order to ensure and improve over time the integration and coherence between the ERM framework and ESG issues, periodic information flows with the ESG Function are foreseen (e.g. related to the mapping of material issues and the ESG scorecard) also for the purpose of preparing institutional reporting and ESG risk reporting for the ESG Committee.

Audit Plan

The *Internal Audit* Function receives the periodic reports prepared by the ERM Function and through the RACI Platform has direct access to the results of the *risk assessments* carried out also for the purpose of drawing up the Audit Plan.

The ERM Function receives the audit reports and assesses with the *Internal Audit* Function the possible identification of new risks to be proposed to the RS within the first useful *risk assessment* "campaign".

6.2 Reporting

The ERM function handles the following reporting activities:

- during each *risk assessment* and/or *monitoring* 'campaign':
 - prepares a report on the results of the activities carried out and any updates to the risk/opportunity mapping to the CEO, the CFO, Officer responsible for the preparation of financial reports, the General Counsel and the SVP Internal Audit;
 - illustrates and submits the above findings and updates to the Audit and Risk Committee, and Related Party Transactions and to the Board of Statutory Auditors in order to allow for the assessments of competence regarding the effectiveness of the SCIGR;
- pursuant to Model 231, on at least a half-yearly basis, meets the Supervisory Board in order to examine the state of implementation of the process of identifying, measuring, managing and monitoring risks;
- on at least an annual basis, submits a report on ESG risks to the ESG Committee;
- on an annual basis, reports to the Snam Board of Directors on the activities carried out, the mapping of risks and opportunities and the implementation of the ERM Guideline.

RS, RIS and RO access reporting on the risks and opportunities mapped in their areas via the RACI Platform. Regular in-depth meetings with the ERM function are also planned.

7 COMMUNICATION AND TRAINING

The implementation of the ERM model is a process that involves the entire management and is carried out in a dynamic and interactive manner through the assignment of specific responsibilities, and related segregation of duties, aimed at the proper definition and functioning of the model itself.

In order to create a full awareness of roles and responsibilities, enabling everyone to contribute adequately to the proper implementation of the ERM model and its improvement, communication and training activities are foreseen according to the purposes and characteristics of the model as well as on the risk assessment methodology.

The ERM function promotes the above-mentioned communication and training activities in cooperation with the Human Resources function.

8 RESPONSIBILITY FOR UPDATING

The ERM function periodically reviews this Guideline to ensure its effectiveness over time and its alignment with emerging *best practices*. Where necessary, it identifies possible revisions or additions and informs the General Counsel and the Organisation Function.

All business units/positions involved in the process described in this Guideline remain responsible, to the extent of their competence, for detecting any business events that entail the need for an adaptation of the ERM Guideline and for reporting them to the ERM Function and the Organisation Function, which ensure the coordination of the activities for updating the Guideline.