ENTERPRICE RISK MANAGEMENT POLICY

GROUP ERM DIVISION

ENTRY INTO FORCE : 28.08.2023

DOCUMENT CODE : GR.ELL.ERM.PL.RSKP.v2-2023/08

TABLE OF CONTENTS

1. INTRODUCTION

Intense volatility at international level and increased regulatory requirements have led all business entities to adopt advanced risk management functions. Enterprise Risk Management (ERM) is nowadays a key competitive advantage of all modern businesses and is considered a prerequisite for continuity and sustainability.

Every business has to deal with a multitude of ever-changing risks at strategic, economic, geopolitical, regulatory and operational levels, turning threats into opportunities. ERM encompasses all strategic pillars of a business, monitors their day-to-day activity, operates proactively in detecting and identifying risks, assessing and managing them - so that their eventual occurrence comes with the least possible consequence/impact on the company objectives.

Entrepreneurship by definition implies risk-taking, thus risk management assists management in decision-making, providing answers to uncertainty and at the same time trying to prevent future surprises in the smooth development of the company – to the extent possible and given, of course, that reality often exceeds imagination!

The generally applicable market trends are crystallized below:

- government decisions for more complex specifications and increasing regulatory requirements, with pressing adjustment times
- clients, partners and shareholders opt for companies with evident, clear and transparent ERM management frameworks
- increased complexity of financial products and instruments
- development and establishment of risk management procedures which shall contribute to optimal decision-making by the management with acceptable risk-taking, facilitate strategic planning and promote continuous improvement of control mechanisms and supporting structures to spread risk, limit undesirable outcomes and sudden events, ensuring the smooth operation of the company's individual units, ensuring seamless attainment of its objectives
- special emphasis and interest on issues related to environmental risks, sustainable development and transition to a circular economy.

The Group has recognized the need to implement a risk management system and aims to make risk management an integral part of the daily activities of all personnel members. The creation of a uniform culture for managing enterprise risks is an ongoing, systematic and long-term process. ERM must be a concern of all personnel and management members, aspiring to raise awareness and ensure prevention.

2. PURPOSE

This POLICY aims to establish the foundations of the general framework, as well as the norms and functions required for effective risk management, a process actually calling for team work regardless of hierarchy. The overall effort is further supported by both individual contributions and

cooperation between different operational units, in order to provide such means, information and material necessary for achieving the specific objectives of risk management, summarized as follows:

- efficiency and effectiveness of risk management functions
- attaining qualitative and quantitative targets safely, avoiding surprises (unexpected outcomes)
- reliability of financial and non-financial reporting and safeguarding going concern
- compliance with the applicable legal and institutional framework.

More specifically, enterprise risk management protects and adds value to the Group and its stakeholders through the support of its objectives by:

- providing a framework within which the Group's business activity is carried out in a stable and controlled manner;
- improving decision-making, planning and priority setting through broad and well-structured understanding of each sub-activity of the group, the volatility / uncertainty involved and the opportunities or threats of each project or decision;
- contributing to a more efficient use / allocation of the Group's capital and resources in general;
- reducing volatility in non-core business areas;
- protecting and improving the assets and profile of the Group;
- developing and supporting human resources and accumulated knowledge and experience within the Group;
- optimizing operational efficiency;
- developing the Group's resilience and adaptability.

3. INSTITUTIONAL FRAMEWORK

In order to ensure transparent, safe and credible operation of businesses, the Greek legislation has adopted EU and Council directives and provisions, such as directives (EU) 2017/828 & 2017/1131.

This framework defines that the Internal Control System (ICS) consists of all internal control mechanisms and procedures, including risk management function, internal control /audit and compliance, which cover, on a continuous basis, every group's activity and contribute to the company's safe and effective operation (Law no. 4706/2020 article 2 par. 7).

More specifically, the Board of Directors (BoD) sets and monitors the implementation of the Corporate Governance System (CGS), which includes the Internal Control System (ICS), safeguarding its proper and effective operation, which, in its turn, aims at the below key objectives: a) consistent implementation of the business strategy by using all available resources efficiently, b) identification and management of material risks pertaining to business activity and operation, c) effective operation of the internal control unit, d) ensuring completeness and reliability of the data and information required for the accurate and prompt determination of the company's financial

and non-financial position, as well as for the preparation of reliable financial statements, (as article 151, Law no. 4548/2018) and e) compliance with the regulatory and legislative framework, along with the internal regulations governing the company's operation (article 4 par.1 & 2, Law no. 4706/2020).

It should be specifically noted (Law no. 4706/2020 article 4 par. 3) that the company's BoD further ensures that the ICS functions, i.e. internal control, risk management and compliance, apply independently of the business sections they control, and that they have the appropriate financial and human resources, as well as the authority and competence for their effective operation, as dictated by their role. Reporting lines and distribution of responsibilities are clear, enforceable and properly substantiated.

The Group has been fully aligned with the above-mentioned applicable institutional framework and abides by the relevant directives.

4. DEFINITIONS

Hazard / Risk

It is generally defined as any event that may involve uncertainty as to the attainment of an organization's objectives or which may result in any deviation from the expected results. Any and all activities may have the potential for events and consequences that represent opportunities for benefit (upside) or threats to success (downside).

Note the distinction between the concepts of hazard, hazard source and risk.

Hazard is by definition a negative event, both in terms of its nature and by what it may entail, i.e. a situation which, when it occurs, causes damage/interruption/interference in a company process or activity.

Hazard source is defined as the inherent ability of an element to cause a hazard, that is an event / fact(s) with a negative outcome.

Risk is defined as exposure to hazard and is a characteristic of an event that entails uncertainty, i.e. it can have either a positive or a negative outcome - hence results / consequences. What organizations are more concerned about is the degree of risk, i.e. their exposure to hazard, characterized by / stemming from facts / events that arise from or are strategically eligible by the company itself within the spectrum of its activities.

Risk can be measured by the degree of likelihood of a negative outcome and the magnitude of the consequence it can potentially bring about.

It is noted that in everyday life, the concepts of risk and hazard are identical (English terminology correctly uses the term "risk"). In other words, a reference to Enterprise Risk Management (ERM) refers to the management of business risks (exposure to hazard), willful and/or unintentional.

Enterprise risks can be classified – depending on their source - as follows:

- *External risks*

refer to all kinds of threats from the environment in which the company / business entity operates and any third party involved therein; they may be related to institutional / legal framework and relative obligations, market and country conditions, productive resources (capital and labor), natural environment, information, etc.

- *Internal risks*

refer to threats deriving from the nature of company's activities (inherent risk), strategic objectives, IT processes, systems and applications, human resources and other productive factors, quality of information for decision-making, assets, etc.

It should be noted that there can be risks with dual origin, i.e. from the external and the internal business environment.

Enterprise Risk Management (ERM)

Enterprise risk management is the process under which businesses approach the risks associated with their activities in a methodical and structured way, aiming to achieve sustainable benefit in all activity sections and over their entire business portfolio. It is the process through which the probability of success is increased, while at the same time, the probability of failure and uncertainty of achieving the Group's overall objectives are reduced.

It is an ongoing, consistent, evolving and continuously developing process that runs through the Group's strategy and its implementation. It methodically addresses risks relating to the Group's past, current and future activities and is embedded in the corporate culture.

Risk management is a recurrent process that gives both directions and controls. It consists of sequential steps which, when done, contribute to the continuous improvement of day-to-day decision-making at all hierarchical levels. It is the logical and systematic method of identifying, analyzing, assessing, managing, monitoring and communicating the risks associated with all activities, functions or processes and it somehow encourages organizations to minimize losses and maximize benefits.

Risk Management Framework (RMF)

It refers to all commitments, responsibilities, organizational structures and arrangements, authorities / tasks, processes, procedures, functions, series of actions, sequence of activities, tools and systems which are the ingredients for achieving the planning, establishment, monitoring, reviewing and continuous development and improvement of how an organization shall manage its business risks.

An important component of the framework is the entire personnel of the organization, regardless of hierarchy, as well as the degree of their familiarity, cognitive training and awareness with the subject of business risks.

Risk attitude / Risk appetite

Each company defines the profile it adopts against the risks it encounters. It delineates its disposition towards the risks it faces and the management of those risks, such as avoidance - deterrence, conservation - retention, transformation - mitigation, transfer or even selective pursuit thereof. The company, as part of its corporate governance, defines its risk tolerance /resistance limits, in consistency with its activities and business profile, determining the desirable range of risk it is willing to undertake in correlation to its risk appetite, setting, in parallel, its risk thresholds per risk category when imposed by the applicable circumstances.

Risk Owner

This is a person who administratively belongs to an operational unit of the company, is well aware of all operations and activities of the unit he/she belongs to and is in charge of the risks within the area of his/her responsibility. He/she shall operate as a point of reference with the Risk Management Division and work as a liaison for information gathering and transfer of know-how to his/her unit. He/she also has the patness and accountability and a to report to the Risk Management Division for timely and accurate information purposes and for implementing the risk action plan of his/her unit, when required so.

Risk Assessment

It refers to the overall process that consists of risk identification, risk analysis and risk evaluation.

Event

It is one or more related occurrences happening under specific circumstances which involve uncertainty and may therefore constitute a threat or an opportunity. An event may have multiple causes (multiple risk sources). Failure to materialize an expected action or situation is also considered as an event. An event can also be anything mentioned as an incident, an accident and, since it has no consequences, be recorded as a near miss, near hit or close call.

Consequence

It is defined as the result that an event may bring about on the organization's objectives. Consequence can be defined as single and specific or as a range. It can be classified as certain or uncertain, with a positive or negative impact on objectives and it can be expressed qualitatively or quantitatively. The initial consequences of an event can escalate and upgrade through interaction (cascading and cumulative) of effects.

The above definitions are fully aligned with risk management standard guidelines (IRM, AIRMIC, "A Risk Management Standard" 2007 & ISO 31000:2009).

5. CORE PRINCIPLES

Pursuant to the standards AS/NZ 4360: 2004 & ISO 31000:2009 & ISO/IEC Guide 73, effective enterprise risk management must satisfy the below ***fundamental characteristics***:

It is primarily of a preventive nature and secondarily of a deterrent - management nature.

Its efficiency relates to the level of timely and prompt risk response.

It combines sectors & objectives: strategic, economic, geopolitical, regulatory, operational, etc.

It creates and protects value, assets, etc.

It is an integral part of all organizational processes.

It is part of the decision-making and a criterion for considering any alternative solutions / treatments.

It explicitly addresses and limits uncertainty, unpleasant surprises and sudden conditions.

It operates in a systematic, structured and timely manner, contributing to the enhancement of the organization, generating stable, consistent, comparable and credible financial results.

It uses/is based on full and credible information.

It is fully tailored in terms of size, nature, range, complexity of the organization's operations, fully serving and supporting its business profile.

It takes human and cultural factors into account.

It is fully transparent and independent.

It is inclusive, i.e. dynamic, intervening and directly responsive to changes; it thus may adequately identify changes at a primary level and promptly respond (proactive)

It promotes, accelerates continual improvement and enhancement of risk management in all aspects of the organization.

It is a fundamental factor for the continuity and sustainability of the company and prepares it for successfully dealing with crisis.

It minds for the integration into the organization processes of points of control for deterring, avoiding or limiting the risks, mostly of operational risks throughout the organization's activities.

In addition, indicatively and not restrictively, risk management ***entails the below processes:***

Risk analysis

Risk analysis involves the identification, description, evaluation and determination of a risk. In particular, risk identification aims to identify the organization's exposure to uncertainty and to determine the associated risk by activity and for all of the organization's activities and decisions, which could be classified as strategic, operational, financial, related to knowledge & information management, and related to compliance. The objective of risk description is to display identified risks in a structured and usable form, for example to indicate the risk's field of occurrence and nature, as well as its potential link to a function or an event. Risk evaluation may be a quantitative and qualitative approach, suggesting the probability of occurrence of the event and its positive or negative outcome, with reference to its results or consequences. Such evaluation must fully adapt to the needs of the Group, i.e. considering the inherent risks resulting from the nature of its activities. The result of identification, description and evaluation processes shapes the general characteristics of each risk, further determining a degree of importance for each risk, which can be used as a tool for setting priorities in the handling / management thereof.

Risk Assessment

When the risk analysis process has been completed, it is necessary to compare the evaluated risks against the risk acceptance or non-acceptance criteria that the organization has chosen to apply. The above criteria are influenced by the relative costs and benefits of accepting risks, legal requirements, socio-economic and environmental factors, stakeholders' concerns, etc. Risk assessment is therefore about making decisions as to the significance of risks to the organization and whether each particular risk should be accepted or considered eligible or treated in a particular way (risk response).

Risk Reporting and Communication

Reporting and communication of risks is either internal or external.

1. Internal

Different hierarchical and operational levels within an organization need different information with regard to business risk. In particular, the Board of Directors (BoD), by continuously ensuring and confirming the effective and independent operation of risk management function, has at its disposal reliable data on business risks and can review the Risk Management Policy in the most appropriate way, preparing the organization and making it capable and resilient in dealing with and managing crises. The BoD focuses on the most significant risks faced by the organization and their potential impact, as well as how to manage them, and decides on the risks to be taken and how to manage this decision in relation to the associated parties.

The Business Units, are informed and aware of the risks that fall within their area of responsibility, monitor them according to the defined action plans drawn-up by the Risk Management Division, proceed to the implementation and report on events that diversify analysis of existing risks or identify new risks. Risk owners understand their accountability for individual risks of their responsibility, along with their obligation to respond to the management processes - in a context not of simple implementation of actions, but of a critical and creative approach, fully aligned with the organization's global culture of risk awareness and activation.

2. External

The organization, within the framework of the corporate governance it adopts, must inform the stakeholders about its risk management policy and attainment of the specific objectives set during its implementation. It is stressed that there is an increasing need for information on the effective management of the organization's performance on non-financial issues in areas such as community relations, human rights, labor practices, health & safety and the environment. The organization informs - as it should - that the BoD, while executing their duties, ensures that the Internal Control System is fully operational and performs satisfactorily and that risk management reporting is accurate and complete and any deficiencies / weaknesses identified by the system or in the system per se are highlighted, whereas specific corrective / improvement actions are immediately initiated to address them.

Risk Management

Risk management is the process of selecting and implementing measures to respond to a risk in order to modify it. Risk handling includes risk avoidance / deterrence, risk control / reduction / mitigation, risk transfer and risk financing (according to this standard, it refers to specialized insurance programs and does not mean providing funds to cover the management costs of risk - ISO/IEC Guide 73, page 17).

The risk analysis process highlights the prioritization of risks to be managed. The organization prioritizes risk management actions based on their possibility to maximize the organization's benefit. Effectiveness of internal control measures is the degree to which the risk will either be

eliminated or reduced by the proposed measures. The cost of risk handling shall be estimated on the basis of the expected benefits of risk reduction and the potential financial impact if no handling actions are taken at all. With regard to compliance risk, it is noted that compliance with laws and regulations is not an option but an obligation, so the relative risk treatment is differentiated. The organization is well-aware of and understands the applicable laws and applies a system of control measures to achieve compliance, a process that the Compliance Division is in charge of.

It should be noted that the organization should also be prepared to assume risks which are not transferable or insurable, such as environmental occurrences, which may morally damage employees or adversely affect the organization's reputation and which the organization may generally classify in its general crisis management procedures.

Risk Monitoring

Effective risk management requires thorough monitoring and review in order to ensure that risks are effectively identified and assessed and that appropriate control measures and responses are in place. The Internal Control Division, through its controls, shall support successful risk monitoring. Effective monitoring should aim to identify changes that take place within the organisation and the environment it operates in a timely manner so that appropriate adjustments to processes may be implemented promptly. The risk monitoring process determines whether and to what extent :

- *the measures adopted for risk handling were effective (i.e. resulted in what was intended/aimed)*
- *the procedures adopted for the risk management function were appropriate for the organization, promptly competent and full*
- *risk management culture in combination with improved knowledge derived from ongoing risk monitoring have helped in reaching better decisions, while in parallel whether the organization has optimized its ability to deal with crisis, as a result of the experienced so far gained.*

It becomes clear that the organization establishes risk management as a responsibility undertaken by all employees, regardless of role and hierarchy, because achievement of its objectives is every single employee's responsibility and goal. The company top management shall ensure that the Risk Management Division shall operate independently and be adequately staffed, providing the necessary resources for developing internal structures, systems and/or training activities, which shall enable it to operate more effectively.

It should be noted that within the framework of the Internal Control System, Internal Control Division shall support Risk Management Division through its controls, focusing on high-risk functional areas, ensuring / confirming the implementation of actions indicated by the Risk Management Division, detecting new risks and specifically identifying operational risks resulting from procedural gaps or weaknesses.

Risk management as a function is integrated and embedded in the procedures and manuals of all group's activities, such as strategy, various projects, product & service activities, training, staff development & appraisal, principles - values - corporate culture, individual and general goals. Also, all operational processes of the organization contain a number of control points which constitute the first line of defense against risks, whereas the second line of defense is Risk Management, with the Internal Control being the third line of defense.

6. OPERATION OF THE RISK MANAGEMENT DIVISION

As statutorily defined and the present organizational chart, the Group's Risk Management Division reports (operationally) to the Chief Executive Officer and to the Board of Directors by him. The CEO assesses annually the effectiveness of Risk Management Division.

Its duties and responsibilities include, at a minimum, the following:

- Define a Risk Management Policy, which shall be brought for approval to the Group's CEO;
- Establish Risk Management Procedures, which, inter alia, shall define the duties and responsibilities of risk owners in relation to all Group operations / activities. It assumes the establishment of similar structures in the Group's operational units which are linked to the Risk Management Division;
- Submit Risk Appetite's proposal (critical risks) for approval by CEO;
- Assisting the management in proper decision-making with regard to risk appetite and risk response;
- Creating and maintaining an appropriate risk awareness culture within the organization, enhanced by related training programs;
- Forming and coordinating operational activities which protect against or mitigate risks, including emergency and business continuity programs;
- Advocating in favor of risk management at strategic and operational level across Group activities;
- Maintaining and reviewing a Group Risk Register with dynamic development and ongoing assessment;
- Developing programs for event recording, which will contribute to the description and identification of risks, timely response / treatment and smooth continuation of business activities;
- Coordinating various third parties which provide the Group with business risk management consulting;
- Preparing and submitting risk reports to the BoD and stakeholders, when required;
- Establishing risk management-related objectives and including the same in the Group objectives.

It should be noted that the key role of the Risk Management Division is to protect and add value to the Group and other stakeholders, supporting its objective purposes.

Through its successful and effective operation, the Risk Management Division robustly contributes to the improvement of the Group's ability to:

- *Balance its strategy with acceptable risk-taking in order to attain its objectives*

Alternative strategies with differentiated risks are evaluated, the most suitable is selected and the related risks are managed so that the residual risk matches / approaches the Group's acceptable / eligible risk. It is noted that risk management operates on the basis of options based upon cost-benefit correlation.

- *Minimize operational surprises and losses*

Each operational unit of the Group identifies the risks that affect it and proceeds to pre-agreed mitigation actions. These actions are defined and monitored by the Risk Management Division in order to gradually achieve deterrence / reduction of identified risks and avoidance / mitigation of their consequences.

- *Evolve and improve over time its response/reaction to risks*, selecting a more effective approach at a lower cost.

- *Manage available resources with increasing efficiency over time*, by integrating risk management into all activities, due to higher added value.

- *Identify and manage all risks from each activity by selecting economies of scale*, through a broad approach and integration of responses, implemented in three stages:

  - *First* - aggregation and grouping of risks across the Group
  - *Second* - single risk transfer strategy
  - *Third* - transformation of risk management from a purely defensive mechanism to a mechanism used for seeking ways to maximize benefit and linking risk management to business development.

- *Link its growth and performance to risk management,* adjusting on a case-by-case basis risk tolerance levels in line with the benefits of taking on such risk.

- *Rationalize organisation and allocation of funds in order to increase return rates and seize opportunities*. One of the most important benefits that risk management offers to the Group is the improvement of business performance, and increase of organizational efficiency.

In order for the Risk Management Division to properly operate and optimize its performance, it is correlated with and supported by the Group Corporate Governance System, also in the way that the latter is aligned with the applicable standards, as well as by the Internal Control System, being actually a part thereof. Point out that the Internal Control Division ensures that quality operation of the risk management system is thoroughly monitored by controlling the Group's operational units, confirming that required actions have been taken, thus actively contributing to the mitigation of the Group's overall business risks and to a more representative

configuration of the Risk Register. It also, on a regular basis, confirms adequacy, appropriateness and effectiveness of the Risk Management Division's operation.

The operations and analytical processes of the Risk Management Division are described in its Procedures.

7. DOCUMENT REVISION

This Policy shall be revised every three years, unless circumstances dictate earlier