**RISK MANAGEMENT POLICY AND INTERNAL OPERATING REGULATION OF THE RISK MANAGEMENT UNIT**

## 1 INTRODUCTION

The present policy and operating regulations of the Risk Management Unit of the company "IKTINOS HELLAS SA" (hereinafter "Company") was prepared in accordance with the provisions of Law 4706/2020 on corporate governance, Decision 1/891 / 30.9.2020 of the Hellenic Capital Market Commission and the Corporate Governance Code followed by the Company.

The Management of the Company realizes that it is exposed in a business environment with different forms and types of risks. Therefore, it has established and implements a Risk Management System in order to be able to operate more efficiently, minimizing the impact of risks on its operation and its financial figures.

The effectiveness of the System is based on the commitment and support of the Management and the involved executives.

This document defines:

• The basic characteristics of the operation of the Risk Management System.

• The composition, composition and operation of the Risk Management Unit.

• The responsibilities and tasks of the Risk Management Unit.

## 2. POLICY / REGULATION IMPLEMENTATION (VALIDITY / AMENDMENT)

This enters into force immediately after its approval by the Board of Directors and binds all persons as defined in par. 3.

The present as well as any modifications thereof, are notified to the persons mentioned in par. 3 of the present. Following a written suggestion / proposal of the Company's Audit Committee and if there is a reason, the Board of Directors evaluates the appropriateness and effectiveness of the policy and Rules of Procedure and approves any changes.

It is reviewed whenever required.

## 3. OBLIGATORS OF COMPLIANCE WITH THE REGULATION

The Head and the members of the Risk Management Unit, as well as the respective members of the Audit Committee are responsible for observing the Rules of Operation of the Risk Management Unit.

Regarding the operation and implementation of the Company Risk Management System, as it is formed through the relevant policies and regulations, it binds the Management and all the involved executives of the Company.

## 4. CURRENT LEGISLATIVE FRAMEWORK

Article 4 of Law 4706/2020 stipulates that the Board of Directors ensures the adequate and efficient operation of the Company's Internal Control System, which aims, among other things, at the recognition and management of the substantial risks associated with its business and operation.

According to article 13 of law 4706/2020, the Company has the obligation to adopt and implement a Corporate Governance System, which among other things includes an adequate Risk Management System.

Also, according to article 14 of law 4706/2020, the Operating Regulations must include, among others, the reference of the main characteristics of the Internal Control System, ie at least the operation of the Internal Control, Risk Management and Regulatory Compliance Unit.

We note that according to Decision 1/891 / 30.9.2020 of the Hellenic Capital Market Commission and in the context of the evaluation of the Internal Control System in accordance with article 14 of law 4706/2020, the review by the Evaluator of the process of recognition and evaluation of risk assessment, the Company's management and risk response procedures and risk monitoring procedures.

In particular, the following are reviewed:

• the role and operation of the Risk Management Committee (if any) or other Body of the Company with corresponding responsibilities.

• the work and responsibilities of the Risk Management Unit, if it exists and otherwise, the service or staff to whom these responsibilities have been assigned.

• The existence of appropriate and effective policies, procedures and tools (such as the maintenance of risk registers - "risk registers") identification, analysis, control, management and monitoring of any type of risk involved in the operation of the Company.

According to article 44 of law 4449/2017, without prejudice to the responsibility of the members of the administrative or management body or other members elected by the General Meeting of shareholders of the audited entity, the Audit Committee monitors the effectiveness of the systems. risk management.

In addition, the Audit Committee reviews the management of the company's main risks and uncertainties and their periodic review. In this context, it evaluates the methods used by the company for the identification and monitoring of risks, the treatment of the main ones through the internal control system and the internal control unit as well as their disclosure in the published financial information in the right way. For the results of all the above actions, the audit committee informs the board of directors with its findings and submits proposals for the implementation of corrective actions, if deemed appropriate.

**5. BASIC PRINCIPLES OF RISK MANAGEMENT OPERATION**

The basic principles of the operation of the Company Risk Management are analyzed as follows:

• The Company identifies and manages the risks that are integrated in all products / services and activities.

• The Company ensures that the risks that will be identified and related to products / services or activities, are governed by adequate procedures and internal controls.

• The Company ensures that for each key risk identified and recorded, appropriate measures are taken to control or mitigate these risks and ensures that they are approved by the Board of Directors and / or other appropriate committees.

• The Company prepares a Report in which the various types of risks that it identifies, records and the actions that are decided for their management, are closely monitored and reported in a timely manner to the appropriate internal principles of the Company.

• The Company has developed and created adequate systems, tools and methodologies (eg Information Systems Risk Management Systems) in order to enhance the efficiency and adequacy of the Risk Management function.

• Risk Management supports and promotes transparency and accountability through distinct communication and reporting procedures.

• All activities and systems for risk identification, assessment, monitoring, reporting, control and mitigation have been properly and timely recorded.

• The Company Risk Management System is reviewed at regular intervals and modified accordingly, taking into account the overall work and strategic objectives of the Company.

## 6. ORGANIZATION AND OPERATION OF THE RISK MANAGEMENT SYSTEM

The organization of the risk management function is crucial and therefore the Company has established a transparent and sufficiently defined structure related to Risk Management.

The Risk Management policy is adopted and implemented by all employees (including the Company's managers), who are involved in risky activities, in order to develop an effective Risk Management Framework in the Company.

The bodies responsible for risk management are the following:

### 6.1. Board of directors

The Board of Directors has the general responsibility of defining, approving and supervising the implementation of the risk management policy and especially the willingness to take risks. At the same time, it ensures the compatibility of this policy with the strategic planning of the Company.

More specifically, the Board of Directors of the Company is responsible for:

• Ensures the adequate and efficient operation of the Company's internal control system, which aims at identifying and managing the essential risks associated with its business and operation.

• Ensures that the functions that make up the Internal Audit System are independent of the business sectors they control, and that they have the appropriate financial and human resources, as well as the powers to operate them effectively, as required by their role. The lines of reference and the division of responsibilities are clear, enforceable and duly documented.

• Defines goals, plans policies and sets limits for Risk Management, defining the overall strategic management framework of the Company's core risks (ie the market risk limit applicable to the whole Company, etc. or specific groups or concentrations).

• Ensures that senior management has taken all necessary measures in accordance with approved policies and monitors risk management metrics systematically.

In particular, the executive members of the Board of Directors, in existing situations of crisis or risk, as well as when the circumstances require that measures be taken that are reasonably expected to significantly affect the Company, such as when decisions are to be made regarding the development of business and The risks undertaken, which are expected to affect the financial situation of the Company, must inform the Board of Directors in writing without delay, either jointly or separately, submitting a relevant report with their assessments and proposals.

**6.2 Risk Management Unit**

The main responsibilities of the Risk Management Unit are the following:

• Identifying, evaluating and reporting the most significant risks, as well as finding appropriate methods to minimize them.

• Suggests about the risk profile and risk appetite of the Company.

• Suggests about risk management policies and procedures.

• Suggests about the overall risk management strategy.

• Estimates capital requirements on existing and future risks.

• Submits risk assessment reports and other reports.

The Risk Management Unit can not be held responsible for anything other than its advisory and control activities, which are performed in a preventive and advisory manner, in order to ensure that the Company recognizes, evaluates and addresses existing and potential risks. The Board of Directors of the Company bears the ultimate responsibility for the adequate and efficient operation of the Company's Internal Control System, which aims, among other things, at the identification and management of the essential risks associated with its business and operation.

**6.3 Head of Risk Management**

The Head of Risk Management is appointed by the Board of Directors of the Company after evaluation and proposal of the Audit Committee. He is a full-time and exclusive employee, personally and functionally independent and objective in the performance of his duties.

The Head of Risk Management is independent of the other business units of the Company and reports administratively to the Chief Executive Officer and operationally to the Company's Audit Committee. The administrative report is related to the facilitation of the daily operation (such as the approval of licenses, the budget, etc.).

The Head of Risk Management has access to all relevant information, with the object of his work and can use all available means of communication within the Company without restrictions, in order to perform his duties.

The Head of Risk Management has sufficient knowledge, skills and experience required to perform his duties. If deemed necessary, he participates in training programs related to the subject of his work.

The Head of Risk Management prepares an annual action / control program which defines the required resources required for the operation of the unit, control areas (policies,

procedures, etc.), any training, control reports and progress reports of the Company in in relation to the treatment of any findings, the way of communication with the Heads of Risk Management of the Departments, the meetings with the Audit Committee, etc.

The main responsibilities of the Head of Risk Management are the following:

• Prepares an annual program of activities.

• Develops and uses an appropriate methodology for all the risks exposed by the company,

• Proposes monitoring limits for each type of risk,

• Proposes Key Risk Indicators (KRIs) for each type of risk and monitors them,

• Ensures that senior management and risk owners take the necessary steps in accordance with approved policies and procedures to manage risk

• Monitors the achievement of the Company's objectives, as set out in the strategic planning and sub-plans,

• Monitors the effective implementation of the risk management policy and reports to the Audit Committee and the CEO possible deviations,

• Participates in business decisions, where the company assumes significant risks, e.g. new products, installation of a new computer system, new processes, etc.

• Coordinates and monitors the work of risk owners, through applications,

• Works as a coordinator in all workshops for evaluation of processes (processes), risks and safety valves,

• Prepares and submits to the Board of Directors, periodic reports related to the Company's risks,

• Prepares quarterly reports and annual summary report / report,

• Contributes to the Board of Directors in order to set objectives, design policies and set limits for risk management,

• Contributes to the Board of Directors in order to ensure the adequate and efficient operation of the Internal Audit System,

• Contributes to the Board of Directors in order to set the risk tolerance limits,

• Informs the Audit Committee and the Managing Director about possible situations of crises or emergencies and conducts periodic stress tests of emergencies,

• Recommends to the Board of Directors the adoption of an appropriate risk management strategy,

• Performs stress tests at least annually, with specific scenarios, reports results and makes recommendations where required,

• Suggests risk-sharing or hedging techniques.

The Head of Risk Management may request the assistance of an external consultant, with the approval of the Chief Executive Officer, to assist in the execution of his work.

The responsibilities of the Head of Regulatory Compliance and Head of Risk Management of the Company may be assigned to the same person following a decision of the Board of Directors and with the consent of the Audit Committee.

**6.4 Heads of Departments regarding Risk Management**

The Head of Risk Management is based on a network of executives, who have been appointed as responsible for risk management in relation to the individual functions / departments of the Company (Financial Management, Production, Human Resources, etc.).

They integrate the Risk Management policy and the risk-taking framework into day-to-day operations and limit their activities within the approved limits. They implement controls and procedures in order to be able to detect in time any deviations from the approved framework. They provide directly to the Management and the Head of Risk Management, the required information, with clarity and accuracy.

The Head of the Risk Management Department is an executive, appointed by the CEO of the Company who leads a specific business operation and is responsible for supervising, managing risk management issues of the business unit and implementing the decisions taken regarding the management measures.

His responsibilities include the following:

• Provides the Head of Risk Management with any support needed in order to perform his / her duties and information on cases of changes regarding new risks, changes in the impact or probability of occurrence as well as the methods of dealing with them.

• Supervises the implementation of the risk management function in the business unit under its responsibility.

• Provides information and training to executives of its business unit, regarding risk management issues.

• Notifies the Head of Risk Management and manages any changes on specific risks, evaluates them and suggests the adoption of appropriate management measures.

**6.5 Audit Committee**

The Audit Committee advises and supports the Head of Risk Management in order to fulfill his responsibilities.

The Audit Committee ensures that the operation of the Risk Management Unit is adequately staffed with staff who have sufficient knowledge and experience to carry out the responsibilities and recommends its training, in cooperation with the Human Resources Department when deemed appropriate.

The Audit Committee approves the annual action plan of the Risk Management Unit and is responsible for monitoring its implementation and examines the reports of the Head of Risk Management and the findings and evaluates their completeness and adequacy. It also reviews the relevant suggestions regarding the definition of appropriate corrective actions.

Among other things, the Audit Committee monitors the effectiveness of risk management systems through the Internal Audit Unit and the Head of the Risk Management Unit. More specifically, it reviews the management of the main risks and uncertainties of the Company and their periodic review. In this context, it evaluates the methods used by the Company for the identification and monitoring of risks, the treatment of the main ones through the Internal Audit System and the Internal Audit Unit as well as their disclosure to the published financial information in a correct manner. For the results of all the above actions, the Audit Committee informs the Board of Directors with its findings and submits proposals for the implementation of corrective actions, if deemed appropriate.

**6.6 Internal Audit Unit**

The Internal Audit Unit carries out its own independent evaluation in the context of the Evaluation of the Internal Audit System. Ensures that a system of internal safeguards is in place and that all stakeholders exercise their responsibilities, as provided by the policies and procedures set out in the Company Risk Management Policy. If it finds deviations from the approved risk-taking framework, it makes recommendations and monitors the elimination of any deviations.

Provides regular assessments of the risk-taking framework, at Company level, as well as at lower levels as per department / operation as appropriate.

Checks if the exceedances of the risk limits are detected in time and communicated to the competent levels.

**7. RISK MANAGEMENT SYSTEM**

Developing an effective risk management system requires:

• appropriate organizational structure and operation

• clear roles and responsibilities

• Adequacy of resources, human resources and support infrastructure

• perception of the concept of risks

• knowledge of risk management techniques

• outsourcing rules

• proper internal communication

• Reliable data and reports

• adequate documentation and information

• effective controls

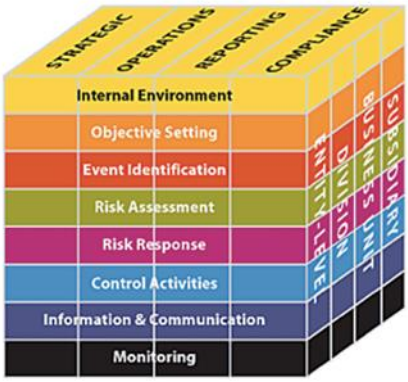
• possibility of continuing the smooth operation of the business

The focus of good risk management is on identifying and managing these risks.

This section presents in more detail the basic principles and stages that govern the Risk Management System of the Company.

**7.1. Risk Management Framework**

The Company implements the business risk management framework established by the COSO Commission in 2004. In accordance with the COSO framework. Business risk management is defined as “a process performed by the entity's board of directors, management and other personnel, applicable to the regulation of the strategy and throughout the business. It is designed to identify potential events that may affect the entity, manage risks and provide reasonable and assured assurance about the achievement of the business objectives. This frame consists of three different dimensions, as shown in the graph below.




According to the methodology, the risks should be identified after the Company's objectives have been identified and related to them. These objectives are aligned with the eight risk management components and are represented by the horizontal series. These 8 components are: the internal environment, goal setting, fact-finding, risk assessment, risk management, control activities, information and communication, and monitoring.

Also, in order to have a comprehensive management of risks through a single approach, the risks that characterize the company as a whole (Entity level), at the level of Management or service (Division), at the level of business unit (business unit) and at the level of Subsidiaries.

The categorization of risks is done at the level of strategy (Strategic risks), operations (Operational risks), reliability of financial reports (Reporting risks) and compliance with relevant laws and policies (Compliance risks).

**7.2. Identification and Evaluation of the Internal Environment of the company**

The first step in the risk management process is the recognition and evaluation of the Company's internal environment. Indicative parameters are the philosophy of the management, the structure of the Board of Directors, the human resources policies, etc.

Management formulates the Company's philosophy regarding risk and determines the behavior, the attitude towards risk as well as the ethical values. The internal environment lays the foundation for the way in which risk is perceived and dealt with by executives. The internal environment is also the basis for all other components of business risk management, providing discipline and structure. It affects how strategies and goals are defined, how business activities are structured and how risks are identified, evaluated and addressed. Affects the design and operation of control, information and communication systems activities, and monitoring activities.

The examination and evaluation of the internal environment as well as the administrative and organizational structure of the Company helps the Management in order to determine the scope and extent of the risk management procedures. For the evaluation of the internal environment, the Management must examine and review the following that constitute its internal environment:

• Compliance with the regulatory framework.

• The composition of the Board of Directors

• The processes of developing and monitoring business plans and their strategy and review procedures

• Defining and communicating goals

• The procedures of preparation and submission of the company's financial statements and periodic internal reports

• The procedures for determining specific business performance indicators and monitoring any deviations from the desired level.

• The organizational structure of the company through relevant organizational charts and job descriptions and jobs.

• The reference lines in the Company.

• The policies and procedures for all transaction cycles of the Company

• The Code of Conduct of the Company.

• The adequacy and suitability of human resources.

The review of the internal environment by the Management will help to have a more complete picture in terms of its philosophy, strengths and weaknesses, values and culture and then to set its goals and objectives.

**7.3. Defining Objectives**

The Company faces and manages risks arising from both internal and external factors. A prerequisite for the adequacy of the risk assessment process is the definition by the Management of business objectives and their connection with the different levels of the organization.

Objectives are set at a strategic level and form the basis for defining individual business objectives related to the activities of business units such as operating and objectives related to financial information and performance.

Strategic objectives are dynamic and adapt to changes in internal and external conditions. Recognition of objectives precedes the effort to assess and classify the risks associated with achieving them.

Operational objectives refer to the efficiency and adequacy of the Company's operations and include, among other things, the goals of efficiency and profitability as well as the goal of protecting the assets of the organization from possible losses. These objectives vary depending on the decisions of the Management regarding the structure of the organization and the expected performance. The operational objectives concern, among others: expansion of activities that are profitable activities / actions, penetration into new markets, development of methods to attract new customers, retention of existing customers, expansion of market shares in the Greek banking market, improvement of the quality of services offered of customers etc.

Reporting objectives refer to reliable administrative information with accurate and complete information required. They enhance the decision-making by the Management and the

monitoring of the activities and the performance of the individual business units. Examples of such reports can be the various marketing programs, daily valuations of profits and losses, amount and size of debtors, results of measuring customer and executive satisfaction, etc. Reliable reference lines give the Management additional assurance for the preparation of reliable external reports. shareholders, public). Such benchmarks refer to financial statements, management decisions and analyzes, and regulatory compliance reports.

Compliance objectives refer to the actions that the various business units are required to take in order to harmonize their functions with the various regulations and regulations. Such requirements may be related to matters of supervision, purchasing, pricing, taxation, etc. The legal regime establishes the minimum levels of level of conduct, which the business unit in turn configures in its own data.

Management should have set its goals before attempting to identify potential events that affect those goals. Business risk management ensures that there is a specific process for defining the entity's objectives, which support and align with its mission, but also its risk behavior.

More specifically, the Company, under the responsibility of the Board of Directors and with the participation of the Management, clearly defines its objective objectives. These stem from the Company's mission / vision, are in line with them, but also reflect the choice of actions through which the Company will create value for its shareholders. They should also be easy to understand and measure.

Management should ensure that staff are aware of the Company's objectives so that they are able to carry them out effectively.

The indicative objectives set, measured, evaluated and monitored by the Management are presented in order to make decisions:

- Profitability ratios
- Turnover development
- Market share
- Revenue from new customers as a percentage of total revenue
- Profit margin from new customers
- Total operating expenses as% of turnover
- Total fees / Total operating expenses
- Revenue per product / service
- Revenue per customer
- Total cost per average customer
- Customer satisfaction
- Customer / stock / supplier days
- Equity to foreign capital

- Export rate
- Export analysis by country
- Concentration per customer
- Research and development costs to total operating costs
- Customer retention
- Acquisition of new customers
- Customer profitability
- Market shares
- Customer complaints
- Number of personnel
- Income per employee
- Division of employees by address / function
- Utilization rate
- Inventory level
- Warehouse renewal time
- Delivery to in relation to the order
- Average delivery delay time
- Fira - product failure / failure
- Effectiveness of promotional actions
- Permanent and seasonal staff
- Degree of staff use
- Staff evaluation
- Resignation rate
- Recruitment index
- Number of new products
- Staff training hours

**7.4. Event Recognition**

The internal and external events that affect the achievement of an entity's objectives must be identified and separated into risks or opportunities. This is followed by the redefinition of the business strategy taking into account the existing opportunities of the internal or external environment.

In particular, the events that can either negatively or positively affect the fulfillment of the business strategy and the achievement of the objectives should be recognized under the responsibility of the Board of Directors and the involvement of the Company's Management. The factors from which these events may arise may originate both inside and outside the Company. In addition, it is obvious that these factors are constantly changing, for this reason it is necessary to establish a process of updating the recognition of events both periodically and when deemed necessary, eg due to changes in specific quantities or data.

The business risks that will be identified based on the above should be appropriately categorized and linked to the respective objective and corporate processes. The units that are likely to have a corresponding impact on the events that are likely to have a positive impact on the achievement of the Company's objectives should provide feedback on the process of determining it in order to be exploitable by implementing relevant actions.

In this context, each unit of the Company records common events that may occur in itself or affect it positively or negatively, such as changes in the macroeconomic environment in which the Company operates or its customers, fines for non-compliance with the regulatory environment, opportunities created for customer expansion, new markets, changes in technology, etc.

Also, the Company's executives through their daily engagement and communication with customers, suppliers, shareholders, supervisory authorities, etc. record their views and any plans in order to examine whether these could be a potential opportunity or risk for the Company.

Finally, the recording of events that occurred in the past and affected the Company and its performance is important to capture the manner and size of the impact and to avoid incorrect management / response choices.

**7.5. Risk Assessment**

**7.5.1 Risk identification**

At this stage, the main risk categories that characterize the Company and its activities are identified, which are related to the goals of the organization. Risks are recognized at the entity level, at the division level, at the business unit level and at the subsidiary level.

Business risk is defined as the threat of an event or action affecting the Company's ability to achieve its business objectives and successfully carry out its strategies. The various categories of risks stem from the nature of each activity of the business units, from the external environment but also from the decisions of the Management. Therefore, effective identification of risks requires obtaining information regarding the internal and external environment of each business unit.

When examining external factors, parameters such as technological developments, competition, economic changes, changes in the Company's field of activity, as well as political and social developments are taken into account. When examining the internal factors, the risks arising from administrative decisions regarding the structure and the way of operation of the Company are taken into consideration and which are related to the adequacy, completeness and overall management of the human resources, the nature of the work and activities of the individual. units of the Company, the operational and

technological infrastructure, the characteristics of the information processing mechanism and other factors.

In order to avoid cases of neglect of significant risks, in the phase of risk identification, all possible risks of the organization are recognized, regardless of their probability of occurrence and their impact, as this is the subject of the assessment that will be carried out at a later stage of the process. Even events or actions that are considered important but have a low probability of occurrence are not ignored inthe stage of recognizing whether their potential impact on the achievement of an important goal is great.

The Company has recognized the following risk categories:

**General indicators**

**Price or Market Risk**

Market Risk refers to the possible reduction of revenues from sales of products. Consequently, the possible reduction of the share price is included.

**Interest Rate Risk**

Interest rate risk is directly related to changes in loan interest rates.

The factors that increase the interest rate risk are mainly the changes in the interest rate levels and the changes in the loan repayment agreements.

**Credit and Counterparty Risk**

Credit Risk is considered the risk of non-fulfillment of the obligations of the Company's customers.

**Concentration risk**

Concentration Risk refers to the collection of all revenue by a customer.

**Liquidity risk**

It is the possible possibility of inability of the Company to finance its operation smoothly or to finance it with high borrowing costs.

The risk is directly related to creditworthiness, which determines its lending factors by banks. It is due to insufficient monitoring of cash inflows and outflows.

**Operational hazards**

Operational Risk is related to a large number of control points, in the absence of which the possibility of inefficient operation of the Company increases.

Includes cases already mentioned, such as:

• Inability to replace staff,

• Access to prohibited (handwritten or computerized) systems and files,

• Lack of a limit system on expenditures / investments,

• Negotiation and approval of actions by unauthorized executives,

Dependence on a limited number of executives with key positions.

In addition to the above, special attention must be paid to the following operational risks:

**Accounting and Data Processing Risk**

The following risks are included:

• The risk of differences in results between accounting subsystems and applications or between different valuation methods.

• The risk of not detecting significant accounting errors in the General Ledger.

• The risk of losses due to incorrect treatment of income / expenses.

• Risk of Completeness and Correctness of documents and data. The first mainly concerns the lack of documents that will secure the Company functionally and legally in case of disagreement with a counterparty, while the second concerns the inability to execute a transaction in case of insufficiency of basic data.

**Information Systems Risk (IS)**

This category includes:

**Logical Security**

Related to employees' access rights to the Company's computer systems, networks, applications and files

**Physical Security**

It concerns the level of physical access to computer sites. It is treated with precautionary safety valves that prohibit the possibility of creating unexpected situations, due to accidental or premeditated actions, ensuring smooth operation and immediate recovery in cases of emergencies.

**Human Resources Risk**

Possible deficiencies in the internal control system such as:

• Excessive authority and trust in key executives,

• Dissatisfaction and negative attitude of staff due to poor working conditions or level of remuneration,

• Low staff morale due to poor leadership and / or mismanagement,

• Lack of perspective and career,

• Insufficient education and lack of continuing education programs,

• Bias or non-meritocracy,

• Unreliable recruitment evaluation process.

**Risk of Insurance Coverage**

It is related to the insufficient insurance coverage and / or the vague wording of insurance coverage terms.

The main areas of coverage should clearly indicate the following:

• Adequate insurance coverage of fixed assets and means of operation,

• Adequate coverage of general disasters (fire, floods, earthquakes, power outages, terrorist acts and vandalism, civil liability, etc.),

• Adequate coverage for fraud and sabotage,

• Adequate coverage for cash loss including the case of robbery from custody / transfer,

Adequate coverage of medical staff.

**Risks of Legal / Legislative Framework**

Incomplete contracts or unclear terms, completeness of documents, disputes with clients that lead to litigation.

This category also includes risks arising mainly from instructions of the Hellenic Capital Market Commission and other Supervisory Authorities.

**Reputation Risk**

For example, a decrease in customers due to poor product quality, negative spreads, etc.

**Event Risk**

For example unforeseen cases of political and economic developments that may adversely affect the course of the Company / Share.

**7.5.2 Observation tool Tracking the risk register (risk register)**

The risks identified are monitored through a consolidated table of categorized risks in the risk register to identify in detail the stages of analysis and treatment. The risk register is monitored by the relevant Executives of the Directorates and is updated when required by the Head of Risk Management in order to provide risk information in an organized and centralized manner and to determine the analysis, how to deal with, categorize and classify risks. used to deal with them. The risk register is also sent to the Internal Audit Unit in the context of their own risk assessment.

**Risk Register**

| Risk Type | Risk Description | Risk Assessment | | | Safety Tips | Responsible Unit |
|---|---|---|---|---|---|---|
| | | Probability Rating | Risk Impact | Risk Rating | | |
| | | | | | | |

The above risks should be assessed under the responsibility of the Board of Directors and the involvement of the Management and consultation with the Head of Risk Management. As risk identification is a dynamic process, periodic reassessment is required, at least on an annual basis.

It is noted that both the inherent risks, ie those faced by the company without taking into account any benefits from the operation of specific Safety Gaps, and the residual risks, ie the risks after the impact should be assessed. of Safety Valves.

The Company on an annual basis at least identifies the risks by basic category and are recorded in the Risk Register. The ways of identifying risks used by the Company are the following:

• Interviews between the Head of Risk Management and the executives of the Directorates.

• Group Production of Ideas with the participation of more executives.

• Risk List: The list is a set of risks that have occurred in the past and may occur in the future.

• Risk analysis structure: The sources of risk are ranked (internal audit reports) and then the Company focuses on one area in order to identify as many as possible.

• Incident reports based on forms as mentioned above.

• External consultants: Reports are taken into account which are prepared by assigning specific projects to external consultants.

As the identification of risks is a dynamic process, the Risk Register can be updated with new risks and on a more regular basis (eg quarterly), as well as after each audit if required or whenever deemed necessary. The contribution of the Responsible Departments involved with the Risk Management is considered important in terms of updating the risks and reassessing the already recognized risks.

**7.5.3 Risk Classification**

Having identified the inherent risks (inherent risks) and having correlated them with the respective business objectives, their analysis and assessment is carried out in terms of the possible impact of each risk (impact) to which it is associated each time, and the probability of its occurrence.

Therefore, each risk is analyzed in two dimensions:

• the probability (Likelihood) (the probability of occurrence of the risk in the business unit)

• Impact (the potential damage that the occurrence of risk will cause to the business unit)

In order to achieve as much uniformity as possible in the risk assessment and to have a common grading methodology, each dimension is graded on a tertiary scale, which is categorized as follows:

1 = Low

2 = Medium

3 = High

If deemed necessary for purposes of greater accuracy, a five-point rating scale may also be used.

Analytical determination of scales for risk assessment helps to reduce subjectivity in risk assessment. Nevertheless, the crisis and the experience of the Management remains the most important factor in risk assessment.

**7.5.4 Risk assessment**

When assessing the risks, the Management rates each risk based on the probability of occurrence of the risk and the impact of its occurrence. Risks are assessed at the level of the business unit and / or at the level of operation or activity. The decision depends to a large extent on the number of risks identified as well as on their level of development (eg at secondary or tertiary level).

With regard to the IT systems risk assessment, the assessment concerns the specific IT systems that are connected to the respective business unit and is carried out in the context of the overall assessment of that unit. Information systems risk rating is based on the probability (Likelihood) of the occurrence of the risk and the impact (Impact) of its occurrence as for other risks.

Risk assessment is largely subject to the subjective perception and experience of management, the use of historical data, if any, and data collected from previous evaluations.

**Chance of Appearance (Likelihood)**

The probability of occurrence is an estimate of how often a particular risk may occur in a given period. Gives an estimate of the incidence of a hazard. To assess the probability of occurrence, the risk is scored on a scale between one and four (1-3 with increasing importance where 1 is the lowest value and 3 the highest) according to the following classification:

**Likelihood**

1 = Low

2 = Medium

3 = High

**Impact**

Impact is an impact assessment risk in the financial results of the Company for each individual implementation of the risk. If the risk materializes the result can be immediate loss (eg embezzlement - linked to fraud) or indirect loss (eg fines, litigation against the Company).

For the assessment of the impact on the Company from the implementation of the risk, the risk is valued on the basis of value (in Euros) and is rated on a scale between one and three, (1-3 with increasing importance where 1 is the lowest price and 3 the higher) according to the following categorization:

Impact Rating (based on value)

1. Low - from € 0 to € 30,000

2. Medium - from € 30,000 to € 300,000

3. High - from € 300,000 and up

As the impact of risk on financial value can not be determined in each case, its assessment is based on the experience and judgment of Management and historical data if any.

Taking into account the results of the assessment based on the probability of occurrence of the risk and the impact that the occurrence of the risk will have on the business unit and each risk is finally rated on a higher scale, which is categorized as follows:

1 = Low

2 = Medium

3 = High

1 = Low

The characterization of the level proves that only low-risk weaknesses exist but are satisfactorily addressed by the Management and its desire to correct them therefore they can successfully deal with strong business fluctuations. There is substantial compliance with the regulatory and legal framework and as a result the Company is able to demonstrate excellent performance and methods of risk assessment and grading depending on its size, the complexity of its procedures and its levels of risk. There is no reason for strong concern and as a result supervision / control may be informal and limited.

2 = Medium

These risks are of medium importance and in the short term may cause disruption to the in-house environment. However, the level of weakness is not high enough to justify an increase in scale. Management may not have the ability or desire to effectively address weaknesses within predetermined timeframes. These risks are usually more difficult to deal with effectively in cases of variability in the business environment and are more prone to external influences than those mentioned above. In addition, there may be no substantial compliance with the regulatory and legal framework and as a result the Company may not be able to demonstrate excellent performance and risk assessment and rating methods depending on its size, the complexity of its procedures and the levels of risk. of.

3 = High

These risks can be classified as significant. They may have a high or low incidence / probability of occurrence, but the potential consequences are significant enough to require consistent and adequate treatment (since they are classified as high). Appropriate care must be taken to develop risk mitigation strategies.

In addition, for illustration purposes in the form of a thermogram (heatmap) the following are specified:

• High Risk Area (High). Displays the result of the formula score (impact and probability / 2) and includes overall scores high and very high.

• Medium Risk Area. Displays the result of the formula score (impact and probability / 2) and includes overall average results.

• Low Risk Area. Displays the result of the formula score (impact and probability / 2) and includes the other overall results (low).

**Heatmap**

| | | | | |
|---|---|---|---|---|
| (Likelihood) | High | | | |
| | Medium | | | |
| | Low | | | |
| | | Low | Medium | High |
| | (Impact) | | | |

**7.6. Risk Response**

After the evaluation of the various risks, the determination of the way of responding to them (risk response) follows, under the responsibility of the Board of Directors and with the cooperation of the Company's Management. This process consists of evaluating the costs (direct, indirect and opportunity costs) and the benefits that each possible response will bring, and choosing how to reduce the likelihood and potential impact of each risk within acceptable risk limits. tolerance). These limits should be notified by the Board of Directors to the Company's Management whenever it is deemed that there have been changes in the internal or external environment, which may affect them.

Specifically, for each risk that has been identified and assessed, Management may choose to act in one of the following ways:

a. to avoid risk avoidance by stopping the activities that cause it,

b. to reduce (risk reduction) the probability of occurrence of the risk and / or its potential impact, usually by activating relevant Safeguards,

c. transfer part of the risk or share it with third parties (risk sharing), limiting the possibility of its occurrence or its potential impact,

d. to accept the risk (risk acceptance), ie not to take any action aimed at reducing the likelihood of occurrence of the risk or its consequences.

**7.7. Control Activities**

Safeguards (also called Checkpoints or Safeguards) are the policies, procedures, techniques and mechanisms that are put in place to ensure that risk management decisions are implemented that threaten the achievement of its objectives. Company. They concern the whole Company and are executed by the executives of all levels (Board of Directors, Management, other staff) and in all corporate operations.

Safety Gates consist of many categories of actions, which vary in level of implementation, cost and degree of effectiveness, depending on the circumstances. They include approvals, authorizations, confirmations, operational performance reviews, asset security and more. They are part of the day-to-day work of employees and are integrated into corporate policies and procedures, which should be reviewed periodically in order to be properly updated.

As mentioned above, the formation of Safety Gaps takes into account the inherent risks that are likely to have a negative impact on the fulfillment of the business strategy. Therefore, every applicable Security Code should be linked to the existence of a relevant risk, as otherwise its operation burdens the Company with costs (direct or indirect), without providing a benefit in terms of achieving its business goals. Also, when choosing between possible alternative Safeguards to cover some risk, the cost-benefit ratio should be taken into account.

The Company's Management chooses between various types of control activities and safety valves, some of which are the following:

• Top-level inspections - senior executives inspect actual performance based on budgets, forecasts, prior periods and competitors.

• Activity Management: The Managers who manage the functions or activities inspect the performance reports.

• Information processing: various checks are performed to check the accuracy, completeness and approval of transactions.

• Physical checks: equipment, inventories, securities, cash and other assets are insured periodically measured and compared with the amounts presented in the accounting and other books and records of the Company.

• Performance indicators: link different sets of data, operational or financial together with relationship analyzes and corrective actions

• Separation of duties: tasks are divided or separated between different employees to reduce the risk of error or fraud.

**Safety Levels at Company Level**

There are a number of Safety Valves, which are designed and operate beyond and above the individual corporate activities. These Safeguards cover more than one or even all of the company's processes and transactions. They are prepared by the Management and approved by the Board of Directors and their effectiveness is controlled by the Management and mainly the Internal Audit Department.

**Procedural Levels**

For each process at risk there is an appropriate balance between preventive / detective (preventive / detective controls), as well as systemic and of non-systemic Safety Valves (automated / manual controls). A basic principle in their formation is the achievement of a logical and adequate separation of responsibilities.

As the effectiveness of the Safety Legs depends (to a small, large or absolute degree) on the respective competent employees in the various departments and units of the Company, it is

absolutely necessary to inform and train them regarding the correct implementation of what is required by them.

In general, for each process / transaction that is exposed to risk, the Company through the Managers of the Departments / Directorates and the approval of the Management ensure that there are and operate Security Guarantees that aim to ensure the completeness, accuracy and validity of the transactions. , as well as limited access to systems / data / assets.

**Information Systems Security Locks**

Extensive use of information systems for corporate operations requires the application of Security Gates - at least on the most important systems - in order to ensure the provision of reliable and complete information, as well as the uninterrupted and proper operation of these systems. The areas that should at least be covered are the following:

a. System Development

b. System Changes

c. Security & Access

d. Daily Operations (Computer Operations)

e. Business Continuity Plan & Systems Restoration

f. End-User Computing Programs

**8. RISK MANAGEMENT SYSTEM EVALUATION**

Head of Internal Audit

A basic condition of the Company's Internal Control System is the efficient operation of the Risk Management Unit.

The Internal Audit Unit evaluates the reports and findings of the Regulatory Compliance Unit and conducts independent periodic audits in order to evaluate the adequacy of the Risk Management System.

In particular, the Internal Audit Unit monitors, controls and evaluates, among other things, the operation of risk management, prepares reports with findings regarding the effectiveness of the operation of risk management and comments on the possibility of improvements.

**Independent evaluation of the Internal Control System**

As mentioned above, according to Decision 1/891 / 30.9.2020 of the Hellenic Capital Market Commission, it is required, among other things, the review by an independent Appraiser on a three-year basis of the risk identification and risk assessment process, the Company's management and response procedures. (risk response) and risk monitoring procedures.

In particular, the work and responsibilities of the Risk Management Unit are reviewed, the existence of appropriate and effective policies, procedures and tools (such as the maintenance of risk records - "risk registers") to identify, analyze, control, manage and monitor any type of risk that involves the operation of the Company.