GROWTHFUND
THE NATIONAL FUND OF GREECE

GROWTHFUND
RISK MANAGEMENT POLICY

April 2024

Table of Contents

A. Introduction **3**
B. Objective of the Risk Management Policy **3**
C. Scope of Application **3**
CHAPTER 1: KEY ROLES IN RISK MANAGEMENT **4**
1.1 Risk management governance structure **4**
1.2 Stakeholders in Risk Management **5**
1.3 Risk Management Collaboration with Other Units and Companies of the Group **8**
CHAPTER 2: METHODOLOGY OF RISK ASSESSMENT **9**
2.1 Methodological Framework **9**
2.2 Fundamental Principles **9**
2.3 Risk Assessment **9**
2.3.1 Inherent Risk 9
2.3.2 Residual Risk 11
CHAPTER 3: RISK MANAGEMENT PROCEDURES FRAMEWORK **12**
3.1 Risk Identification **12**
3.2 Risk Assessment **13**
3.3 Mitigation of Risks **14**
3.4 Crisis Management **15**
3.5 Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) **15**
3.6 Risk Monitoring **15**
3.7 Risk Reporting **16**
APPENDIX 1 – RISK ASSESSMENT CRITERIA **16**
APPENDIX 2 – RISK REGISTRY **19**

A. Introduction

The present document includes the Risk Management Policy of Growthfund (hereinafter "**Company**"). In particular, the text describes significant aspects of Risk Management such as the governance model, the categorization, the procedures, and the methodology that underpin the development of an early recognition system and effective Risk Management aimed at establishing an advanced risk culture for achieving sustainable benefit in every activity of the Company.

The scope of this Risk Management Policy includes Growthfund and forms the basis for all initiatives related to Risk Management in all subsidiary companies of the Group, which are required to align with the guidelines of this document.

The Risk Management Policy is submitted by the Risk Management Director to the Internal Audit & Risk Committee of the Board of Directors, which reviews, oversees, and approves it in order to be submitted for approval by the Board of Directors. The Executive Management and the Risk Management Unit of the Company are responsible for the implementation of the Policy.

B. Objective of the Risk Management Policy

The Company, operating in a sensitive and continuously changing economic and social environment, recognizes its exposure to risks and the need for effective management of these risks. Furthermore, it accepts the need for efficient use of the resources that have been allocated to it in order to fulfill the multifaceted expectations of its Shareholder.

Risk Management is an integral part of the Company's commitment to fulfill its active role in order to accelerate the country's economic development. Achieving its objectives depends on finding the right balance between risk and performance in its daily activities to implement its Strategic Planning.

The mission of Growthfund in relation to Risk Management is:

'*To create added value for the economy, citizens, society, and the environment, improving operational effectiveness and minimizing losses related to all kinds of risks, in a manner consistent with best practices and in compliance with legal and regulatory requirements, according to its Strategic Plan.*'

Towards this direction, the Company has developed a Policy regarding Risk Management, analyzing the key issues concerning its approach to Risk Management. The Risk Policy aims to record the way in which Risk Management is integrated into the operation of the Company through the involvement of its structures in the risk management processes. The Risk Management Policy is updated as deemed appropriate, in order to align with the overall strategy of the Company and to meet the needs for effective Risk Management.

C. Scope of Application

The scope of the Risk Policy concerns Growthfund and forms the basis for all initiatives related to Risk Management. The Risk Management practices in the subsidiary companies of the Group must align with the provisions of this document

CHAPTER 1: KEY ROLES IN RISK MANAGEMENT

1.1 Risk management governance structure

Risk Management is an integral part of the Company's operation and is based on the Three Lines of Defense Model. The main principle of this model is that Risk Management involves the entire Company and is not the exclusive responsibility of a single role or unit.

The three roles involved in the Three Lines of Defense Model are as follows:

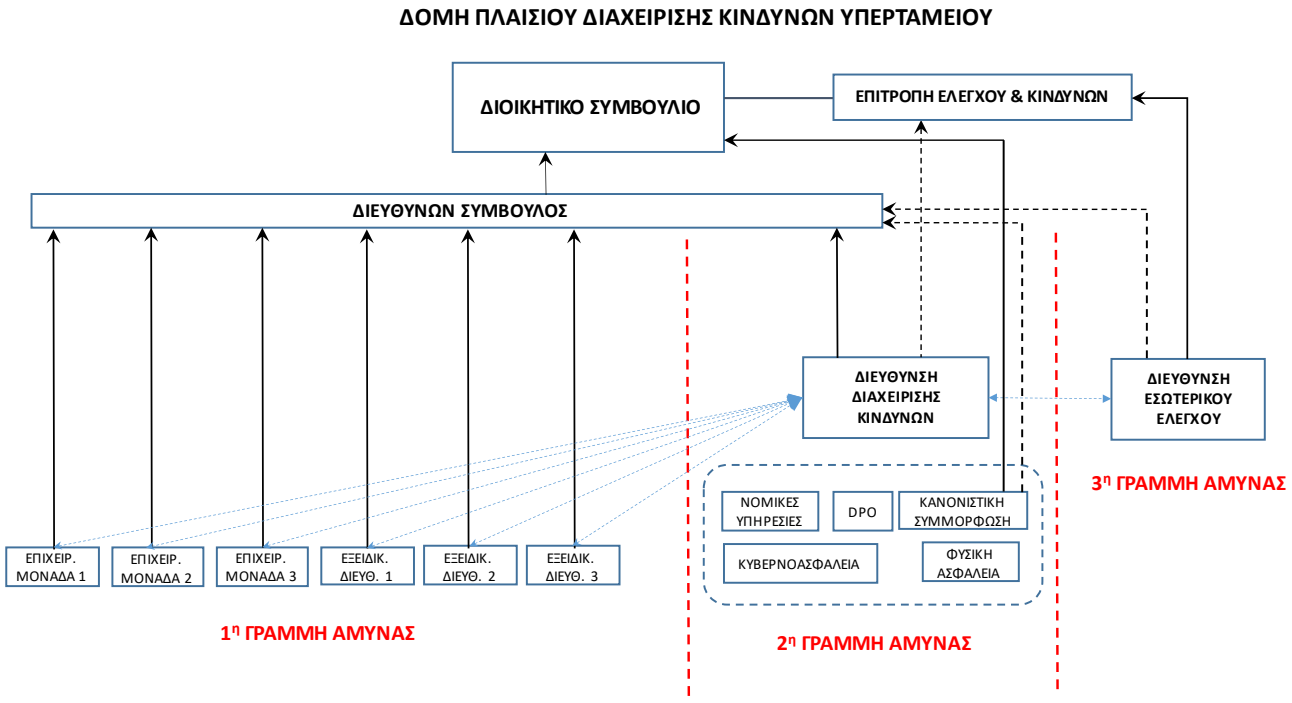
1. **1st line,** which includes the Units responsible for identifying, assessing, controlling, and minimizing risks.

2. **2nd line,** which includes the Units that provide guidance, support, methodology, training, and coordination to the 1st line Units.

3. **3rd line,** which provides an independent assessment of the implementation of the Risk Management Framework.

The Board of Directors oversees the design and implementation of an effective Risk Management system that is developed and implemented within the lines of the model.

The risk management governance structure of the Company is diagrammatically presented below.



Specifically, the Company's risk governance model includes:

1. The Operational Units and Specialized Directorates of the Company, which are part of the **1st line**.

2. The Directorates/Units that are part of the **2nd line**:
    - Risk Management
    - Compliance
    - Legal Services
    - Physical Security
    - Cybersecurity
    - Personal Data Protection (DPO).
3. The Internal Audit Directorate, which is part of the **3rd line** of the model.

A key role in coordinating the implementation of Risk Management processes is played by the Risk Management Unit, which communicates with the other Units of all three lines and is responsible for drafting risk reports to the Executive Management, the Internal Audit & Risk Committee, and the Board of Directors of the Company (as required).

1.2 Stakeholders in Risk Management

Τα κύρια εμπλεκόμενα μέρη στη Διαχείρισης Κινδύνων της Εταιρίας είναι:

The primary stakeholders in the Company's Risk Management are:
Board of Directors (BoD)

- The BoD ensures the adequate and effective operation of the Risk Management system in all the Company's activities.
- It reviews, with the assistance of the Internal Audit & Risk Committee, and approves the Risk Management Policy and the Risk Appetite Framework.
- The BoD understands the nature and extent of the risks faced by the Company and ensures that the structure and complexity of the mechanisms for managing and monitoring these risks are appropriate and sufficient in relation to the Risk Appetite and the business plan it has approved.
- It continuously monitors the effectiveness of the Risk Management actions, revisits and updates them regularly, and periodically assesses the main risks to which the Company is exposed.
- The BoD supervises and evaluates the Risk Management system on an annual basis through reports prepared by the Risk Manager, as well as the controls performed by the Internal Audit Unit through the Internal Audit & Risk Committee, to which it reports, ensuring that the main risks are identified, prioritized, addressed, and managed in a correct, complete, proportional, and effective manner.
- The BoD is regularly informed by the Internal Audit & Risk Committee about current risk exposures, ensuring that the Group's risk profile remains within the approved risk appetite and relevant limits.
- It is responsible for enhancing the Group's risk culture and awareness of all personnel regarding the risks and the Risk Management Policy.

Internal Audit & Risk Committee (A.R.C) of the BoD

- The Internal Audit & Risk Committee oversees the effective operation of the Risk Management Unit and ensures that the Company's Directorates and Units have the necessary governance structures, develop and demonstrate the necessary culture and due diligence concerning Risk Management as part of their daily operations, and operate within the tolerance limits that have been set and approved.
- The A.R.C regularly examines and approves for submission to the BoD the Risk Management Policy and the Risk Appetite Framework of the Company and monitors their proper communication across the entire Growthfund Group.
- It certifies that all personnel have the necessary tools, training, and skills to identify, record, evaluate, measure, and report risk incidents.

- It supervises the upgrading and review of the Risk Management framework, assessing current and emerging risks and how they can impact the Company's strategic goals. For this purpose, it receives reports and monitors the progress of risk indicators (Key Risk Indicators-KRIs), regarding new risks and business developments.
- It examines the evolution of the Company's residual risk profile on a regular basis to assess the effectiveness and adequacy of the actions taken by the Management for monitoring, controlling, and mitigating such exposures.
- It is informed by the Risk Manager and oversees the Risk Register, rating and prioritization of risks.
- It examines the planned containment measures, evaluates their effectiveness, and approves the submission of the Risk Manager's Recommendation to the Board of Directors for approval.
- It also supervises the progress made by the Company's Management in implementing the approved risk containment actions and measures and their successful integration into the Company's daily operations.
- It regularly updates the Board of Directors on the evolution of the Company's substantial risks as well as the adequacy and effectiveness of the Risk Management Framework.
- It provides advice and support to the BoD in its supervisory role regarding the independent examination, approval, and monitoring of the effectiveness of Risk Management.
- It examines the Risk Management practices of the Company and ensures they are subject to effective and comprehensive internal control.

Executive Management

- Executive Management is responsible for implementing and effectively operating the Risk Management processes and managing residual risks, based on the Risk Appetite Statements and limits that have been determined.
- It actively participates in the Risk Management processes under the coordination of the Risk Management Unit.
- It is responsible for developing and operating the appropriate framework and required culture for Risk Management in all operational processes executed.
- It communicates the BoD approved Risk Appetite Framework for all types of risks, authorizes the appropriate executives to manage them, assigning accountability to them, and submits proposals regarding the determination of risk indicators (Key Risk Indicators- KRIs) and risk tolerance limits.
- It ensures the necessary resources for the smooth and effective operation of the Risk Management Framework at the desired level and ensures the existence of structured and suitable methodologies and systems for the timely and effective handling of risks.
- It monitors the Risk Indicators, is informed by the Risk Management Unit, and makes necessary decisions for preventative actions and measures, as well as corresponding actions for risk mitigation.

Risk Management Unit

The Risk Management Unit serves as the link between the Executive Management, the Company's Directorates/Units, and the Internal Audit & Risk Committee, and actively participates in the daily Risk Management of identified risks. Specifically, the role of the Risk Management Unit includes the following:

- Participates in the meetings of the Internal Audit & Risk Committee and informs its members on matters within its competence.
- Recommends for approval by the BoD, through the prior evaluation and approval by the Internal Audit & Risk Committee, the appropriate Risk Management Policy and Risk Appetite Framework and the changes deemed necessary.
- Ensures the recording, evaluation, and prioritization of identified risks and communicates risks to the Internal Audit & Risk Committee, emphasizing those of high importance.
- Is responsible for the methodologies, procedures, and appropriate tools of the risk assessment process.
- Provides active support for Risk Management to all the Company's Directorates and Units.
- Collaborates with other Directorates and Units, the Legal Services Department, the IT Security Manager, the Physical Security Manager, Regulatory Compliance, the Data Protection Officer, and Internal Control for mutual information and coordination regarding risk events or new risks that arise.
- Monitors trends and changes/developments in the market, diversifications in the legal and regulatory framework, changes in technology, and generally in the external environment, and recommends to the Internal Audit & Risk Committee necessary diversifications in Risk Management practices.
- Ensures that the acceptance of residual risks by the Administration is carried out based on the defined policies, procedures, and parameters and by appropriately authorized approving echelons.
- Compiles reports on Risk Management for the Executive Management, the Internal Audit & Risk Committee, and the Board of Directors (if required).
- Collaborates with the Human Resources Department for the organization of training of personnel in Risk Management.

Operational and Specialized Units

- Implement the Risk Management practices within their respective fields of action, managing their own risks.
- Proactively communicate and exchange information with other Units within the guidelines of Risk Management.
- Provide advice and specialized guidance on managing specific types of risks and the corresponding action plans of their subsidiary companies.
- Bear the responsibility for monitoring the implementation of the containment actions concerning the regularization processes of the subsidiaries they oversee.
- Assist where required in developing a culture of risk awareness, and notify the relevant information to the Risk Management Unit.

Regulatory Compliance Unit

- Supervises the compatibility of Risk Management practices in relation to the supervisory/regulatory framework.

Cybersecurity Unit (IT Security)

- Monitors, supervises, and actively coordinates the handling of risks arising from the operation of information systems.

Physical Security Unit

- Designs the framework for maintaining a high level of physical security and monitors and coordinates its implementation.

DPO

- Designs and supervises the Personal Data Management Framework.

Internal Audit Department

- Is responsible for providing appropriate independent assurance that Risk Management is operating reliably and has been implemented sufficiently and effectively. It reports to the Internal Audit & Risk Committee.

1.3 Risk Management Collaboration with Other Units and Companies of the Group

To achieve more effective Risk Management in the Company and throughout the Group, the involved parties are required to collaborate continuously and effectively. For this reason, there is an alignment of methodologies applied for Risk Management by the units that are part of the 2nd line of the Company. There is also communication between the units of the 2nd line regarding risk assessments conducted to minimize task repetitions of the same subject with the 1st line units. Continuous communication enhances the creation of more complete and consistent risk reports to the Management and the Board of Directors of the Company.

In relation to the Internal Audit Department (3rd line), the Risk Management Officer provides the Internal Audit with the results of the business risk assessment through the risk profile report, which is an important source of information for the annual Internal Audit plan as well as the prioritization of Internal Audit areas. It is noted that despite the interactions, Internal Audit remains independent in the selection of Internal Audit areas and the scope of the Internal Audit.

Regarding the subsidiary companies, the Risk Management Unit of the Company must receive updates regarding the operation of Risk Management of the subsidiaries, in order to support them in adopting correct/best practices following the provisions of legislation and the respective regulatory framework. To this end, the relationship between the Risk Management Unit of Growthfund and the corresponding Risk Management Units of the subsidiaries is governed by the "Collaboration Framework of the Risk Management Unit of Growthfund (RMU-GF) with the Risk Management Units (RMU) of the subsidiaries.

CHAPTER 2: METHODOLOGY OF RISK ASSESSMENT

2.1 Methodological Framework

The adoption of a methodological framework for risk assessment offers practical guidance on defining the fundamental principles for the assessment and management of risks. A robust framework establishes consistent risk management procedures allowing for substantive communication and decision-making.

2.2 Fundamental Principles

The following principles apply to the methodology of risk assessment:

- The implementation of the risk assessment methodology is coordinated by the Risk Management Officer.
- Risk assessment is carried out based on a five-level assessment scale (where one (1) is the lowest value and five (5) the highest possible value) with the participation of the involved structures of the Company.
- The stages of implementing the risk assessment methodology, the main categories of risks, and the grading scale can be modified if deemed appropriate. Any change/modification is approved by the Company's Board of Directors through the Internal Audit & Risk Committee, which also bears the overall responsibility for the operation of the Company's Risk Management.

2.3 Risk Assessment

The assessment of recognized risks occurs at two levels: a) Inherent and b) Residual.

2.3.1 Inherent Risk

The assessment of inherent risk pertains to the level of risk without considering the existence and adequacy and effectiveness of any control mechanisms applied to mitigate or eliminate the risk. Specifically, the calculation of inherent risk is based on the likelihood of the risk's occurrence and the impact of the risk (Probability X Impact) where:

(a) The probability of occurrence is an estimation of how frequently a specific risk can appear within a predetermined time frame. A five-level scale is used, where 1 represents the lowest value and 5 the highest.

(b) The impact is an estimation of the potential damage (impact) the risk's occurrence can have on the financial results and/or strategy and/or reputation of the functions under assessment. A five-level scale is used, where 1 represents the lowest value and 5 the highest.

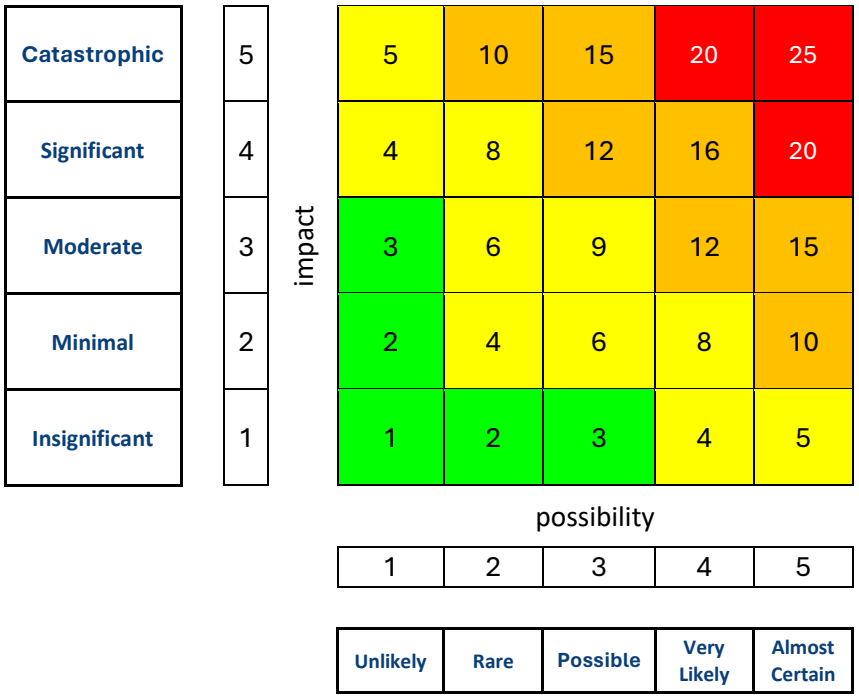
Criteria based on a five-level scale are used for estimating the probability of occurrence and the impact of the risk, as presented in Table A and Table B of Appendix 1.

The risks, based on the results of the Total Risk Grading (**Probability X Impact**), are collectively and diagrammatically displayed on a related graph—Risk Map (thermograph). The overall grading of risks defines the following classification areas:

- Low Risk Area
- Medium Risk Area
- High Risk Area
- Very High Risk Area

Risk Level Grading	Risk Grading
Low	1-3
Medium	4-9
High	10-17
Very High	18-25

The Inherent Risk Map (thermograph) is diagrammatically presented using a two-axis graph where horizontally the grading of the Probability of risks' occurrence is displayed and vertically the Impact of the risks. The grading is displayed in colors within the graph according to the respective scale.



The Risk Map (thermogram) helps in the optimal understanding of the overall Risk Profile and their prioritization based on their overall grading. Therefore, the ability to identify the most significant inherent risks and the optimization of Risk Management actions is provided.

2.3.2 Residual Risk

For the assessment of residual risk, the existence, adequity, and effectiveness of any Internal Audit mechanisms applied to limit or eliminate the risk are considered in order to ascertain whether safety locks exist, are sufficiently designed, operate effectively, and yield the expected results. The evaluation of both the adequacy and the effectiveness of the safety locks (Internal Audit mechanisms) is also the subject of the Internal Audit Unit and is reflected in the Internal Audit Reports of the Unit. Therefore, this specific information is taken into account for the rating of the Internal Audit mechanisms during the risk assessment process.

For the rating of Internal Audit mechanisms, evaluation criteria based on a five-point scale are used, which are detailed in Table C of Appendix 1.

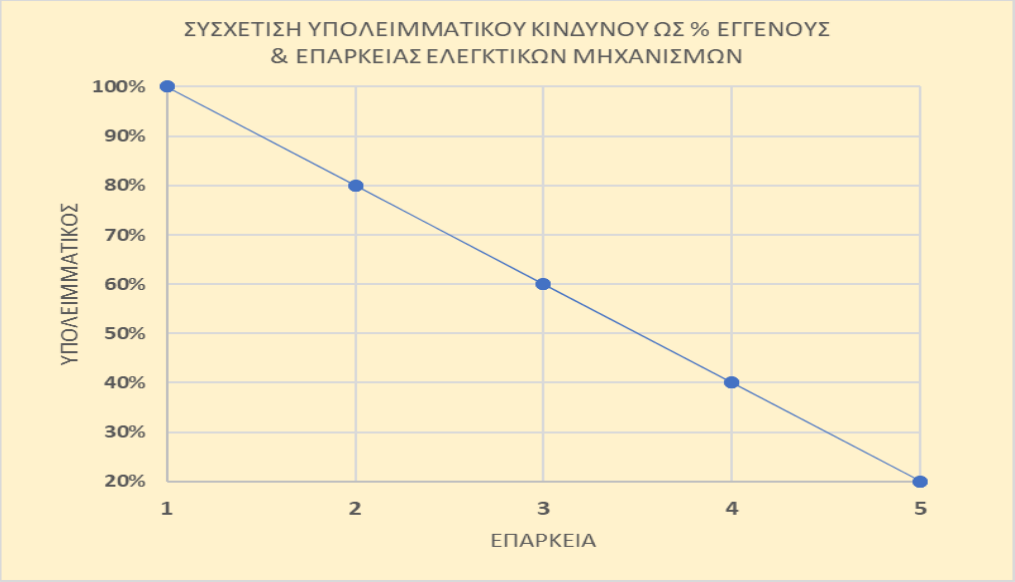
Internal Audit mechanisms constitute the means of ensuring the implementation of risk management actions of the Company. Such mechanisms concern the framework of policies and procedures implemented by the Company aiming at standardizing its operations and reducing exposure to risks, providing authorizations, approval procedures, verification processes, account agreements, and other practices of segregation of duties. They also play a significant role in the control mechanisms applied to the information systems.

The adequacy of Internal Audit mechanisms mitigates the inherent risk according to its gradation, and the lowest level (1) indicates a complete lack of internal control mechanisms, consequently the residual risk coincides with the inherent (100%). However, it is estimated that even at its highest value (5), it is not possible to completely eliminate the inherent risk. Empirical studies and statistical data determine the residual risk as around 20% of the inherent risk when the rating of the Internal Audit mechanisms approaches its maximum level (5).

The residual risk is calculated as follows:

Inherent risk - (Inherent risk * Rating of Internal Audit mechanisms / 5) + (0.2 * Inherent risk).

Consequently, the linear correlation between the adequacy of Internal Audit mechanisms and residual risk as a percentage of the inherent risk is illustrated in the following diagram:

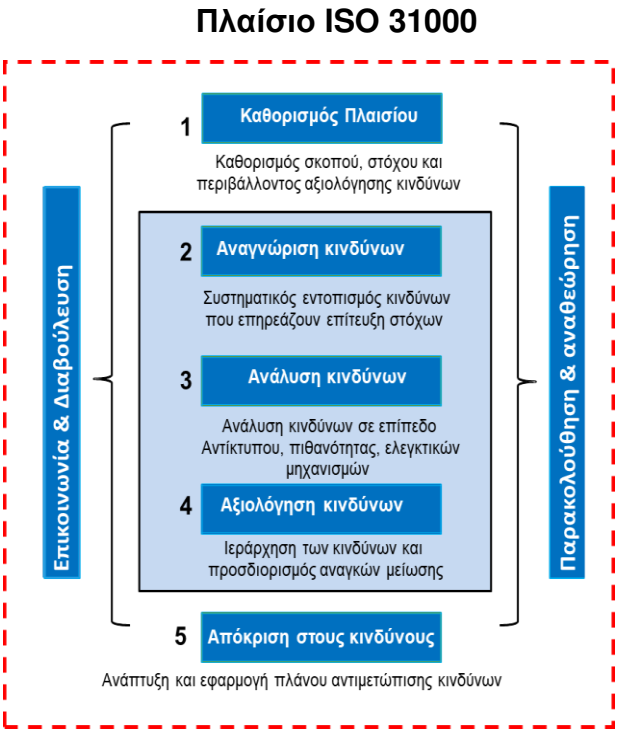


CHAPTER 3: RISK MANAGEMENT PROCEDURES FRAMEWORK

The risk management procedures implemented by the Company align with the international standard ISO 31000. The objective of these risk management procedures is to establish a common approach to risk management across all company activities and to enhance the flow of information to the responsible executives/bodies for decision-making regarding activities that impact risks.

More specifically, the Company applies the following procedures for Risk Management:

- Risk identification
- Risk assessment
- Risk mitigation
- Risk monitoring
- Risk reporting



3.1 Risk Identification

Based on documented activities and procedures, the main types of risks faced by the Company are identified and categorized according to the Company's Risk Typology. A regular review of the results of risk identification is conducted to ensure the continuous relevance of the identified risks.

The identification and recording of risks include, for example, conducting the following:

- Interviews with the responsible executives of the Company to understand all their functions and activities.
- A detailed review of all existing Policy manuals, procedures, and other useful elements and documents.

The recognized risks – depending on the nature of the respective activity – either stem from the Company's internal environment or from external factors. Therefore, the following distinction has been made for the effective monitoring of the source of each identified risk:

- **Internal Environment**: includes risks that originate internally from the operational environment of the Company and are indicative of human resources, internal technological and informational infrastructures, available financial resources, etc.
- **External Environment:** includes risks that originate from the external environment of the Company and are indicative of the general structure and development of the economy, the political regime, the legislative framework governing its operation, etc.

In some cases, the environment from which the risk originates may relate to both the internal and the external environment.

Initially, the relevant risks are identified and recorded in relation to the purpose and operational framework of the Company, the structure of Corporate Governance, and the specific activities of the Company. The risks are then mapped to the Typology of the Risk Registry and registered in the corresponding category in collaboration with the Heads of Operational Units. Appendix 2 presents the existing Risk Registry of the Company.

For the categorization of risks, the relevant standards for Risk Management and the best practices of risk grouping followed by major companies in Greece and abroad are considered.

The result of the process is the depiction/update of the Company's Risk Registry under the basic five (5) risk categories that the Company faces:

1. **Strategic Risk**

This risk significantly affects the ability of a business to achieve its strategic and business objectives. Consequently, it is the risk that affects the company's value and reputation and the ongoing viability of the business.

2. **Operational Risk**

This is the risk of corporate operations being ineffective and inefficient in executing the business model and achieving the operational goals of quality, cost, and time. It arises from inadequate or failed internal processes, people, and systems, or from external events.

3. **Compliance Risk**

Refers to non-compliance with laws and regulations, company-specified policies and procedures, resulting in degradation of quality, loss of revenue, unnecessary delays, sanctions, fines, legal entanglements, etc.

4. **Financial Risk**

Concerns the risk arising from inefficient management of cash flows and financial indicators resulting in minimized available liquidity, increased uncertainty from foreign exchange risk, interest rate risk, credit and other financial risks, and the inability to place available liquidity quickly and without loss of value where most needed.

5. **Information Systems Risk**

This is the risk that the information technology systems used by the Company do not operate according to their original design, jeopardizing the completeness and accuracy of data and information, exposing significant company assets to the possibility of loss or misuse, and jeopardizing the company's ability to support the operation of critical processes.

3.2 Risk Assessment

The identified risks are inherently and residually assessed by the responsible executives of the Company. A standardized methodology of self-assessment of risks and control mechanisms is applied (based on the methodology described in "Paragraph 3. Risk Assessment" of Chapter 2 of this document).

Specifically, inherent risk is analyzed as follows:

(a) Probability: The likelihood of occurrence is an estimate of how frequently a specific risk may occur within a predetermined time period.

(b) Impact: Estimation of the impact (potential damage) that the occurrence of the risk may have on the financial results and/or strategy and/or reputation of the functions under assessment.

The overall grading of each risk (inherent risk) is derived based on the values given to the likelihood of occurrence and its impact.

Subsequently, the results of the overall grading of inherent risks are classified on the relevant risk map (based on the methodology described in "Paragraph 3. Risk Assessment" of Chapter 2 of this document), where the following classification areas are defined:

- **Low Risk Area**

- **Medium Risk Area**
- **High Risk Area**
- **Very High Risk Area**

For the assessment of residual risk, the existence, adequacy, and effectiveness of any control mechanisms that are applied to mitigate or eliminate the risk are considered to determine whether safety locks exist, are adequately designed, function effectively, and deliver the expected results.

The types of control mechanisms are as follows:

- **Preventive:** Preventive Control Mechanisms are applied on a regular basis to prevent the occurrence of errors and irregularities. Examples include the need to use passwords and controlled access to systems or facilities, the need to supervise significant tasks, etc.
- **Detective**: Detective Control Mechanisms are designed to "detect"/identify deficiencies and errors once they have occurred. Examples include regular inventories and monthly agreements, payroll checks, conducting inventories, etc.
- **Corrective**: Corrective Control Mechanisms are applied to correct any errors or to prevent the performance of additional errors or irregularities. Examples include taking backup copies, signing insurance contracts, reporting errors to a higher hierarchical executive for corrective action to be taken timely, etc.

The same scale of risk grading used for the assessment of inherent risk is used for estimating residual risk.

The result of the risk assessment process is the depiction of the Company's Risk Profile, which includes the ranking of risks by their importance.

3.3 Mitigation of Risks

Based on the results of the risk assessment and the Risk Appetite Statement, the Executive Management proposes how to further manage the risks. The Internal Audit & Risk Committee is informed by the Risk Management Officer about the Risk Register, the scoring and ranking of all recognized risks, and the planned related actions to mitigate them. It reviews the Risk Register and the classification of risks, examines the planned measures, evaluates their effectiveness, and approves the submission of the Proposal of the Risk Management Officer to the Board of Directors for approval. For the risks that are decided to take further measures for their mitigation, more specific proposals are outlined in this direction. The Company uses a series of methods to reduce the risks in its activities, such as:

- Standards and operating procedures. The Company develops and improves on a regular basis operational standards and formal procedures to control and mitigate risks. Compliance with these operational standards of Strategic Planning is continuously monitored, while early warning mechanisms are applied to signal the possible increased risk from non-compliance with these operational standards.
- Training on risk issues. The Company provides its employees with training on risk, including courses and seminars on risks, specialized training on issues (such as information security, fraud, accessibility, etc.), and through internal communication initiatives.

The result of the risk mitigation process is the recognition of risks that require further actions along with proposals for their management.

3.4 Crisis Management

The Company is likely to face risks that lead to a crisis. A crisis is defined as an extraordinary event or series of events that can negatively affect the reliability of the Company, its services or products, its reputation or financial position, or the health of employees and the public, and which cause harmful and undesirable attention from the Mass Media or other business interest groups.

A crisis situation with a high degree of impact puts great pressure on the organization, which is called upon to face it by taking integrated, documented, and adequate decisions, and executing the necessary actions with precision and speed. Incorrect, delayed, or negligent/inadequate handling of a crisis can have serious negative consequences for the Company.

Growthfund considers it a primary obligation to its staff and all other stakeholders to be in a position to protect human life, the environment, society, the company's assets, and its reputation in the event of an emergency.

In this context, the recognition of a new risk that may cause very significant negative impacts on the Company and potentially lead to a crisis is immediately communicated by the Risk Management Directorate to the Management for the immediate decision-making and execution of the required actions based on a Business Continuity Plan.

3.5 Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

Growthfund's Business Continuity Plan aims to develop a preventive process that will keep the Company operational even in the event of a significant crisis, covering all aspects of the company, including operational processes and human resources. Correspondingly, the Disaster Recovery Plan focuses on ensuring data protection, preventing damage to systems, and recovering them as quickly as possible.

The Business Continuity Plan describes how Growthfund will continue to operate and serve its subsidiaries, even in the face of a dramatic event such as a natural disaster, a major information systems failure, or a cyberattack. The ultimate goal is the continuation of daily procedures, the progress of ongoing projects, meeting deadlines, and maintaining the company's reputation, even in the face of a crisis.

The design of the Business Continuity covers every aspect of the company, including:

- ✓ Operational processes — how a process can continue to function even if critical equipment or supplies are missing
- ✓ Human resources — how critical personnel can continue to perform their work if, for example, workstations are destroyed or there is no Internet connection
- ✓ Business partners (Subsidiaries and consultants) — how they can continue their cooperation with Growthfund if, for example, communication lines or road transport are not available

For successful crisis management, the Company:

- has planned for the implementation of action plans in anticipation of an impending crisis
- has defined predetermined roles, responsibilities, and responsibilities for its members
- has appointed a communication manager with the mass media
- conducts preparation and regular training of directors and all personnel
- has ensured the creation of specified reports and communications between executives and the extraordinary updating of the Management and the Board of Directors.

3.6 Risk Monitoring

The Company aims for the regular monitoring of identified risks, as well as their related impacts, and for this purpose maintains an advanced culture of risk examination, which includes two dimensions:

a) monitoring of action plan implementation and

b) development and monitoring of the evolution of risk indicators (Key Risk Indicators- KRIs) that are developed for the most significant risks that help in identifying increasing trends of risks.

Risk monitoring is continuously carried out by the involved executives. The Risk Management Responsible is in charge of coordinating actions to regularly conduct the process.

The result of the process is the recognition of changes in the Company's Risk Profile through the implementation of action plans to limit them and the monitoring of the evolution of risk exposure.

3.7 Risk Reporting

The Company places particular emphasis on being informed about the risks it faces and aims at the timely detection of their trends. Specifically, reports are conducted to the Management and the Board of Directors of the Company, which include the results of the risk assessment, the application of additional action plans, and the evolution of risk monitoring indicators.

Given that information on risks is monitored on a regular, extraordinary, or occasional basis, the reports that can be conducted follow the same frequency and are addressed to all appropriate levels of the company's hierarchy.

APPENDIX 1 – RISK ASSESSMENT CRITERIA

A. Probability of Occurrence

To estimate the likelihood of occurrence, the risk is rated on a scale between one (1) and five (5), where 1 represents the lowest value and 5 the highest, according to the following classification of Table A':

TABLE A'			
Probability Grading			
Scale	**Grading**	**Definition**	**Occurency**
1	Very Low	Unlikely to occur	Once every 10 years or more
2	Low	Minimally likely (rare) to occur	Once every 6-9 years
3	Medium	Possibly (likely) to occur	Once every 2-5 years
4	High	Very likely to occur	Annually
5	Very High	Expected, almost certain, usually occurs	Multiple times a year

B. Risk Impact

The impact constitutes an estimate of the risk's effect on the Company's strategy, compliance with regulatory and legislative environment, smooth operation, financial results, information systems, or a combination of all these categories. If the impact relates to more than one (1) category, the one deemed to have the highest risk level is selected. The impact is estimated and rated on a scale from one (1) to five (5) (where 1 represents the lowest value and 5 the highest) according to the categorization in Table B.

Διαβάθμιση Επίπτωσης Κινδύνου						
Κλίμακα	**Διαβάθμιση**	**Στρατηγική**	**Συμμόρφωση**	**Λειτουργία**	**Πληροφοριακά Συστήματα και ψηφιακές υπηρεσίες**	**Χρηματοοικονομικά**
5	Καταστροφική	Η βιωσιμότητα της Εταιρείας είναι αμφίβολη. Απώλεια εμπιστοσύνης κρίσιμων ενδιαφερόμενων μερών.	Επιβολή κυρώσεων από ρυθμιστικές και νομοθετικές αρχές που θέτουν σε μεγάλο κίνδυνο τη βιωσιμότητα της Εταιρείας. Σημαντικές αποκλίσεις στην εφαρμογή του εταιρικού πλαισίου χωρίς πλάνο ενεργειών για βελτίωση.	Η βιωσιμότητα της Εταιρείας είναι αμφίβολη. Αδυναμία συνέχισης των λειτουργιών της Εταιρείας.	Κρίσιμα πληροφοριακά συστήματα και υπηρεσίες δεν λειτουργούν, διακοπή εξυπηρέτησης πελατών και επιχειρησιακών λειτουργιών ή/και απώλεια κρίσιμων επιχειρησιακών και προσωπικών δεδομένων	Τα οικονομικά μεγέθη της Εταιρείας επηρεάζονται σημαντικά, σε σημείο που η βιωσιμότητα της Εταιρείας είναι αμφίβολη. Επανέκδοση οικονομικών καταστάσεων.
4	Σημαντική	Πολλαπλές αλλαγές στελεχών ανώτερης διοίκησης, αναδιοργάνωση, σημαντικές αλλαγές στο στρατηγικό πλάνο. Απώλεια εμπιστοσύνης μεγάλου μέρους ενδιαφερόμενων μερών.	Επιβολή κυρώσεων από νομοθετικές και ρυθμιστικές αρχές που πλήττουν σημαντικά την Εταιρεία. Σημαντικές αποκλίσεις στην εφαρμογή του εταιρικού πλαισίου με πλάνο ενεργειών για βελτίωση.	Ανάγκη άμεσης αλλαγής σε μεγάλο μέρος λειτουργιών της Εταιρείας. Σημαντικές διακοπές βασικών λειτουργιών της Εταιρείας.	Κρίσιμα πληροφοριακά συστήματα και υπηρεσίες παρουσιάζουν προβλήματα που τα καθιστούν εν μέρει λειτουργικά ή/και μη κρίσιμα πληροφοριακά συστήματα και υπηρεσίες δεν λειτουργούν, διακοπή δευτερευόντων/εσωτερικών επιχειρησιακών λειτουργιών ή/και απώλεια μη κρίσιμων επιχειρησιακών δεδομένων	Τα οικονομικά μεγέθη της Εταιρείας επηρεάζονται σημαντικά. Η Εταιρεία ανταποκρίνεται με δυσκολία στις οικονομικές της υποχρεώσεις. Σημαντικές παρατηρήσεις εξωτερικών ελεγκτών επί των εκδοθέντων οικονομικών καταστάσεων.
3	Μέτρια	Περιορισμένες αλλαγές στελεχών ανώτερης διοίκησης, σημαντικές αλλαγές στο επιχειρηματικό σχέδιο και στην υλοποίησή του. Απώλεια εμπιστοσύνης περιορισμένου μέρους ενδιαφερόμενων μερών.	Σημαντικές κυρώσεις από νομοθετικές και ρυθμιστικές αρχές στις οποίες η Εταιρεία μπορεί να ανταπεξέλθει. Περιορισμένες αποκλίσεις στην εφαρμογή του εταιρικού πλαισίου.	Ανάγκη περιορισμένης αλλαγής σε μεγάλο μέρος λειτουργιών της Εταιρείας. Περιορισμένες διακοπές βασικών λειτουργιών της Εταιρείας.	Μη κρίσιμα πληροφοριακά συστήματα παρουσιάζουν προβλήματα που τα καθιστούν εν μέρη λειτουργικά ή/και απώλεια μη κρίσιμων επιχειρησιακών δεδομένων	Τα οικονομικά μεγέθη της Εταιρείας επηρεάζονται αρκετά. Η Εταιρεία έχει κάποιες δυσκολίες να ανταποκριθεί στις οικονομικές της υποχρεώσεις. Παρατηρήσεις εξωτερικών ελεγκτών που επιφέρουν περιορισμένες αναπροσαρμογές στις οικονομικές καταστάσεις.
2	Ελάχιστη	Εκτεταμένες αναπροσαρμογές στο επιχειρηματικό σχέδιο και στην υλοποίησή του. Απώλεια εμπιστοσύνης μικρού μέρους ενδιαφερόμενων μερών.	Περιορισμένες κυρώσεις από νομοθετικές και ρυθμιστικές αρχές. Διερεύνηση εταιρικών υποθέσεων. Ελάχιστες αποκλίσεις στην εφαρμογή του εταιρικού πλαισίου.	Επηρεάζεται περιορισμένο μέρος των λειτουργιών της Εταιρείας. Αν και οι επιχειρηματικές λειτουργίες/ δραστηριότητες επηρεάζονται, δεν υπάρχουν σημαντικά εμπόδια και προβλήματα στη συνέχισή τους.	Περιορισμένες δυσλειτουργίες σε μη κρίσιμα πληροφοριακά συστήματα ή/και καθυστερήσεις σε επιχειρησιακές λειτουργίες	Τα οικονομικά μεγέθη της Εταιρείας επηρεάζονται σε περιορισμένο βαθμό. Η Εταιρεία έχει ελάχιστες δυσκολίες να ανταποκριθεί στις οικονομικές της υποχρεώσεις. Περιορισμένες ελλείψεις στη λειτουργία ελεγκτικών μηχανισμών ως προς τη χρηματοοικονομική πληροφόρηση.
1	Ασήμαντη	Περιορισμένες αναπροσαρμογές στο επιχειρηματικό σχέδιο και στην υλοποίησή του. Περιορισμένη επίπτωση σε ενδιαφερόμενα μέρη.	Συστάσεις από νομοθετικές και ρυθμιστικές αρχές. Δεν παρατηρούνται αποκλίσεις στην εφαρμογή του εταιρικού πλαισίου.	Επηρεάζεται μια μονάδα. Οι επιχειρηματικές λειτουργίες/ δραστηριότητες συνεχίζουν με ελάχιστα προβλήματα.	Χωρίς επιπτώσεις στη λειτουργία των πληροφοριακών συστημάτων και υπηρεσιών, χωρίς απώλεια δεδομένων	Τα οικονομικά μεγέθη της Εταιρείας επηρεάζονται ελάχιστα. Οι ελεγκτικοί μηχανισμοί λειτουργούν ικανοποιητικά ως προς τη χρηματοοικονομική πληροφόρηση.

C. Internal Audit Mechanisms

For the evaluation of the Internal Audit mechanisms, a five-point scale is used, based on their classification into one of the following categories (Table C):

TABLE C'		
Control Mechanism Grading		
Scale	**Grading**	**Description**
5	Very High	The Company considers the control mechanisms to be adequately designed and operationally effective.
4	High	The Company considers the control mechanisms to be appropriately designed and operational, but there is room for improvement.
3	Moderate	The Company considers that basic control mechanisms are in place, while there is considerable room for improvement.
2	Low	The Company considers that limited control mechanisms have been designed and implemented, resulting in a high level of risk and significant room for improvement.
1	Very Low	The Company considers that there are no control mechanisms in place, resulting in significant weaknesses and very substantial room for improvement.

APPENDIX 2 - RISK REGISTRY

RISK TAXONOMY	
1. STRATEGIC	
A1	Social / Political Risk
A2	Strategic (Direction / Management Support)
A3	Reputation / Public Image / Outreach / Customer Satisfaction
A4	Competition
A5	Concentration (customers, markets, products)
A6	BoD & Committees (structure & operation)
A7	Organizational Structure, Org Chart & Job Descriptions
A8	Internal Policies & Procedures
A9	Environmental, Social, Governance (ESG)
2. OPERATIONAL	
B1	Equipment & Infrastructure Maintenance
B2	Natural Disasters / Business Continuity
B3	Procurement - Third Parties - Supplier Dependency
B4	Quality of Products & Services
B5	Staffing (adequacy) / evaluation / training / succession
B6	Work environment - attraction - compensation - development
3. COMPLIANCE	
G1	Legal & Regulatory Risk
G2	Contract Risk (execution, compliance, disputes)
G3	GDPR & Data Confidentiality
G4	Health & Safety
G5	Fraud & Ethics
G6	Tax & Social Security Contributions
4. FINANCIAL	
D1	Capital Structure / Liquidity Management
D2	Budgeting & Monitoring
D3	Pricing Policy
D4	Credit & Collections (Credit Risk)
D5	Investment
D6	Management Reporting / Financial Statements
D7	Profitability
5. IT	
E1	Cybersecurity / IT Systems Security (Cyber Risk)
E2	Availability, Loss & Recovery of Data (DRP/BCP)
E3	Data Integrity - Data Quality Risk
E4	Technology Change Risk
E5	Transaction Processing Risk

** The Codes may be updated upon the completion of the specialized IT Risk Assessment Exercise conducted by Growthfund.*