HELLENIC REPUBLIC

2024

STANDARD OF RISK MANAGEMENT POLICY AND FRAMEWORK

October 2024

NATIONAL TRANSPARENCY AUTHORITY

EDITORIAL

This Standard of Risk Management Policy and Framework was prepared in accordance with the guidelines of the Interim Governor of the National Transparency Authority, Ms. Alexandra Rogkakou, under the guidance and coordination of the Head of the General Directorate of Integrity and Accountability, Ms. Maria Konstantinidou.

The project team consists of: Aspasia Fatsiadou, Head of the Directorate of Corruption Risk Assessment and Special Sectoral Anti-Corruption Strategies, Mr. Argyrios Tsomokos, Head of the Corruption Risk Management Department and the executives of the Corruption Risk Management Department, Ms.Adamantia Xouri, Ms. Kyriaki Perdikaki and Irini Koumbarouli.

Foreword by the Interim Governor of the National Transparency Authority

The ability of entities to identify and manage the risks that threaten their proper operation contributes to improving their efficiency and effectiveness, preventing corruption and strengthening integrity and good governance. Good risk management contributes to improved service provision through better decision-making, greater preparedness against unforeseen events and support for innovation.

The preparation of this Standard of Risk Management Policy and Framework , in accordance with the provisions of Law no. 4795/2021, is an important step for the public sector towards the uniform application of the institutional framework. In this innovative effort, particular emphasis is placed on the roles and responsibilities of all staff in relation to risk management, as well as on the analysis - with practical steps - of this process.

The Interim Governor
Alexandra Rogakou
Head of the Inspections and
Audits Unit

Contents

Introduction

All public entities, irrespective of their size, structure or responsibilities, face risks on a daily basis at all levels of their activities. As defined in article 3 of Law no. 4795/2021, *"risk" is defined as "the possibility or threat of damage, loss or, in general, a negative consequence for the objectives of the entity, which may be caused by both endogenous and exogenous factors and which can be mitigated by preventive actions and control measures".*

Entities should therefore be aware that risks have the potential to have a negative impact on their operations, including the making of wrong strategic decisions, operational errors, legal liabilities or financial uncertainty. While it is utopian to assume that all risks are avoidable, entities can control the scale and scope of the risks they wish to take on through effective risk management. By 'risk management', we refer to all the activities required to **identify the risks** faced by the entity, **assess** (evaluate and prioritise) them, **address them**, and **monitor** and **update** them[1].

Creating a culture of risk

In order to achieve effective risk management within an entity, it is first necessary to implement the relevant actions, as well as to develop a corresponding culture.

Risk culture refers to "values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people with a common purpose. This applies to all organisations - including public entities, governments and non profit organisations" [2].

Key parameters of the risk culture are:

Tone at the top: risk management must be supported and promoted by the leadership, as this reinforces its importance throughout the entity.

Accountability: staff at every level of the entity must recognise their responsibility for risk management and decisions must be made in awareness of the risks. For this reason, the roles of staff and the objectives of risk management should be clearly defined.

[1] Article 22B par. 3(b) of Act No. 4795/2021

[2] IRM https://www.theirm.org/what-we-say/thought-leadership/risk-culture/

Integrating Risk into Strategy: Risk management is an integral part of the strategic planning and decision-making process at all levels of the entity.

Communication: There is transparency and open communication throughout the entity regarding risks, as well as how to address them.

Awareness and Training: Staff and management are informed and/or trained about the importance and methods of risk management.

To ensure the effective integration of risk management into their operations, public sector entities develop and implement a Risk Management Policy and Framework[3]. The Risk Management Policy and Framework is subject to approval by the Head of the entity and is developed in collaboration with the risk management body.

The National Transparency Authority has defined the Standard of Risk Management Policy and Framework[4] that public sector entities must implement, adapting it to their specific characteristics and needs. This standard provides guidelines and instructions for drafting and implementing the Policy and Framework, with a view to ensuring uniform application of the regulation.

Part A'

Risk Management Policy

The Risk Management Policy is reflected in a document that guides the entity in making decisions and taking actions related to the management of the risks to which it is exposed.

The Policy outlines the management of risks by purpose and objective, the risk appetite and level of risk tolerance, as well as the roles and responsibilities of the relevant management levels, in relation to the design, monitoring and implementation of the Risk Management Framework[5]. The approval of the Policy by the head of an entity (Minister, Special Secretary of the Decentralised Administration, Governor of an Independent Authority, etc.) clearly demonstrates their commitment to integrating of risk management into the administrative practice of the entity and the objectives it serves.

[3] Article 22B of Law no. 4795/2021
[4] Para. 5 of article 22B of Law no. 4795/2021
[5] The risk management framework is developed in Part B herein

It is noted that risk management is not a distinct process/procedure within the entity, but should be an integral part of the culture of all entities' units, reflecting the way the entity operates and addresses challenges.

The Risk Management Policy should at a minimum be structured by the following sections with the corresponding content:

A. Purpose/ Head Declaration

The preamble of the Risk Management Policy should reflect the purpose and objectives pursued through it, as well as the statement by the leadership that risk management is an integral part of all procedures of the entities.

B. Roles and responsibilities

Risk management is not the sole responsibility of the risk management body. Instead, it is the responsibility of all staff within the entity. Everyone in the entity, from the senior management (Secretaries General, Directors General, etc.), the risk management body, to the Directors and employees, as well as the executives of the Internal Audit Unit, all contribute to creating an environment in which effective risk management can thrive. For this reason, risk management requires a clear definition of the roles and responsibilities of staff at all levels.

This section outlines the roles and responsibilities of entity's head and its senior managers and employees in relation to risk management.

More specifically:

The head of the entity is responsible for the following :

(a) the determination of the risk appetite and risk tolerance of the entity,

(b) the approval of the entity's Risk Management Policy and Risk Management Framework and ensuring the entity's compliance with the Risk Management Policy and Risk Management Framework,

(c) the integration of the risk management process into the entity's operations and service provision,

(d) the implementation of risk management strategies to address the risks of the entity,

(e) the priority treatment of very high (extreme) risks to the objectives and operation of the organisation,

(f) any other action resulting from the existing institutional framework regarding risk management and the operation of the Risk Register (such as approval of risk management measures, introduction of new risks in the Register, etc.).

The risk management body is responsible for:

the exercise of its competences, as described in Article 22D of Law No. 4795/2021, and in particular:

a) the recommendation of the Risk Management Policy to the head of the entity,

b) the development, monitoring and updating of the entity's Risk Management Framework, in accordance with its strategic and operational objectives,

(c) informing and instructing the staff of the entity on how to identify and address risks in the exercise of its competences and monitoring the audit mechanisms,

(d) the supervision of the risk management process carried out by all the entity's units,

e) the maintenance, continuous monitoring and updating of the Risk Register of the entity and the provision of guidance to the other entity's units,

(f) the submission of periodic and ad hoc reports to the head of the entity on the risks to which the entity is exposed; and

(g) submitting an annual report to the entity's head, which it will be notified to the National Transparency Authority.

The Internal Audit Unit is responsible for:

(a) providing reasonable assurance on the adequacy and effectiveness of risk management as a fundamental component of the entity's internal audit system[6],

[6] Article 22A of Law no. 4795/2021

(b) assessing the effectiveness of the existing risk audit safety nets within the entity in the context of its projects,

(c) an assessment of the effectiveness of the risk management processes throughout the entity and in particular whether:

- the Risk Management Policy and Framework is applied,
- significant risks are identified and assessed,
- appropriate measures are selected to address the identified risks, depending on the acceptable risk tolerances of the entity.

Heads of entity's units at all levels are responsible for:

(a) the implementation of the Risk Management Policy and Risk Management Framework in the entity's unit to which they belong, as well as the risk management measures within their entity units,

(b) the proper integration of the risk management process into the business processes under their competency,

(c) identifying the risks that threaten the achievement of the objectives of the entity unit they head, their causes and their consequences,

(d) evaluating existing audit mechanisms and proposing additional audit mechanisms/risk mitigation measures within their competency,

(e) monitoring the risks (existing and emerging) that fall within their area of responsibility,

(f) the ongoing support, training and awareness-raising of staff so that they understand their role and competences, as well as the risks related to their area of responsibility.

In addition, the Heads of Directorates General are also responsible for:

(a) ensuring the cooperation of the Directorate General with the risk management body and the actions required in this context,

(b) any other action resulting from existing institutional framework regarding risk management and the operation of the Risk Register (such as approval of risk management measures, introduction of new risks in the Risk Register, etc.).

Employees are responsible for:

(a) compliance with the entity's policies, procedures and guidelines for risk management,

(b) monitoring the implementation of the control mechanisms in their area of responsibility and reporting incidents of non-implementation or incorrect implementation to their immediate superiors,

(c) identifying potential risks in the exercise of their day-to-day competences and reporting them to their immediate superiors.

General obligations

In addition to the above, all personnel of the entity, regardless of their role, have some general responsibilities, which are crucial for the successful implementation of risk management in the entity. These obligations are:

(a) participate in risk management education and training activities to keep abreast of best practices, institutional requirements and policies of the entity,

b) to comply with the Code of Ethics and Professional Conduct for Public Servants and any other Codes of Conduct of their entity,

(c) in the exercise of its competences, comply with the applicable laws and regulations of the entity regarding the confidentiality of information, as well the applicable institutional framework for the processing of personal data.

It is noted that the responsibilities of each role, as regards the completion of the Risk Register[7] of the entity, are further specified in the Joint Decision of Art. 4795/2021. In any case, the above roles must be completed and harmonised in accordance with the applicable institutional framework concerning risk management.

[7] Para. 3 of Art. 4795/2021

Γ. Risk Categories

The risks faced by entities can be categorised according to the nature of their characteristics. The categorisation of risks helps: **a)** to create a structured approach to risk assessment, ensuring that key areas of risk in the entity are not overlooked; **b)** to better understand the nature and source of each risk, facilitating more effective risk assessment and management; **c)** to identify areas and operations where there is a high concentration of risk; and **d)** to design and implement targeted and appropriate risk response strategies for each category.

In this section, the categories of risks are listed. The following categories of risks will be mandatory in the policy document of each entity, each of which may be further subdivided into subcategories for better monitoring.

Natural or non-natural disaster risks: Risks in this category refer to major external contingent events threatening life, health, people, property or the environment, which may directly or indirectly affect the operation of the entity.

Examples: extreme weather events, extreme natural phenomena, pandemics, terrorist attacks.

Strategic risks: Strategic risks refer either to internal and external events that can prevent or hinder an entity from achieving its goals and strategic objectives, or to risks arising from the entity's strategic choices.

Examples: risks due to changes in the economic environment (price level increases, interest rate hikes, liquidity shortages, etc.), risks due to changes in the political environment (change of government, minister, or elected local government official), risks due to the unexpected performance of a major project (misjudgment of the capabilities or resources required for the project's completion, unforeseen technical difficulties or problems arising during project implementation, budget overruns, failure to meet quality specifications, negative impacts on sustainability and social welfare)."

Operational risks: These are risks that affect the entity's operational functions through which it carries out its competences and over which it has direct management responsibility and control. They are risks that may arise from the entity's internal processes, human resources, governance and management oversight, lack of effective and efficient decision-making and leadership structures leading to the loss of critical milestones for the entity, etc.

Examples: inadequate or ineffective procedures that may lead to loss of resources or poor quality service provision to the citizen; incorrect or incomplete procurement procedures resulting in substandard services or goods; errors or omissions by staff due to lack of appropriate training and skills; high staff turnover rates leading to loss of institutional knowledge and disrupting continuity in the operation of the entity; poor communication between staff or with the interacting public; lack of guidance due to inadequate policies, which may lead to wrong decisions or unauthorised activities, errors in procedures due to non-adherence to administrative practices, etc.

Information technology risks: This category refers to risks that may arise from ineffective approaches to technology management and implementation (policies and procedures), as well as from weaknesses in information technology systems.

Examples: IT system not functioning for a long period of time; failures in critical IT systems; system failure due to old equipment, poor maintenance or software errors; failure to manage information security resulting in the compromise of sensitive information; incidents of privacy breaches; data leakage; breach of security policies; cyber attacks.

Financial risks: This risk category refers to events/threats that may jeopardise the financial objectives of an entity[8].

Examples: The entity's denial of its public claims against third parties, the entity's assumption of public obligations without the ability to meet them, inadequate authorization for expenditures or approval limits that are overlooked, financial

[8] Also relevant is the Commission's Decision No. FG8/55081/2020 decision of the Plenary of the Court of Auditors (B' 4938)

inaccuracies, failure to comply with basic financial policies and procedures, waste, loss or misuse of the entity's assets.

Legal/regulatory/compliance risks: These risks relate to the non-implementation or poor implementation of the public entity's institutional framework, regulations, contractual terms, standards or internal policies that could lead to direct or indirect administrative liability, civil or criminal penalties, regulatory sanctions or other negative impacts, such as the impact on the reputation of the entity.

Examples: failure to record procedures regarding the management and protection of citizens' personal data, failure to enforce an irrevocable court decision, breach of contract, causing damage, injury or death of a third party in the course of the entity's activities resulting in damages, non-compliance with labour legislation (on safety, discrimination, wage), which may lead to legal action and fines, non-compliance with the Code of Ethics and Professional Conduct for Public Servants.

Health and safety risks: This category refers to risks that affect the health and safety of workers.

Examples: accidents at work due to lack of supply of personal protective equipment, poor maintenance of machinery equipment and lack of training, ergonomic hazards, unsuitable working conditions, exposure to chemicals and communicable diseases, workplace stress, lack of hygiene in public facilities.

Risks of corruption and fraud

In law no. 4795/2021 there is a specific reference to the risks of corruption and fraud. According to the OECD corruption is *"the abuse of public or private office for personal gain. The active or passive abuse of the powers of public officials (appointed or elected) for financial or other gain"*[9].

[9] OECD, Greece - OECD Anti-Corruption Technical Assistance Programme (2019), *Guidelines for the Preparation of Sectoral Anti-Corruption Strategies in Greece*

The concept of fraud, on the other hand, is defined in Greek legislation in article 386 of Law no. 4619/2019 (P.K.). Articles 386A and 286B further define computer fraud, as well as fraud concerning grants.

This is a specific horizontal category of threats linked to abuses of power, which may affect the functioning of the institution in the performance of its purpose, in the short and long term, and may have a negative impact on its reputation, revenues and the quality of the services provided to citizens etc.

In the same vein, Transparency International[10] points out, focusing on the consequences of corruption, that "it is harmful to society, deepens inequalities, erodes citizens' trust in public institutions, undermines good governance and social justice, and poses a serious threat to the rule of law, democracy and fundamental rights"[11].

Therefore, corruption and fraud risks may be inherent in and associated with all the categories of risks mentioned above [e.g. legal/regulatory/compliance risks - when breaking the law; health and safety risks - increasing the likelihood of accidents; operational risks - corruption in recruitment, staff movements; information technology risks - concealment of important data; financial risks - misappropriation of an entity's assets] [12].

It should be noted that public sector entities, according to Art. 4795/2021, public sector bodies are obliged to send data to the National Transparency Authority regarding corruption risks for the purpose of updating the Central Corruption Risk Repository.

Examples of corruption: Bribery/accepting bribe, offering to influence, abuse or misappropriation by a public official, money laundering, illicit enrichment[13], conflict of interest, failure to follow procedures, abuse of power, unfair or unequal treatment.

[10] https://www.transparency.org/en/what-is-corruption
[11] Similarly
[12] https://www.u4.no/topics/corruption-risk-management/basics
[13] Laws 3560/2007 and 3666/2008

D. Risk appetite

All entities face both internal and external risks in their operations, which they cannot fully eliminate and therefore will have to manage in order to achieve their objectives, and there will be risks that they will accept.

Risk appetite is defined as "*the type and amount of risk an entity is willing pursue or retain*[14]" in order to achieve its objectives. The Risk Appetite Statement, which is approved by the Head, expresses how much risk an organisation is prepared to take (the 'risk') in pursuing its objectives, ensuring a balance between the benefits sought and the potential risk.

The Risk Appetite may also be expressed by risk category, as the categories are analysed in the previous section, following the following scale. This approach allows focusing on each category separately, assessing and addressing risks in the most effective way.

Risk Appetite Scale

Very high (extreme) risk appetite

The entity considers that the potential benefits of this 'aggressive' risk-taking outweigh the potential negative consequences, and is therefore willing to take the associated risk to achieve its objectives.

Attention! Public sector bodies cannot assume too high a risk appetite, on the one hand, because of their mission, which is to serve the citizen, and on the other hand, because of their obligation to comply with the principles of sound financial management.

High risk appetite

The entity is willing to take greater than normal risks and accept some negative consequences in order to achieve its objectives.

Moderate risk appetite

The entity shall adopt a balanced approach to risk-taking. Potential negative impacts and the achievement of its objectives shall be shall be given equal consideration.

[14] ISO Guide 73:2009 Risk Management - Vocabulary

Low risk appetite

The entity takes a cautious approach to risk-taking and is prepared to accept only minor negative impacts in pursuit of its objectives.

E. Risk tolerance

In this section, the risk tolerance by risk category is defined.

Risk tolerance is defined as *"the readiness of an organisation to assume the remaining risk, after measures have been taken to address it, in order to achieve its objectives"* [15].

This term therefore indicates a level of deviation from the risk appetite that an entity is willing to assume. Consequently, risk tolerance can be defined as a specific and predetermined range of deviation from the risk appetite.

Example: the entity is willing to tolerate the risk remains after all mitigation measures have been implemented because there is a compelling need, such as responding rapidly to emergencies, meeting important strategic objectives or meeting tight deadlines to complete a critical project.

It should be noted that risk tolerance is sometimes limited by institutional and regulatory arrangements, such as health and safety legislative requirements.

Risk tolerance may relate to subcategories of risks or to individual risks, specific projects, individual objectives, initiatives, etc., so as to take into account the specificities of each risk, project or risk area (subcategory).

For the uniform application of the provisions of Law no. 4795/2021, institutions should apply the risk appetite graduation as reflected in this text.

[15] ISO Guide 73:2009 Risk Management - Vocabulary

Relationship between Risk Appetite and Risk Tolerance

Example

Public Entity: Ministry X

Risk appetite in the category of information technology risks

"As public sector bodies committed to serving citizens with integrity and security, we have a low risk appetite for our IT initiatives and operations. We prioritise the protection of sensitive data, the continuity of our services and the trust of citizens. As such, we will avoid adopting cutting-edge technologies without thorough testing and proven security. Our investment in new IT solutions will be prudent, favouring established technologies with a strong track record of reliability and security. As a result, the risks we are willing to take in this category are of a magnitude of 1-2 (based on the importance scale we have provided)[16]".

Risk tolerance

Despite the entity's low risk appetite for unproven technologies, due to the growing need for remote working capabilities, it is decided to introduce an innovative cloud-based system. This system promises significant improvements in efficiency, scalability and remote accessibility. For this project, the public body is prepared to tolerate risks with a magnitude of 3-7 (based on the importance scale we have provided)[16], a level higher than the risk in the information technology risk category.

[16] See. Scale in the section *Defining Risk Criteria*

Part B

Risk Management Framework

The Risk Management Framework contains the guidelines and organisational arrangements for **the design, implementation, evaluation and continuous improvement of the entity's risk management, as well as the methodology for conducting the risk management process**.[17] The main purpose of the Framework is to support the entity in integrating risk management into existing organisational structure and business operations. This ensures that risk management is not a stand-alone function, but is seamlessly integrated into the day-to-day operations and decision-making of the organisation. Since this integration is the main purpose of the Framework, factors such as the size of the entity, its business activity as well as its organisational structure should be taken into account in the design process.

The Risk Management Framework shall be monitored and evaluated in terms of its implementation by the risk management body, which shall recommend to the Head the revision and updating of the Risk Management Framework if it finds that it is no longer aligned with the strategic and operational objectives of the organisation.

Evaluation may include monitoring key performance indicators, conducting audits and gathering feedback from involved/participating parties. Improvement, on the other hand, focuses identifying opportunities to increase the efficiency and effectiveness of risk management in the organisation. By analysing the results of the assessment, operators can identify areas for improvement or adaptation in their risk management, implement necessary changes and promote a culture of continuous progress. This ensures that the Risk Management Framework remains dynamic, responsive and continuously aligned with the evolving needs and objectives of the entity.

The participation and awareness raising of the staff of the organisation is a key element for the successful implementation of the Framework.

For the implementation of the above Framework, which sets out the general principles and guidelines for the proper integration of risk management, the entity shall develop an implementation plan (draft), which is a detailed document that describes at least:

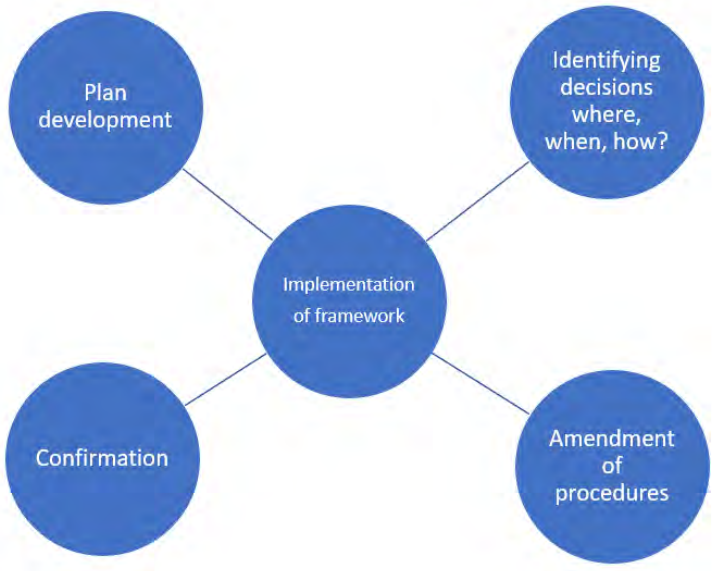
[17] Para. 3 of article 22B of Law no. 4795/2021

- the approach and procedures for identifying, analysing, assessing, evaluating, addressing and monitoring risks in alignment with the organisational objectives of the organisation,
- the necessary human, financial and technological resources and the timetables for implementing the plan,
- the communication and reporting mechanisms.

The development of the plan ensures that the organisation's arrangements and procedures for risk management are understood and put into practice. Alongside appropriate design and implementation, the Risk Management Framework ensures that the risk management function is an integral part of activities throughout the entity, including decision-making, and that changes in its internal and external environment are adequately captured.

Figure 1. Risk Management Framework Implementation Plan

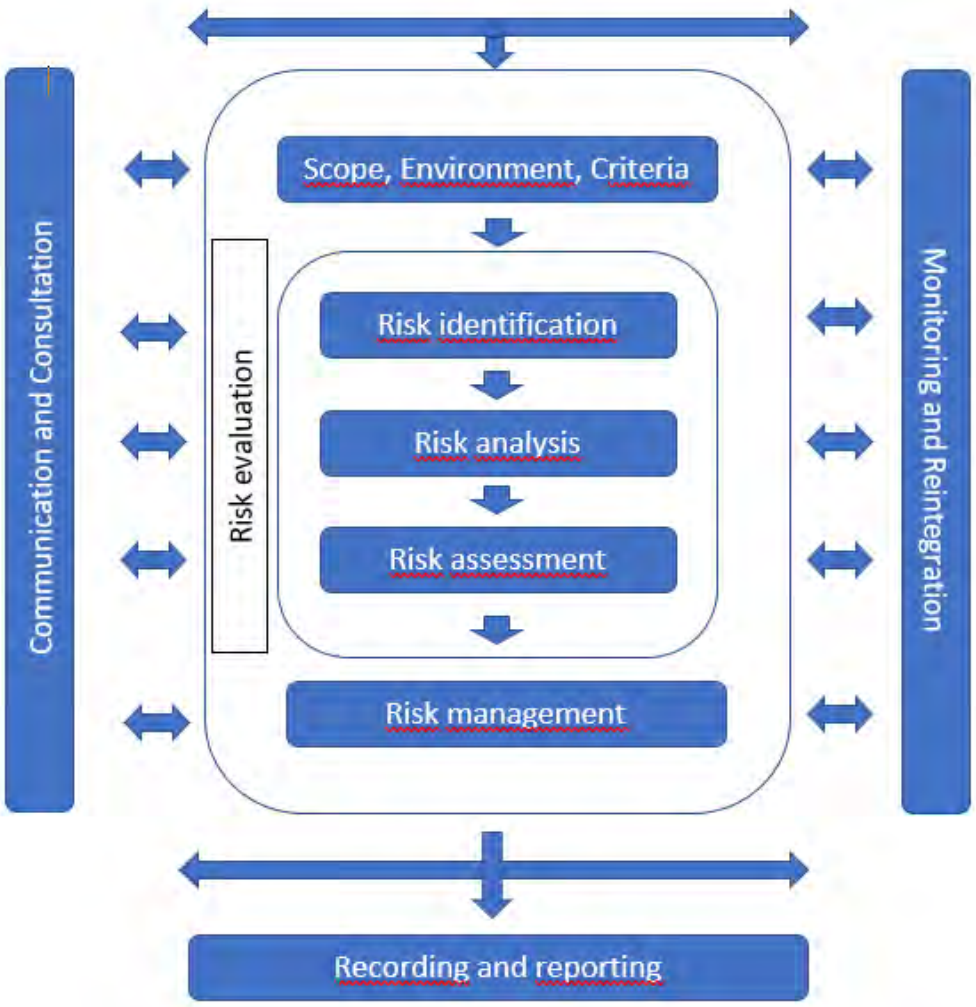
Risk Management Process - Methodology



The Risk Management Framework shall include a summary description of the risk management methodology that the entity applies. Examples, questionnaires, etc. may be provided to further support the staff involved in risk management, in accordance with the roles already defined by the entity in its Policy. 4795/2021.

ISO 31000:2018 "Risk Management - Guidelines" describes the risk management process as a set of steps that are carried out in a coordinated, but not necessarily sequential, manner. The figure below lists the stages of the risk management process, which will be briefly described below.

Figure 2. Risk management process (based on ISO 31000:2018)



Scope of Application, Environment, Criteria

The first step in the risk management process is "setting the context". This includes defining the scope, the internal and external environment of the entity, and the risk criteria.

Step 1a: Define the scope of risk management

The entity's risk management process may focus at the strategic, operational or other organisational level or at the project or programme level. Choosing the appropriate scope is a critical step for all subsequent activities, as it ensures the best use of time, effort and

resources of the organisation.

By clearly defining the scope at the appropriate level, an entity can ensure that risk management activities are targeted and inclusive of all significant risks.

For this reason, the first step in the process is to clearly define the scope of the risk management framework.

Fields of Application:

Strategic level: It refers to the management of risks that may affect the overall direction and strategic objectives of the organization.

Operational level: Refers to operational functions either as a whole or to a specific department or operation within the body. For example, the risk management activities in Department A, with a focus on risks related to its processes and responsibilities.

Project level: Here, the scope is narrowly defined around a specific project and may include managing risks related to its timelines, budget, quality and expected outcomes.

Programme level: when it is a series of linked projects, the scope may include the whole programme. This could include managing interdependencies, aligning the objectives of individual projects with objectives of the programme and coordinating resources across multiple projects.

For public sector bodies, the risk management process should be applied, as a minimum, at the strategic and operational level. It is recommended that risk management is applied to major projects or programmes.

Step 1b: Defining the Environment

The definition of the environment can be understood as a "map" that captures the key factors that affect the operation of an entity and consequently the range of risks to which it is exposed. Such factors in the internal environment of the entity include governance, budget, organisational structure, regulations and organisational culture. Similarly, the legislative, political, regulatory, financial, technological, climate and natural events are important factors in the entity's external environment.

This step is fundamental to the risk management process, which take into account the operating environment of the entity. Otherwise, risk management strategies may be flawed, superficial or fail to address the most important and relevant risks to the entity, leading wasted resources and potential failure to achieve its objectives. At the same time, the above factors may constitute significant sources of risk.

The risk management framework should capture the identification of the environment as a step in the risk management process, with indicative questions.

Indicative questions to identify the environment

Indoor Environment:

1. What is the organisational structure of the entity?
2. What is its budget for next year and what are the main sources of funding?
3. Is there a framework for identifying the training needs of staff?
4. What are the organisation's information systems and how adequate and up-to-date are they?
5. How would you describe the organisational culture of the entity?

External Environment:

1. What planned legislative changes may affect the entity?
2. Are there any major technological trends and developments that may applied to the organisation or affect its operation?
3. How do the economic conditions of the country affect the operation of the entity?
4. Is there a risk of natural disasters in the area where the entity operates?
5. Are there any significant political, geopolitical, demographic developments and trends that may affect the realisation of the objectives of the organisation?

Step 1c: Defining Risk Criteria

The risk criteria, as described in this section and in Annex 2, should be clearly reflected in the risk management framework. On the basis of these criteria, the significance or magnitude of a risk is assessed and therefore entities are able to prioritise risks and allocate appropriate resources to address them.

Furthermore, the establishment of criteria facilitates effective communication between the organisation's risk management staff involved in risk management, as it allows for a common understanding of their importance and provides a benchmark for evaluating the effectiveness of risk management actions and measuring progress over time. Risk criteria are dynamic and should be continually reviewed to remain appropriate and up to date.

For example, the risk criteria may state that any event with a potential economic impact of more than €1 million and a probability of occurring more than 50% or twice in the next year is considered a "high" risk.

In particular, risk criteria support decision-making such as:

- How to decide that a risk has been adequately controlled.
- When a risk is not acceptable.
- When the potential benefit is sufficient to make a risk acceptable.
- How risks are prioritised and the resources needed to manage them are allocated.
- When the head of the organisation, the management bodies (Board of Directors, General/Special Secretaries) and the higher hierarchical levels of the organisation's management (such as Directors General) should be informed immediately.

The risk criteria are expressed on a scale with the corresponding description of each tier and the numerical value corresponding to that tier, and are generally relevant:

- The scale of the probability of occurrence of the risks.
- The impact of risks.
- Grading the effectiveness of the control mechanisms.
- The classification of risks.

The risk criteria are detailed in Annex 2.

It is noted that,

- The application of the proposed gradations (scales) is mandatory for all public sector entities falling under the provisions of Law no.4795/2021.
- The descriptions of the impact of the risks listed in Annex 2 are indicative and are intended to guide the risk management bodies in the design of the relevant criterion.

Risk assessment

Risk assessment is the overall process of **risk identification, analysis and evaluation**, which is carried out systematically and iteratively, with the cooperation and utilisation of the knowledge and opinions of interested parties (staff, experts, professional organisations, etc.).

Risk identification

Risk identification refers to the identification, recognition and description of risks that may adversely affect the achievement of the entity's objectives, their sources[18] (causes), and their possible consequences for them. In identifying risks, consideration is given to what might happen, why it will happen, where it will happen and how it will happen. Since the internal and external environment of an entity is constantly changing, the risks, as indicated below, are reviewed and revised periodically.

Risk identification requires knowledge of the operational/policy area of the entity, the legal, social, economic, political and technological environment, the processes and systems supporting its operation (such as information systems), as well as its organisational structure. Various techniques are used to identify risks (brainstorming, Delphi, root cause analysis, surveys, interviews, SWOT analysis, etc.), which draw on the knowledge and experience of interested parties. It should be noted that, during this phase, risks are identified without taking into account whether the entity has adequate control mechanisms in place.

[18] A distinction is often made between sources of risk and causes of risk, which refer to events that directly lead to the occurrence of a risk - e.g. an employee opens an email containing malware files, resulting in the leakage of sensitive personal data - and factors that indirectly lead to or enhance the occurrence of a risk (risk drivers), e.g. lack of training of employees to protect themselves from cybersecurity threats, outdated cybersecurity systems, etc.

Risk identification: Example

Corruption risk: Accepting Bribe
A public servant accepts a bribe or receives any form of compensation in order to favour a specific supplier.
Indicative sources of risk
Inadequate oversight mechanisms
Opaque procurement procedures
Weak institutional framework/Non-implementation of the institutional framework
Culture of impunity/lack of anti-corruption policies
Low wages/public servants hard times
Risk Identification Process
Gather the views of interested parties. Make good use of the experience and knowledge of your executives. You can use simple techniques such as brainstorming - structured, semi-structured interviews etc.
Overview of audit findings: Search for corresponding incidents through your available resources.
Process analysis: Analyze procurement processes, step by step, to identify potential vulnerabilities.
Remember the environment of the entity: Review the wider external and internal environment in which the entity operates. For example, factors such as the tolerance of corruption by citizens or the lack of motivation and low morale of employees may contribute to the occurrence of corruption.

Risk analysis

The second step of risk assessment is risk analysis, i.e. a deeper understanding of its nature and characteristics, as well as its significance. Risk analysis involves three (3) key sub-steps, which should be captured in the entity's risk management framework:

Stage 1º: assessing the likelihood and impact of the occurrence of the risk in the absence of control/mitigation measures. This step is referred to as the inherent risk assessment.

The entity assesses each risk based on two parameters:
- the **likelihood** of the risk occurring,

- **the impact** that the occurrence of the risk may have,

without examining, at this stage, any existing audit mechanism (existing procedures, policies, etc. already in place by the entity to address the risks).

Probability relates to how often a particular risk event is considered likely to occur within a given period of time and impact relates to the consequences that the risk may have if it occurs. The above assessment is made on the basis of the respective ratings (risk criteria) which, as mentioned above, are also defined in the risk management framework.

The calculation of the level or significance of the **inherent risk** is the result of the following product:

It is recalled that the corresponding scales (see risk criteria) have been given numerical values. For example, an inherent risk, whose probability is assessed as **probable, having a numerical value of 3**, and whose impact is assessed as **significant, having a numerical value of 4**, is given an importance rating of **3 x 4 = 12.**

Factors that are normally taken into account when assessing the probability of risks occurring:

- **Historical data:** Previous incidents or occurrences of similar hazards
- **Expert judgement:** findings and opinions of individuals or groups with specialised knowledge or training
- **External factors:** Economic, environmental, political or social trends
- **Indicators:** Early warning signs or triggers that signal an increase in the probability of risk
- **Feedback from :** Views from people who are affected by or have an interest in the outcome

Factors that are normally taken into account when assessing the potential consequences of a risk:

- **The scope of the impact:** How widespread the impact could be (e.g. local or national)
- **Economic impact:** Potential economic losses or additional costs incurred
- **Reputation effects:** Potential negative impact that the risk may have on the reputation of the entity
- **Operational implications:** Potential disruption to normal operations/processes or to the ability to provide products/services
- **Impact on interested parties:** Impact on workers, citizens or other interested bodies
- **Health and safety impacts:** potential harm to the health and safety of workers or persons/groups associated with the organisation and the services it provides
- **Regulatory and legal implications:** Fines imposed or other legal consequences due to the occurrence of the risk
- **Environmental impact:** Impacts on environment , including sustainability problems
- **The duration of the impact:** how long the impact may last e.g. short term disruption, long term or permanent changes

Step 2º: Identify and assess the effectiveness of the existing audit mechanisms in place to mitigate the risk.

Audit mechanisms refer to any action or process implemented by an entity to manage risks and enhance the probability of achieving its stated objectives and targets. An accurate assessment of the adequacy and effectiveness of audit mechanisms is important for the final assessment of residual risk. When assessing the effectiveness of audit mechanisms, it is essential to consider the views of the managers responsible for their implementation, on the one hand, and of information on their effectiveness and consistent application, on the other hand, through audits carried out for this purpose and by using existing data on their effectiveness (how they have worked in the past in similar incidents). At the same time, the audit mechanisms must be evaluated in terms of cost-benefit, as an effective mechanism must also be cost-effective.

The roles of the three (3) lines are listed in relation to the evaluation of the checks and balances.

First line of roles:

- Implement and monitor the audit mechanisms established for risk management in their area of responsibility.
- Identify potential failures of existing audits in their area of responsibility.
- Implement corrective actions to address deficiencies in procedures and audit mechanisms.

Second line of roles:

Informing and guiding the entity's staff on the monitoring of the audit mechanisms.

Third line of roles:

Evaluate the effectiveness of existing risk control networks within the organisation within their projects.

A related scale regarding the adequacy of the audit mechanisms is provided in Annex 2 (risk criteria).

Stage 3º

Assessment of the level/significance of residual risk

In risk management, the probability and impact scale is used to determine the level of a risk. If you have an inherent risk with a score of 5 in probability and 2 in impact, the inherent risk is rated 10.
The adequacy of controls reduces the risk you face, i.e. the residual risk. The greater the adequacy of the control, the lower the level of risk.
Consequently, for each level of adequacy of the control there is a corresponding reduction in the final risk score. A simple approach to accurately calculate the reduction is as follows:
Let's say that each proficiency level reduces the risk by a certain percentage from the initial rating:
Very Low Adequacy: 0-10% reduction
Low Adequacy: 10-25% reduction
Medium Adequacy: 25-50% reduction
High Adequacy: 50-75% reduction
Very High Adequacy: 75-90% reduction
Thus, for an initial risk with a score of 10, if the control has a moderate adequacy (3), it can reduce the score by 25-50%, i.e. bring the final score between 5 and 7.5.

Having assessed the adequacy and effectiveness of the existing controls, the entity is in a position to make an assessment of the residual risk. As a general rule, the controls reduce the likelihood of the risk occurring. However, some controls reduce the impact of the risk when it occurs. For example, a business continuity plan may reduce the impact of a natural disaster, but not the probability of its occurrence. When assessing the residual risk, the probability x impact product is recalculated, taking into account the configuration of the two parameters, based on the assessment of the checks and balances.

Risk assessment

The risk assessment is the final stage of the assessment, where the information from the previous stage is used and, through predefined acceptance criteria, the organisation decides whether the residual risk is acceptable in the current situation or whether further measures/controls and/or strengthening existing mitigation measures/routines should be taken.

The risk assessment takes into account:

- the risk appetite of the entity,
- the risk tolerance of the entity,
- the costs and potential benefits to the entity of accepting or not accepting a risk.

This assessment allows the prioritisation of risks, as it will allow a better allocation of resources, financial and non-financial, to manage them. For the proposed scale (extreme, high, medium, low) see Annex 2 for risk criteria.

The above categorisation can be represented graphically, using the colour gradations in a risk hierarchy map (Figure 3). The purpose of the risk hierarchy map is to provide a visual representation of the risks, their impact (on the horizontal X-axis) and their probability of occurrence (on the vertical Y-axis) in order to facilitate decision-making on risk management. Risks with a higher probability and higher impact are placed at the top of the hierarchy, while risks of low importance are placed at the bottom.

It should be noted that the risk prioritisation map should be adapted according to risk appetite set by the organisation.

Risk Hierarchy Map

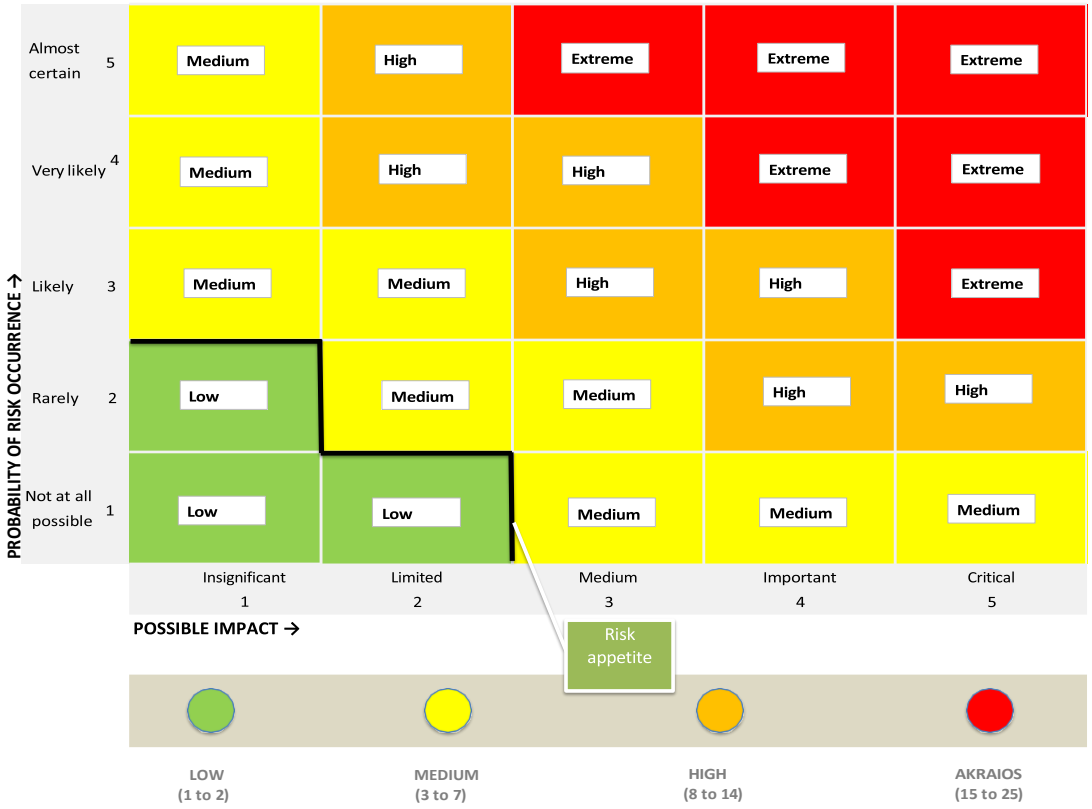


Figure 3. Risk hierarchy map

Risk management

Risk management involves identifying the range of options for dealing with the risk, evaluating those options and preparing and implementing response plans.

Depending on the type and nature of the risk, the objectives of the entity, the risk criteria, the available resources, the values, the entity chooses its risk attitude among the following:

- **Avoiding the risk, not starting or stopping the activity that creates the risk**. A public entity removes the use of a software as it creates cybersecurity risks that cannot be addressed by other means of improvement.
- **Elimination/removal of the source of danger**. A public body shall remove all asbestos from its buildings to protect the health of its staff.
- **Risk reduction through measures that decrease either the likelihood or the impact**

A public body installs advanced fire-fighting systems in public buildings to reduce the risk of fire damage.

- **Passing on all or part of the risk to third parties**. A public entity insures its building or movable property (vehicles, machinery).
- **Risk-sharing through which the risk is distributed among several entities who take on part of the activity associated with the risk.** A public entity collaborates with private companies (public - private partnership) to build large projects, sharing the risks involved.
- **Accepting/maintaining the risk with an informed decision, while monitoring and reviewing it**. A public body accepts the risk of using legacy software, with regular upgrades to avoid bugs, due to very high replacement costs and a history that does not demonstrate serious problems in its operation.

It should be noted that the risk appetite as well as the risk tolerance should be set low to ensure that measures are taken for those risks which, despite a low probability of occurrence, may have extremely adverse consequences (e.g. earthquake and other natural disasters). At the same time, where the risk has a high probability of occurrence or a significant impact, it is prudent for the entity to have made provision for the preparation of a contingency plan.

The selection of the most appropriate risk mitigation actions involves balancing the potential benefits of achieving the objectives against the costs, effort or disadvantages of implementation.

In order to implement the actions decided upon, the body should develop an appropriate action plan which will be monitored and reviewed on a regular basis. The information provided in the plan shall include, inter alia, the proposed actions, the resources required, performance measures, constraints, assumptions, timelines, etc. It is understood that the preparation of action plans requires prior approval by the competent body. (e.g. hiring of staff requires the approval of the head of the organisation, organisational measures concerning an organisational unit are normally approved by the head of the organisational unit).

It is noted that the entity can monitor the progress of the implementation of the action plan, using the Risk Register as a tool (see section *Record Keeping of Information Logs*).

Risk management: Examples

Risk Avoidance

Cancellation of a planned infrastructure project due to excessively high risks in terms of environmental impact or high financial risks.

Elimination/Removal of the Source of Risk

Withdrawing and replacing old and dangerous machinery with new and safer equipment can eliminate the risks associated with malfunctions or accidents.

Reduction of Risk

Reducing the possibility of risks associated with misapplication of legislation through appropriate training of staff.

Reducing the impact of the loss of the entity's files, due to natural disasters, through the creation of copies in the cloud.

Risk Transfer

Purchasing an insurance that covers damages to a public building caused by natural disasters."

Risk sharing

A public entity decides to build a new public project through a partnership with a private entity. In this way, the risk of budget overruns or delays can be shared between the two entities.

Acceptance of Risk

A municipality organises an event in a public place accepting risks of minor material damage.

Record Keeping Information Logs

Recording all stages of risk management allows the entity to document and accurately measure the results of the process. Appropriate documentation provides information on the effectiveness of the risk management process and how to improve it, ensures that the entity complies with legal, regulatory and contractual obligations, ensures consistency and traceability, facilitates communication about risks and their management, facilitates risk-related actions, etc.

Public sector bodies falling under the provisions of Law no. 4795/2021 record the information concerning the risk management of their entity in the Risk Register (art. 22ΣΤ, Low 4795/2021)

The Risk Register is a log, usually a spreadsheet in electronic format, through which all the risks of an entity are monitored. The spreadsheet includes information on the likelihood and impact of each risk (inherent and residual), the controls (existing and new/additional), who is responsible for monitoring them and the timetable for addressing them. The Register enable the entity to collect and analyze all the information on the potential risks to which it is exposed, analyse it and at the same time to draw conclusions on the level of overall risk it faces at any given time. The Register - particularly in entities with a large number of responsibilities and organisational units - may also be maintained via an electronic platform.

Updating the Register is an ongoing process, that should be explicitly defined by the entities and includes updating existing risks, adding new ones, as well as reviewing the entire Register. In order to assist the entities, a Risk Register Template and instructions on how to maintain and update it will be established by a joint decision of the Ministers of the Interior and Digital Governance and the Governor of the National Transparency Authority (Annex 3: indicative Risk Register template).

Submission of Reports and Documentation

Reports and Documentation are created with the main objective of capturing and communicating important information about the risks faced by the entity, the challenges arising from its environment, as well as assessing the adequacy and proper implementation of the entity's risk management policy and framework. Through Reporting, a permanent mechanism is established within the risk monitoring framework to ensure that the right information is communicated effectively and at the right time among those involved in the entity's risk management. In this way, risk reporting improves the quality of decision-making, influences the prioritisation of activities and enhances organisational oversight.

Particular reference is made to article 22D of Law No. 4795/2021, on the obligations of the risk management bodies to submit periodic and extraordinary reports to the head of the entity on the risks to which the entity is exposed, as well as

and annual report. The model of the Report, as well as the instructions for its preparation, are provided by a joint decision of the Minister of the Interior and the Governor of the National Transparency Authority.

The entity's risk management framework shall indicate, as a minimum:

- The time of submission of the Annual Risk Management Report, as defined by the relevant joint ministerial decision (par. 2 no. 22H of Law 4795/2021).
- The frequency and content of periodic reports.

Reports of the Risk Management Bodies:

Frequency and content of periodic reports:

- **Frequency of submission**: The frequency of submission of periodic reports should be regular and should be adjusted according to the number, the importance and the severity of the risks faced by the entity. For example, quarterly.
- **Content of the reports**: Periodic reports should include updates to the head on the risks'current status, the effectiveness of management measures, potential new risks, changes in the internal or external environment that may affect the risks faced by the entity.

Indicative cases in which risk management bodies shall submit exceptional reports:

- When a significant risk arises that had not been identified or had been assessed lower, which requires immediate attention.
- In case of serious incidents or accidents related to the entity's risks.
  When the risk mitigation actions taken are ineffective or when there is a significant deviation from the expected outcomes.
- When there are significant changes in the external environment (legislative, social, economic, etc.) that may affect the risks faced by the entity.

Monitoring and review

Continuous monitoring and periodic review of the risk management process and its results are essential, as ensure that risks are effectively identified and assessed and that the measures taken to address the risks are adequate and appropriate.

Entities operate in a changing environment and therefore risk management is a dynamic process. Therefore, they need to monitor and review their risks, their environment and the effectiveness of their risk controls/mitigation measures on a regular basis. The effectiveness and efficiency of the mitigation measures may be reviewed, through performance criteria and updated risk assessments, to determine whether the entity's resources are being used in the best possible way. Any delays or deviations in the implementation of measures shall also be monitored and reported to interested parties on a periodic basis to ensure timely implementation.

Communication and consultation

The purpose of communication and consultation is to help interested parties (inside and outside the organisation) understand the risks, the basis on which decisions are made and the reasons why specific actions are required. It is an ongoing and iterative process, with the aim of providing, sharing or obtaining information following dialogue with interested parties.

Communication and consultation should take place within the risk management process and throughout its stages. This will ensure that risks are adequately reported to the higher levels of the hierarchy and that decisions taken on which risks are tolerable or intolerable, as well as the priorities for action to address them, are communicated to the level of the business unit.

At the same time, effective communication and consultation ensures that:

- the risks are fully understood by the executives and management of the organisation.
- the specialised knowledge and experience of the participants is fully exploited in order toidentify the risks faced by the organisation.
- the different approaches of the participants contribute to improving the overall understanding of the risks.
- the risk management strategies adopted are widely supported.

Communication and consultation methods may include meetings, reports, electronic communication systems, training activities and newsletters.

A public body should ensure the involvement of appropriate executives, at all levels of management, at each stage of the risk management process, in accordance with the intended roles and responsibilities set out in the body's Risk Management Policy and Framework. At the same time, external interested parties (civil society organisations, professional associations, financial bodies, scientific community, etc.) may be involved in the consultation process.

Update of the Risk Management Policy and Framework

The entity's Risk Management Framework and Risk Management Policy should be reviewed and updated to ensure that they remain current and effective and that they are consistent with the current level of risk, the entity's strategic objectives and regulatory requirements. Regular review contributes to the proactive identification and mitigation of risks, protecting the entity from potential losses and ensuring its sustainability and growth.

The frequency of reviewing and updating the Risk Management Policy and Framework in a public entity depends on a number of factors and may vary depending on the specific needs and circumstances of each entity. However, some general cases are listed below:

- Changes in the legal and regulatory framework: in case of amendments to legislation or regulations affecting the operation of a public body, the Risk Management Policy and Framework must be adapted accordingly.
- After major events or crises: it is recommended that the Risk Management Policy and Framework be reviewed after major events or crises in order to incorporate past experiences and improve future risk management.
- Periodic review: in any case, regular review of the Risk Management Policy and Framework is recommended (e.g. every two years or at another frequency deemed appropriate for the organisation).

Definitions

Risk identification:
The process of finding, identifying and describing risks.

Risk analysis:
Process that takes place to clarify the nature and determine the level of risk.

Risk tolerance:
The readiness of an entity or interested part to assume the residual risk, subsequent to the implementation of measures to address it, in order to achieve its objectives.

Risk treatment:
Risk control - modification process.

Risk assessment :
Overall process of a) identification, b) analysis and c) risk assessment.

Risk evaluation:
The process of comparing the outcome of the risk analysis with the risk criteria is undertaken to clarify whether the risk is acceptable on the basis of its magnitude or significance.

Risk appetite:
The magnitude and type of risk an entity is willing to pursue or retain.

Risk management:
The process of identification, evaluation and audit of potential adverse or favourable events or situations, through which the entity takes a methodical approach to the risks associated with its activities and provides reasonable assurance for the achievement of its objectives (Article 3, Law 4795/2021).

Control:
Any action or procedure undertaken by the entity to manage risks and increase the likelihood of achieving its defined objectives and goals (Article 3, Law 4795/2021).

Measure that reduces or modifies the risk.

Inherent Risk:

The risk that exists before any measure is taken to mitigate it, such as when any risk control is missing.

Interested party/stakeholder:

A natural or legal person who may influence and/or be influenced or consider himself/herself to be influenced by the decisions and/or activities of the entity.

Risk:

The possibility or threat of damage, loss or, in general, a negative consequence for the objectives of the entity, which may be caused by both endogenous and exogenous factors and which can be mitigated by preventive actions and risk controls (Article 3, Law 4795/2021).

Risk criteria:

The benchmarks against which the significance of a risk is assessed.

Risk management framework :

The set of guidelines and organisational arrangements relating to the design, implementation, evaluation and continuous improvement of the entity's risk management, as well as the methodology for conducting the risk management process.

Risk management policy:

It includes how risks are managed by purpose and objective, the risk appetite and level of risk tolerance, and the roles and responsibilities of the appropriate levels of management with regard to the design, monitoring and implementation of the risk management framework.

Level of risk:

The magnitude or significance of a risk, as a result of the combination of impact and probability.

Residual Risk:

The risk that remains after management has taken measures to reduce the probability and impact of an adverse event.

ANNEX 1: Risk Management Policy

A. The preamble to the policy expresses the purpose and commitment of the organisation. Indicatively,

As the head of [Name of Body] I would like to express our commitment to the systematic identification, assessment and management of risks, with the aim of providing high quality public services to citizens.

This document aims to:

- Ensuring public confidence: We wish to maintain and strengthen public confidence in our entity.
- Optimising the use of available resources: We aim to handle our resources effectively and efficiently to provide quality services and to ensure that our customers are provided with the best public service.
- Evidence-based decision-making: we rely on evidence and data to make sound and informed decisions.
- Ensuring regulatory compliance: we ensure compliance with laws and regulations.
- Supporting the implementation of public policies and programmes: We support the successful implementation of our public policies and programmes.
- Informing employees on issues relating to: their role, responsibilities and accountability for risk management as it relates to their work.

B. In this section, the entity, outlines roles and responsibilities related to risk management, based on its organizational structure.

Indicatively, the role of each position of responsibility in relation to risk is outlined.

Position of responsibility	**Role**
Head (*Minister, Governor, Secretary of the Decentralised Administration)*	α) determine the risk appetite and risk tolerance of the entity. b) Approve the Risk Management Policy and Risk Management Framework and ensure that the entity complies with them. c) Ensure that the risk management process is integrated into the operations of the entity and the provision of services.

	d) Decide on the implementation of risk management strategies to address the identified risks of the entity. e) Decides on the priority management of very high (extreme) risks affecting the entity's objectives and operations. f) They are responsible for any other action resulting from the existing institutional framework regarding risk management and the operation of the Risk Register (such as approval of measures, measures to manage risks, introduction of new risks in the Register, etc.).
General Secretary - Permanent Secretary of Ministries	α) They shall be responsible for all risks in their area of responsibility. b) Foster and promote a culture of integrating risk management within all activities of the organisational units under its supervision and control. c) Ensure the implementation of risk mitigation measures. d) Ensuring that adequate resources are allocated to risk management and the implementation of risk mitigation measures within the organisational units under its supervision and control.
Internal Audit Unit	α) provides reasonable assurance on the adequacy and effectiveness of the risk management system as a core component of the entity's Internal Audit System. b) Evaluates the efficiency of existing risk control networks within the organisation in the context of its projects.

	c) Assess the effectiveness of risk management processes throughout the entity and in particular whether: • the Risk Management Policy and Framework is applied, • significant risks are identified and assessed, • appropriate measures are selected to address the identified risks, depending on the acceptable risk tolerances of the entity.
Risk management body	α) Recommends the Risk Management Policy to the head of the entity. b) Develop, monitor and update the Risk Management Framework of the entity, in accordance with its strategic and operational objectives. c) Inform and instruct the staff of the entity on how to identify and manage risks in the exercise of their responsibilities and the monitoring of audt mechanisms. d) Supervise the risk management process carried out by all the organisational units of the entity. e) They are responsible for maintaining, monitoring and updating the Risk Register of the entity and provides guidance to the other organisational units. f) submit periodic and ad hoc reports to the entity's Head on the risks to which the entity is exposed. g) Submit the Annual Report to the head of the body, which shall be communicated to to the National Transparency Authority.

General Managers	They are responsible for monitoring the implementation of the Risk Management Policy and Framework within their Directorate General, as well as the implementation of risk management measures within their organisational units. This includes: (a) the proper integration of the risk management process into the business processes under their responsibility, (b) identifying the risks that threaten the achievement of the objectives of the organisational unit they head, their causes and their effects, (c) the evaluation of existing audit mechanisms, (d) monitoring the risks (existing and emerging) that fall within their area of responsibility, (e) the ongoing support, training and awareness-raising of staff so that they understand their role and responsibilities, as well as the risks related to their area of responsibility, (f) ensuring the cooperation of the Directorate General with the Risk Management Body and the actions required in this context, (g) any other action resulting from the existing institutional framework regarding risk management and the operation of the Risk Register (such as the adoption of measures to manage risks, introduction new risks in the Register, etc.).

Directors/ Heads Department	Managers and heads of departments are responsible for: (a) the implementation of the Risk Management Policy and Framework within the organisational unit to which they belong and the risk management measures within their organisational units, (b) the proper integration of the risk management process into the business processes under their responsibility, (c) identifying the risks that threaten the achievement of the objectives of the organisational unit they head, their causes and their consequences, (d) evaluating existing audit mechanisms and proposing additional audit mechanisms/risk mitigation measures within their area of responsibility, (e) monitoring the risks (existing and emerging) that fall within their area of responsibility, (f) the ongoing support, training and awareness-raising of staff so that they understand their role and responsibilities, as well as the risks associated with their area of responsibility.
Executives of the organic units	All staff are responsible for complying with the entity's policies, procedures and guidelines for risk management, including: a) monitoring the implementation of the audit mechanisms in their area of responsibility and reporting incidents of non-implementation or incorrect implementation to their immediate superiors, (b) the identification of potential risks during the the exercise of their day-to-day responsibilities; and

	reporting them to their immediate superiors.

Γ. In this section, the entity shall reflect the categories of risk, in accordance with the guidance set out in this Standard, and subcategories, taking into account the scope of its responsibilities and its organisational structure.

Natural or non-natural disaster risks: Risks refer to major external contingencies that threaten life, health, people, property or the environment. These risks may directly or indirectly affect the operation of the entity.

Strategic risks: Risks that relate either to internal and external events that may prevent or impede an entity from achieving its goals and strategic objectives, or to risks arising from the entity's strategic choices.

Operational risks: Risks that affect the entity's operational functions through which it performs its responsibilities and over which it has direct management responsibility and control. These risks may arise from the entity's internal processes, human resources, governance and management oversight, lack of effective and efficient decision-making and leadership structures leading to the loss of critical milestones for the entity, etc.

Information technology risks: Risks that may arise from ineffective approaches to managing and implementing technology, and from weaknesses in policy or procedures in information technology systems.

Financial risks: Risks related to events/threats that may jeopardize an entity's financial objectives.

Legal/regulatory/compliance risks: Risks related to the non-implementation of the public entity's institutional framework, regulations, contractual terms, standards or internal policies that could lead to direct or indirect administrative liability, civil or criminal penalties, regulatory sanctions or other negative impacts on the reputation, operation and exercise of the entity's responsibilities.

Health and safety risks: Hazards that may affect the health and safety of workers.

Risks of corruption and fraud: Risks associated with the abuse of public or private office for personal gain or with cases of fraud.

D. In this section the institution shall determine the risk appetite and risk tolerance.

Example 1º

Risk category	Risk appetite scale	Declaration of willingness to assume and tolerate risk
	Low High	
Strategic risks		Our entity has a low risk appetite, committed to achieving its goals and strategic objectives. However, our entity, recognising that there is an inherent risk in the nature of some of the work involved in the implementation of a major project it has undertaken, can tolerate the possibility of delay in the completion of the project by up to 3 months from the date initially set for delivery.
Legal/regulatory risks/ compliance		Our entity has a low risk appetite, committed to faithfully applying its institutional framework, regulations, standards and internal policies. Our entity will not tolerate any risks associated with fraudulent activity.

Alternatively, the institution may define the risk appetite and risk tolerance in certain categories with clear quantitative limits.

Example 2º

Risk category	Declaration of willingness to take risks (qualitatively defined)	Risk appetite (quantitative) specified)	Risk tolerance	Unacceptable risk
Information technology risks	Our entity has a low risk-taking attitude towards technology Information	up to 1 ½ hours the period of time during which the information system is not functioning	up to 2 hours the period of time during which the information system is not functioning	more than 2 hours the period of time during which the information system is not functioning

RISK APPETITE RATING

RISK APPETITE	DESCRIPTION
VERY HIGH (EXTREME) RISK APPETITE	The entity considers that the potential benefits of this 'aggressive' risk-taking outweigh the potential negative consequences, and is therefore willing to take the associated risk to achieve its objectives.
HIGH RISK APPETITE	The entity is prepared to take risks that are greater than normal and accept some negative consequences in order to achieve its goals.
MEDIUM RISK APPETETE	The entity shall adopt a balanced approach to risk-taking. Potential negative impacts and the achievement of its objectives shall be taken into account in equal measure.
LOW RISK APPETETE	The entity takes a cautious approach to risk-taking and is prepared to accept only minor negative impacts in pursuit of its objectives.

ANNEX 2: Risk criteria

Table 1: Indicative Probability Scale of Risk Event

Rating		Description	Indicative frequency
5	**Almost certainly**	The risk is expected to occur in the majority of cases. Many known cases (records/experience).	The risk can occur more than once a year.
4	**Very likely**	The risk is likely to occur in most circumstances. Known incidents (records/experience).	The risk may occur once a year.
3	**Possible**	The risk could happen in certain circumstances.	The risk may occur once every two years.
2	**Rare**	The risk could happen at some point but it is not expected. No known incident has been recorded or experienced in the recent years.	The risk may occur once every five years.
1	**Not at all likely**	The risk can only happen in exceptional circumstances.	The risk may occur after five years.

Table 2: Indicative Impact Scale of Risk Event

(based on Information and public services for the Island of Jersey - Risk management guidance)

IMPACT	*Not important (1)*	*Limited (2)*	*Middle (3)*	*Important (4)*	*Critical (5)*
At the level of operations /service provision	Individual partial interruption of public service(s) of a few hours' duration. (periodic/intermittent interruption or a problem in a section of public service(s). Negligible impact on citizens. Minimal delays in the implementation of entity's objectives /entity's operational plan, or entity's programmes.	Limited partial interruption of public service(s) of one day's duration. Little impact on citizens. Small delays in the implementation of entity's objectives /entity's operational plan, or entity's programmes.	Regular partial interruption of public service(s). Medium impact on citizens. Regular delays in the implementation of entity's objectives /entity's operational plan, or entity's programmes.	Complete cessation of public service(s). Significant impact on citizens for a short period of time (<7 days). Important delays in the implementation of entity's objectives /entity's operational plan, or entity's programmes that may lead to significant changes to entity's strategic and operational plan	Complete cessation of public service(s). Significant impact on citizens for a long period of time (>7 days). Important delays in the implementation of entity's objectives /entity's operational plan, or entity's programmes that threaten the the achievement of the strategic and operational objectives of the body; and may

					lead to no reversible situations.
In reputation	Individual complaints of minor importance which the entity considers that they do not require examination or evaluation. Minimal and transient loss of trust of citizens/private sector/suppliers/international organization .	Internal investigation (e.g. conducting a sworn administrative inquiry) to prevent further escalation Replacement/movement of agency staff Complaints against employees. Small loss of trust of citizens/private sector/suppliers/international organization that can be recovered quickly.	Coverage by local media resulting in external audit of the entity. Replacement/movement of middle and lower management of the organisation. Reduced trust of citizens/private sector/suppliers/international organisations that can be recovered over time.	National media coverage resulting in extensive public scrutiny. Replacement/movement of senior and top management of the organisation. Complaints against the The entity's management. Serious loss of trust of citizens/private sector/suppliers/international organisations.	National media coverage that is causing a public inquiry and outcry. Replacement of the entity's Head. Significant reduction in state funding of the entity. Irreversible loss of trust of citizens/private sector/suppliers/international organisations.

Compliance laws and regulations	Violation of standards/guide lines. No legal action is expected. Negligible financial impact.	Infringement policy/regulations. One-off claims or legal issues. Minor financial impact.	Serious infringement leading to an investigation. Ongoing legal/judicial issues. Significant financial impact	Significant violation leading to fines Significant legal actions/prosecutions. Research by a supervisory body. Significant fines with imprisonment.	Repeated significant violations. Imposed penalties/sanctions Repeatedly large fines.
Financial Management	Negligible impact on the execution of the entity's budget.	Limited impact on the execution of the entity's budget (transfer of appropriations between itemized bills).	Moderate impact on the execution of the entity's budget (negative deviation of less 10% from their quarterly financial targets).	Significant impact on the execution of the entity's budget (negative deviation of more than 10% from the quarterly financial targets).	Serious, impact on the execution of the entity's budget (cases of deviations exempted from the application of the provisions of the article 172 of Law No. 4270/2014).

Environment/ Society	Minimal damages to individual infrastructures/properties. No permanent harmful impact on the environment. Minimal impact on the local community.	Minor and local damage to infrastructures/properties. Short-term and limited adverse environmental impacts. Noticeable but manageable impacts on the local community.	Significant, short-term losses in infrastructures /properties. Long-term adverse environmental impacts. Serious but manageable impacts on the local community.	Severe, long-term damage to infrastructures/ properties. Extensive damage to the environment. Serious damage to the entire community.	Complete destruction of basic infrastructures. Widespread and irreparable damage to the environment. Significant, permanent damage to the entire community.

Where possible, impact is captured in a clear and measurable way.

Table 3: Indicative scale for assessing the adequacy of controls

(based on a publication of the Victorian Managed Insurance Authority "Risk criteria examples")

Rating the effectiveness of controls	Description
Fully effective	No action is required other than to review and monitor existing controls. Controls are well designed and address the root causes of the risks. Management believes they are effective and reliable.
Quite effective	Most controls are well designed, implemented and effective. Some work is still needed to improve their effective operation. Management has some doubts about their effective operation and reliability.
Partially effective	Although the design of the controls may largely be correct, as they address most of the root causes of the risk, controls are currently not very effective. or Some of controls do not appear to be well designed, as they do not address the root causes of the risks. Those that are properly designed are working effectively.
Largely ineffective	Significant gaps in the controls. Either the controls do not address the root causes of the risks, or they are not working effectively at all.
Absence of controls or completely ineffective	Almost no reliable control. Management has no confidence that any degree of control is being achieved, due to poor design of the controls or very limited operational effectiveness.

Table 4. Indicative risk rating

(based on the Corruption and Fraud Risk Management Guide, N.T.A., 2021)

ADVERTISEMENT	RESPONSE
EXTREME RISK (VERY HIGH)	• **Response:** immediate measures must be implemented. The entity's senior management must be kept informed so that the risk and the control measures put in place are monitored on a regular basis.
HIGH RISK	• **Response:** Measures must be taken to shift the risk to the Moderate or Low Risk area. The risk must be regularly monitored by the supervisor and senior management.
MODERATE RISK	• **Response**: the risk may be acceptable, but mitigation is sought whenever feasible to shift it to the Low Risk area. Monitoring of the risk can be carried out by the responsible supervisor.
LOW RISK	• **Response:** can be eliminated or reduced with existing controls

ANNEX 3: Indicative Risk Register Template

1	2	3	4	5	6	7	8	9	10	11
Risk identification	**Risk Categories**	**Risk Description**	**Potential Risk Sources**	**Involved Parties**	**Inherent Risk Likelihood**	**Inherent Risk Impact**	**Inherent risk Significance**	**Existing Control Measures**	**Residual risk likelihood**	**Residual Risk Impact**

12	13	14	15	16	17	18	19	20	21
Residual Risk Significance	**Acceptable or not acceptable Residual risk**	**Short-term Risk Mitigation Measures (additional controls)**	**Long term Risk Mitigation Measures (additional controls)**	**Responsible Person for approving Risk Mitigation Measures**	**Justification for amendment**	**Responsible for the implementation of measures**	**Deadline for implementation of measures**	**Responsible for Risk Monitoring**	**Status Risk**

Description of fields of the indicative Risk Register template

1. **Risk identification :** a unique identifier for each risk given by the electronic Risk Register system.
2. **Risk category:** the category to which the risk belongs (e.g. corruption risk).
3. **Risk Description:** a brief description of the potential risk.
4. **Potential Risk Sources:** conditions or actions likely to trigger the occurrence of the risk.
5. **Involved parties:** organizational units and/or individuals within the entity involved in any way with the potential risk.
6. **Inherent risk likelihood:** an indication of how frequently the inherent risk may occur before any mitigation measures are taken, such as in the absence of controls.
7. **Inherent risk impact':** an indication of how severe the consequences would be before any mitigation measures are taken, such as in the absence of controls.
8. **Inherent risk significance:** classification of risk after considering its likelihood and impact, assuming no measures have been taken to mitigate it, such as in the absence of any controls.
9. **Existing Controls:** existing actions or procedures of the organisation to manage risks and increase the likelihood of achieving defined objectives and goals.
10. **Residual risk Likelihood:** an indication of how often the residual risk may arise after management action (existing controls).
11. **Residual risk impact:** an indication of how severe the consequences would be if the risk were to occur, taking into account the measures implemented by management (existing controls).
12. **Residual risk Significance:** classification of the risk after evaluating its likelihood and impact, considering the measures taken by management (existing controls).
13. **Acceptable or unacceptable residual risk**: determines whether the level of risk is acceptable or not, taking into account the effectiveness of the existing controls, in accordance with the defined risk tolerance level.
14. **Short-term Risk Mitigation Measures (additional controls)":** Short-term measures that the entity must take to address the risk and ensure it remains within the defined risk tolerance level.

15. **Long-term Risk Mitigation Measures (additional controls):** Long-term measures that the entity must take to address the risk and ensure it remains within the defined risk tolerance level.
16. **Responsible person for approving risk mitigation measures:** the Head of the General Directorate or the Directorate, in case there is no General Directorate, or of the independent organisational unit that is not part of a General Directorate, as well as any senior management body of the organisation with decision-making authority for implementing risk mitigation measures (additional controls).
17. **Justification for amendment:** justification for the amendment of the measures recorded in the Risk Register.
18. **Responsible for the implementation of measures:** The Head of any organizational unit responsible for implementing risk mitigation measures (additional controls).
19. **Deadline for implementation of measures:** the deadline for implementing the risk mitigation measures (additional controls).
20. **Risk for Risk Monitoring**: the Head of any organizational unit concerned with the specific risk.
21. **Risk status:** indication of whether the risk has been addressed (e.g. "open", "in progress", "closed").

Bibliography

1. Law 4795/2021 (A' 62), *Public Sector Internal Audit System, Integrity Advisor in the public administration and other provisions for the public administration and local government.*
2. Law 5013/2023 (A' 12), *Multi-level governance, risk management in the public sector and other provisions*.
3. Decision FG8/55081/2020 (B' 4938), *Procedure for the Audit by the Court Audit of the existence, operation and effectiveness of the Internal Audit System in the entities under its audit jurisdiction*.
4. Law 3560/2007 (A' 103), *Ratification and implementation of the Criminal Law Convention Corruption and its Additional Protocol*.
5. Law 3666/2008 (A' 105), *Ratification and implementation of the United Nations Convention against Corruption and replacement of relevant provisions of the Criminal Code*.
6. International Organization for Standardization (2018), *ISO 31000: Risk Management - Guidelines.*
7. International Electrotechnical Commission, International Organization for Standardization (2019), *Risk Management - Risk Assessment Techniques*.
8. United Nations Industrial Development Organization (2021), *ISO 31000:2018.*
9. International Organization for Standardization (2022), *ISO 31073: Risk Management - Vocabulary*.
10. International Organization for Standardization (2009), *ISO Guide 73: Risk Management - Vocabulary*.
11. Information and public services for the Island of Jersey (2023), *Risk management guidance*.
12. British Columbia Risk Management Branch & Government Security Office (2022), *Risk Management Guideline for the B.C. Public Sector*.
13. NSW Government (2022), *Enterprise-wide Risk Management*.

14. UK Government Finance Function (2021), *Risk Appetite Guidance Note*.
15. UNDP Risk Appetite Statement Guidance (2021), *Detailed risk appetite statement guidance*.
16. National Transparency Authority (2021), *Guide to Corruption Risk Management & Fraud*.
17. State of Victoria (2020), *Victorian Government Risk Management Framework*.
18. New Zealand Government (2020), *ICT Risk Management Guidance*.
19. Global Partnership for Education (2019), *Risk Management Framework and Policy*.
20. UK Cabinet Office and Civil Service (2017), *Managing risk in government: framework*.
21. NSW Government (2015), *Enterprise-Wide Risk Management Policy and Framework -. NSW Health*.

NATIONAL TRANSPARENCY AUTHORITY

195 Lenorman & Amfiaraou
104 42, Athens
+30 2132129700
info@aead.gr
www.aead.gr