HELLENIC REPUBLIC

Corruption Risk Management Guide & Fraud

An effective framework to prevent corruption and fraud in public bodies

Version 1.0
February 2021

NATIONAL TRANSPARENCY AUTHORITY

CORRUPTION RISK MANAGEMENT GUIDE & FRAUD

GENERAL DIRECTORATE FOR INTEGRITY & ACCOUNTABILITY

February 2021

ISBN 978-618-84622-3-6

EDITORIAL

This Guide has been prepared in accordance with the instructions of the NTA Governor (hereinafter referred to as "NTA" or "Authority"), Angelos Binis, and with the supervision and coordination of the Head of the Directorate General for Integrity and Accountability, Maria Konstantinidou. The project team consisted of: Christos Kourtis and Prodromos Chatziioannidis, members of the Integrity Policies and Standards Development Department of the Integrity Policies and Standards Division of the Directorate General for Integrity and Accountability.

Foreword by the Director of the National Transparency Authority

It is with great pleasure that I present to you the Corruption Risk Management Guide & Fraud Risk Management prepared by the staff of the Integrity and Accountability Directorate of the National Transparency Authority (NTA). The Guide includes a coherent framework of practical steps and methodologies for identifying, assessing and addressingthe risks of fraud and corruption in the policies, programmes and projects undertaken bythe Greek public administration.

Its objective is to support the efforts of public administration officials to develop and strengthen mechanisms to prevent, deter and detect fraud and corruption based on a risk assessment methodology. Officials and managers responsible for managing the resources of an entity must assess the risks of fraud and corruption in the performance of their duties and take all necessary measures to address them, within the framework of an integrated and effective Internal Audit System. The Guide in your hands provides all the necessary information and tools to assess these risks and use the results to develop a strong anti-corruption strategy at the level of each public organisation.

It also includes good practices for creating the right organisational structures and fostering a culture that is not conducive to corruption. Public sector professionals will also find a range of tools for effectively managing corruption risks, designing and implementing safeguards, monitoring and evaluating anti-corruption mechanisms and taking corrective action where necessary.

This Guide is based on the experience gained by the staff of the H.A.D. during the preparation of the Corruption and Fraud Risk Assessment Report in the Functions of the General Secretariat of Citizenship of the Ministry of Nationality. and in the thorough review of the ISO 31000:2018 standard, as well as corresponding guidelines developed by international organizations such as the UNOOSA and the United Nations Development Programme, and national anti-corruption Audit and anti-corruption agencies such as the Government Accountability Office of the United States of America, the Independent Commission against Corruption of Hong Kong and the Serious Fraud Office of the United Kingdom.

The NTA Governor

Angelos Binis

Introduction

General

The vast majority of civil servants, no doubt, perform their duties with honesty and dedication. However, most public bodies have been confronted with incidents of corruption, which may involve a public contract, the granting of a certificate or any other transaction between a citizen and the body. On the other hand, it is also very likely that persons dealing with public bodies may also seek by fraudulent means to influence or circumvent rules, procedures and decisions. Identifying the areas that are most vulnerability to an incident of corruption is both a challenge and an opportunity for public bodies to implement strategies to prevent incidents of corruption, ensuring that all staff of the body work with integrity to achieve its mission.

> "Theory is not enough, needs application. Good will is not enough, actions are required."
>
> Leonardo Da Vinci

Purpose of the Guide

The development of an integrated risk management function in the Greek public administration can contribute to addressing the pathologies and threats that hinder the improvement of governance systems and the functioningof public organisations.

The National Transparency Authority has drawn up this Guide in order to encourage and facilitates public bodies to adopt a systematic approach to identifying, analysing, assessing and addressing potential risks of corruption and fraud.

Corruption Risk Management and Fraud is a tool that focuses on proactively identifying and subsequently addressing the vulnerabilities of an operator, taking into account both the internal and external environment.

In order to achieve this, the Guide provides all the necessary tools for the institution to identify potential corruption risks and fraud, then evaluate them and finally identify the most efficient and effective ways ofdealing with them.

It is recognised that many organisations do not have the necessary human or financial resources or even the knowledge to implement these tools. However, this Guide provides the methodology for the process of managing potential risks of corruption and fraud, taking into account these limitations.

Therefore, the operator will be able to:

- identify **what** makes them more vulnerable to corruption and fraud,
- identify **where** corruption and fraud are most likely to occur,
- **determine how to** address the risks it has identified by implementing appropriate measures.

> "If you can't explain it simply, you don't understand it well enough."
>
> Albert Einstein

<u>Leadership commitment (Tone at the top)</u>

In order to address the phenomena of corruption and fraud in an organisation, it is essential that its leadership is committed to fostering a climate of integrity and to adopting and implementing policies to effectively address these phenomena. The adoption of this Guide is the first step practical evidence of that commitment.

Structure and content of the Guide

The Guide proposes a structured corruption and fraud risk assessment that could be applied by all public sector bodies.

In the first chapter, the characteristics of an effective framework for preventing corruption and fraud and the types of actions that an institution could take to prevent it are discussed.

In the second chapter, the actions that need to take place in preparation for the risk management process are presented in detail.

Finally, in the third chapter, the risk management process according to ISO 31000: 2018, "Risk management - Guidelines for the conduct of risk management in any type of organization" is detailed, which includes the following stages:

(a) the **identification of the environment** in which the operator operates and is exposed,

(b) the **identification of the risks of corruption and fraud to which** the entity is exposed,

(c) the **analysis of risks** to determine their nature and causes,

(d) the **assessment of risks based on the** magnitude of the likelihood of their occurrence and the impact that their occurrence may have on the achievement of the objectives of the entity,

(e) to **address the risk** through the development of actions, taking into account the limited resources (material and human) available to the organisation.

Approach to corruption and the risk of corruption and fraud

The United Nations Convention against Corruption (UNCAC)[1] recognises that there is no single agreed definition of corruption. However, listed below are all the globally agreed forms of manifestations of corruption, including:

- ➔ Active bribery. Promising, offering or giving an employee an undue advantage in order to act or avoid action on matters related to his/her duties.
- ➔ Passive bribery. Demanding or accepting from an employee, an undue advantage in order to act or avoid action on matters that related to his duties.
- ➔ Misuse / Theft / Misappropriation of assets, funds, securities or any other item of the entity, where the employee, by virtue of his/her capacity, has access.
- ➔ Abuse of power. Execution or failure to execute an act by an official, in violation of the legal framework, in order to gain an undue advantage.
- ➔ Trade of influence. Unfair use of influence exercised by an employee in accordance with the authority given to him/her, with the purpose of gaining an advantage.
- ➔ Illegal enrichment. A significant increase in an employee's assets that is not justified by his or her legal income.
- ➔ Money laundering from illegal activities. Concealing the origin of money from illegal activities, in particular by transferring it to banks or legitimate businesses.
- ➔ Concealment or withholding of property resulting from corruption.

According to the Association of Certified Fraud Examiners (ACFE)[2] , all of the above categories of corruption (internal fraud) can be summarized as follows:

- ➢ Embezzlement/theft/misappropriation, which includes the unlawful withholding or removal or use of an entity's assets. Relevant examples include: theft of the operator's premises, stock or cash, overcharging, fraud in accounts, etc.
- ➢ False reporting, usually in the form of falsification of financial statements for personal gain. It also includes falsified or false documents, such as certificates, attestations, etc.
- ➢ Bribery or acceptance of other forms of facilitation in exchange for unlawful use of confidential information, photo contests and conflict interests.

[1] https://www.unodc.org/e4j/en/anti-corruption/module-1/key-issues/corruption---baseline-definition.html

[2] https://www.acfe.com/fraud-tree.aspx

These types of corruption are summarised in the figure below:

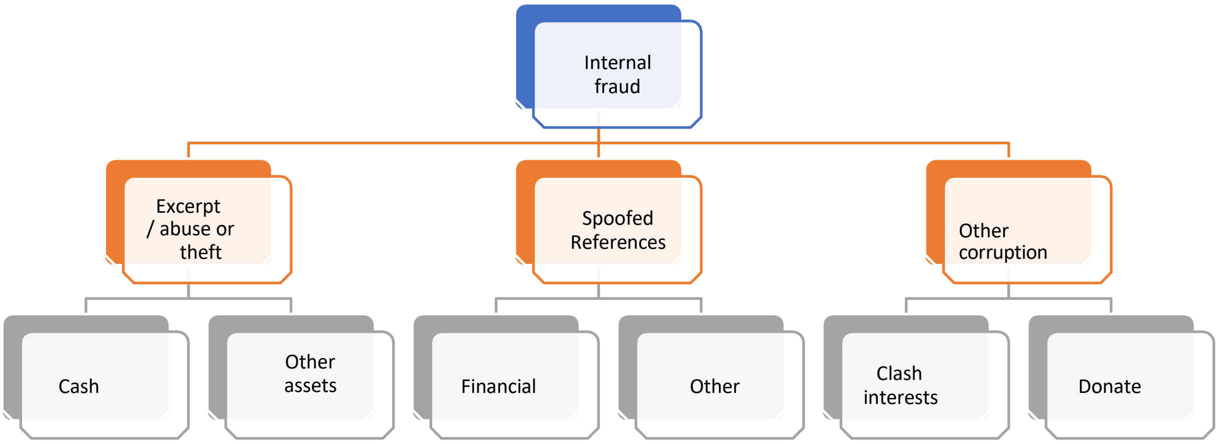
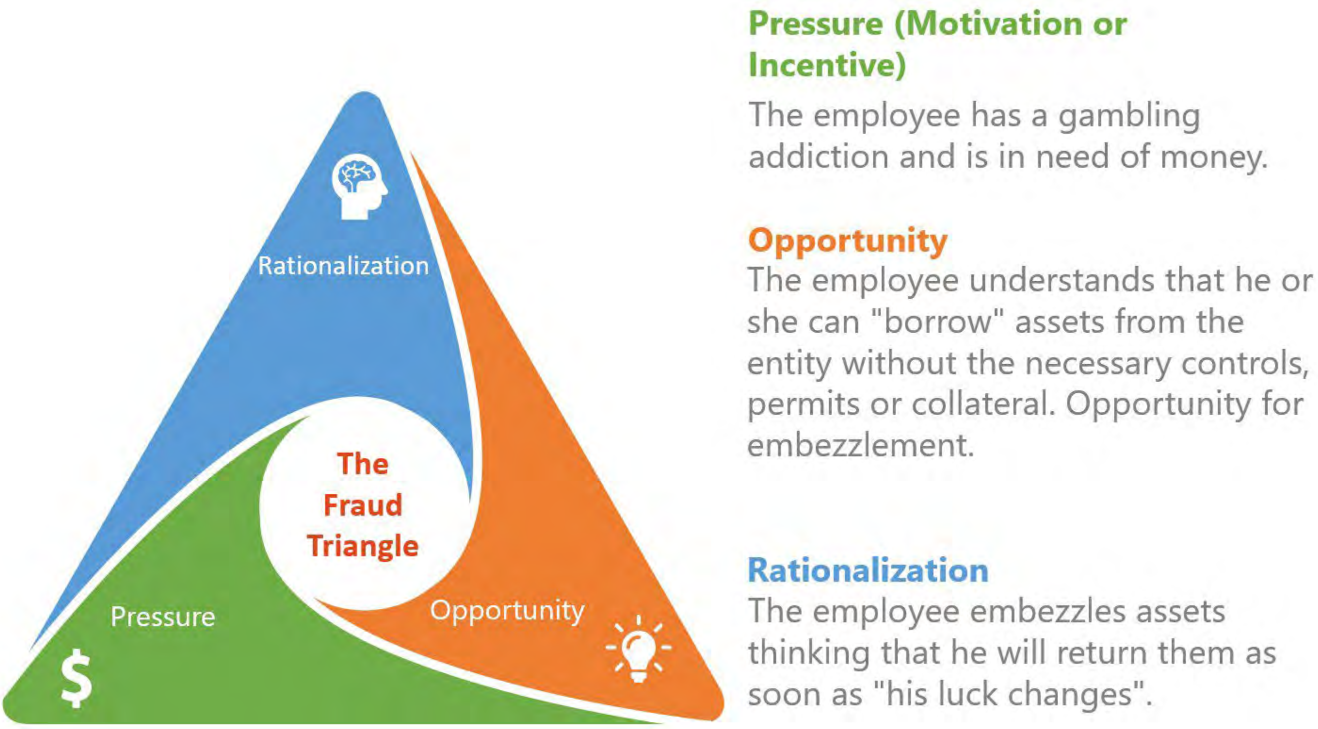


***Figure 1**: Types of internal fraud/corruption*

The reasons why people commit crimes of corruption or fraud vary. The fraud triangle illustrates the factors that contribute to the commission of fraud: motive, opportunity and rationalisation.



Pressure (Motivation or Incentive)

The employee has a gambling addiction and is in need of money.

Opportunity

The employee understands that he or she can "borrow" assets from the entity without the necessary controls, permits or collateral. Opportunity for embezzlement.

Rationalization

The employee embezzles assets thinking that he will return them as soon as "his luck changes".

***Figure 2**: The fraud triangle*

One of the most effective ways to prevent fraud is to adopt methods to reduce incentives and limit opportunities. Although rationalization is largely up to the individual's personality,a strong organizational culture of integrity and adherence to ethical values have proven tobe quite effective.

Framework of actions to prevent corruption and fraud

The purpose of an effective corruption and fraud risk management system is the continuous and systematic effort to reduce the likelihood of undesirable incidents occurring and to mitigate the consequences that they could have. In this way, it ensures that taxpayers' money is spent efficiently, services fulfil their intended purpose and public assets are properly protected. The main actions to prevent incidents of corruption and fraud fall into three general categories: prevention, **detection** and response. These categories of actions are independent, while reinforcing each other. For example, an action to detect corruption, such as an extraordinary audit, also contributes to the prevention of such incidents by creating a climate of discouragement within the organisation. Moreover, after the audit, a decisive reaction to an incident of corruption through the imposition of severe sanctionsacts as a measure of exemplary and deterrent effect.

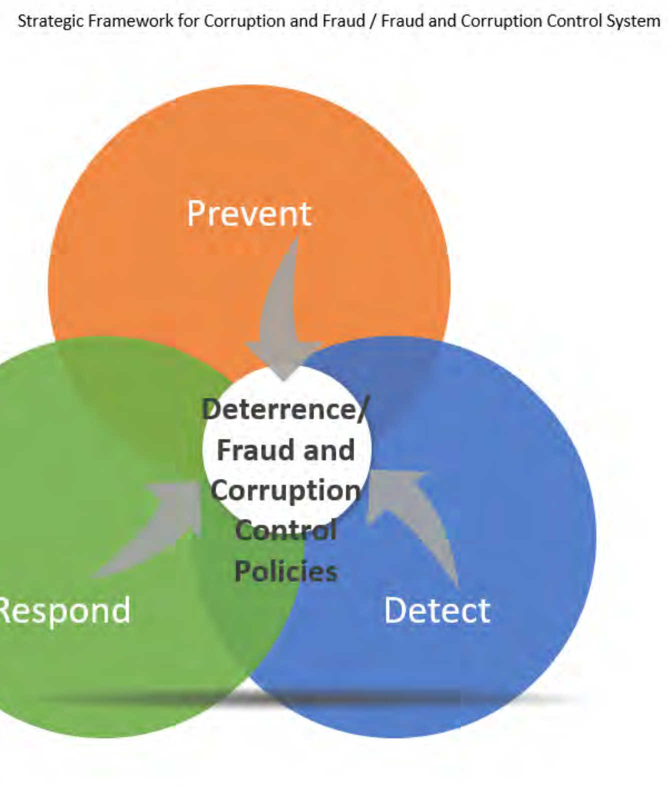

Strategic Framework for Corruption and Fraud / Fraud and Corruption Control System
Prevent
Deterrence/ Fraud and Corruption Control Policies
Respond
Detect

Figure 3: *Framework of actions to prevent corruption and fraud*

Prevention

Prevention techniques include the introduction of policies, procedures and access to data or records, as well as activities such as training and awareness-raising of the organisation's employees against corruption and fraud. However, it should be noted that fraud prevention techniques do not provide complete protection. It is considered difficult, if not unlikely, to eliminate all such incidents.

Localization

An effective strategy to detect corruption and fraud should include the use of analytical procedures to identify weaknesses in the operations of the organisation and theintroduction of reporting mechanisms to provide information on possible illegal acts. The components of an integrated fraud detection system include reporting of unusual procedures, electronic data mining, behavioural analysis and continuous risk assessment. The fraud detection process should identify those functional systems of the organisationthat are most susceptible to fraud or incidents that have already occurred. In this way, it canmake a significant contribution to improving the organisation's internal Audit system.

Reaction

The operator's reaction to incidents of corruption or fraud should be immediate. The existence of a protocol for dealing with incidentsof corruption and fraud underlines the organisation's determination to combat unwanted incidents as soon as they come to its attention. The protocol shall define in detail the persons responsible for conducting the investigation and the procedures for gathering information, it being understood that the investigation will be carried out in a timely and objective manner. In addition, the Protocol ensures that those responsible are promptly sanctioned by the disciplinary bodies and/or referred to the competent prosecuting and judicial authorities.

> "The world will not be destroyed by those who do evil, but by those who see them and do nothing."
>
> Albert Einstein

Preparation of the institution for the conduct of the corruption and fraud risk management process

Launch of the corruption and fraud risk management process

The corruption and fraud risk management function, in order to be effective, requires the recognition by the head of the organisation of the need to identify and address any weaknesses in the organisation and then the commitment of both the organisation's management hierarchy and its staff to this end.

The trigger for initiating the corruption and fraud risk management process may be a corruption scandal, an audit finding, a media report or even the adoption of a national or sectoral anti-corruption strategy that obliges the organisation to undertake this process. There may, of course, be a willingness on the part of the body to act proactively on its own initiative in order to identify areas that make it vulnerable to future risks.

In addition, the trigger for this procedure can be the immediate problems faced by an institution, such as a decrease in its revenues, an increase in complaints from citizens, an obvious change in the living standard of an employee and, of course, a scandal. Focusing therefore on existing, visible problems that this body needs to address in order to improve its performance protects it from a perpetual 'witch hunt' that can cause both resentment and fear among its employees. Nevertheless, whatever the trigger for implementing such a process, there is likely to be caution and perhaps even resistance from the organisation's staff, particularly in the early stages.

Box 1*: Possible reasons for caution in implementing corruption and fraud risk management*

- ➜ Staff are concerned that the obsession with "hunting" corruption ultimately leads to the emergence of "scapegoats " and ultimately to the targeting of specific officials or even entire organisational units.
- ➜ Operators are concerned that the "hunt" for corruption will disrupt the operation of the operator and for a long time.
- ➜ Supervisors fear that concern about corruption is a pretext for their disparagement or even replacement.
- ➜ Operators' management feel that their reputation will be damaged as many perceive the risk management process as an assumption that the their institution is corrupt.

Commissioning of corruption and fraud risk management

In order to achieve an effective management of corruption and fraud risks, it is proposed to delegate it to specific members of the organisation by setting up a working group. Alternatively, the entity may delegate this responsibility to an existing organisational unit.

Box 2: *Factors affecting the composition of the group*

- ✓ **The size of the carrier**. There is variation between the requirements of different operators. This differentiation lies in the fact that the larger the body, the broader the authority that its members must have.
  working group.

- ✓ **The functional structure of the operator**. A more complex administrative structure, which is characterised by a multitude of responsibilities, requires the participation in this working group of officials from several different organisational units of the Operator. Conversely, smaller organisations with limited responsibilities may delegate the assessment of corruption risks to a small group of officials.

In this respect, it should be noted that risk assessment is also carried out by the internal Audit units as part of their responsibilities. However, internal audit takes into account all the risks to which the entity is exposed, one of which is the risk of corruption and fraud. The process shall include an assessment as to whether the Audits put in place by the body are effective. On the other hand, the corruption and fraud risk management process is part of the entity's self-assessment of the operation of the Audits it has put in place in its processes to prevent such a risk.

The composition of the working group should be adapted to the requirements of the organisation. To this end, its members should have sufficient working experience in different operational areas of the organisation so that system pathologies can be more easily detected, while ensuring an information exchange channel within the organisation. In addition, it is important that members have knowledge and experience in legal matters, internal Audit, human resources management, procurement, expertise in risk assessment and more generally on the general operation of the organisation.

The head of the risk management team should be an experienced member of the organisation who is capable of leading the process without requiring the continuous and direct intervention of management.

Informing staff about the start of the risk management process

Based on international experience, there is often a misconception among agency officials about corruption and fraud risk management, believing it to be an investigation to identify wrongdoing. Some may even feel fearful that their position or even the organisational unit in which they serve may be at risk. For this reason, staff are sometimes uncooperative, hence the procedure faces significant obstacles in its implementation.

The best way to deal with this fear is always dialogue. "Open communication" between the agency staff and the team will help to clarify its role, purpose and way of working, reversing any negative climate into a cooperative one.

This is achieved by informing employees, by the tone at the top, who discloses the establishment of the team, its members and its scope, stressing that its role is not to investigate corruption and fraud. In order to foster a climate of trust in the working group, it is also important to stress the confidentiality of the information it handles and the protection of the personal data it contains.

The role of the team

No one knows the processes and vulnerabilities of an institution better than those who work in it. For this reason, it is preferable that the management of the risk of corruption and fraud is carried out by the staff of the body concerned.

This option has the advantage that its managers have greater freedom to adapt the evaluation methodology to its needs, knowing in advance what information and data are available or can be collected in an easier and more cost-effective way. In addition, the self- evaluation process can also help to foster a culture of integrity within the organisation.

In addition, it has been observed that when an internal working group conducts a risk assessment while developing its response plan, the likelihood of acceptance and implementation of its results by other staff in the organisation increases. It is noted that, through a comprehensive self-assessment, the most appropriate and applicable anti-corruption measures are selected.

At this point, it is also a good practice to seek a specialist in the process.

The National Transparency Authority (NTA), responsible for the central planning and coordination of all necessary actions to enhance transparency and accountability throughout the public sector, has the necessary expertise and cooperates with the relevant bodies to provide them with the appropriate expertise in managing the risks of corruption and fraud. In addition, it can make an important contribution to the training of the relevant team members and to the provision of tools and standard forms.

Team empowerment and training

To achieve the objective of the group, there must be a common understanding of the risk management process, its working framework and the roles of all its members.

For this purpose, several meetings of this group must be held beforehand.

In the context of the above, their familiarity with the definition of corruption and the ways in which it occurs within the organisation's operations, as well as the methods of dealing with it through the strengthening of existing Audit mechanisms or the design of new ones, in order to strengthen integrity in the organisation, will be assessed.

Organisational issues such as the functioning and management of the team (duration, tasks of members, how meetings are organised, how information is collected and processed, etc.) should also be addressed.

It is important that the head of the organisation is present at the first meeting. His presence will emphasise the importance of this process and his support for the group.

Corruption and fraud risk management process

Based on internationally recognized standards (ISO 31000: 2018, IEC 31010: 2019, COSO IC-IF 2013, INTOSAI 9100, etc.) and international guidelines (O.O.S.A, United Nations Development Programme (UNDP) and also taking into account the United States Agency for International Development (USAID)), as well as the good practices of countries such as Australia, the Netherlands and Slovenia,[3] lists the steps to be followed in any corruption and fraud risk management process.

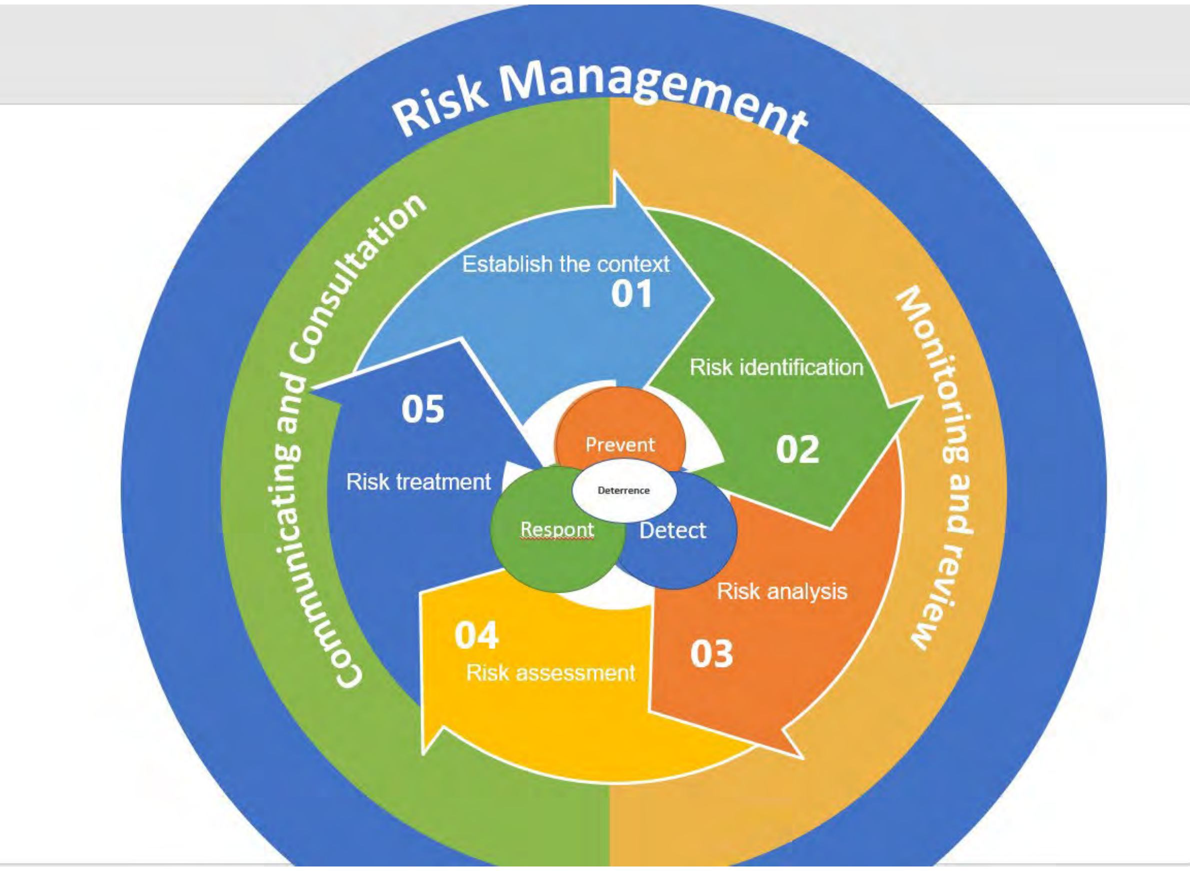


Figure 4: Risk management

[3] Three countries were cited as good practices in Corruption Risk Assessment, according to the recent edition of the Regional Anti-Corruption Initiative: Corruption Risk Assessment in Public Institutions in South Eastern Europe: Comparative Study and Methodology. Available at: http://rai-see.org/focus/corruption-risk-assessment-in- publicinstitutions-in-south-east-europe-comparative-study-and-methodology/

The "identification of the environment" as a **first step** identifies the purpose and criteria by which the risk assessment will be made based on the internal and external factors affecting the operation of the entity.

The **second step,** "risk identification", records the various events that may affect the operations of the organisation.

The **third step**, "risk analysis", identifies the nature and causes of the risk.

In the **fourth step**, "risk assessment", an assessment is made of the likelihood of the event occurring and its impact in areas such as economic loss, loss of reputation, etc. This step includes the calculation of the inherent risk, the review of the Audits and finally the assessment of the residual risk.

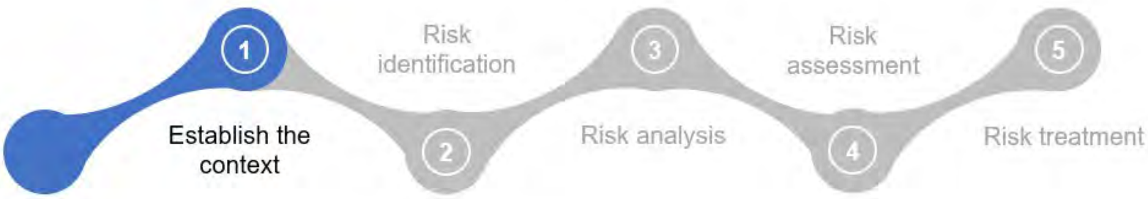
Finally, the **fifth step**, "risk response", concerns the selection of appropriate corrective measures to effectively address the identified and assessed risks of fraud and corruption.

RISK ASSESSMENT

RISK MANAGEMENT

Throughout the process there must be smooth communication and consultation so that the management of the organisation is informed in a timely and appropriate manner in order to take any measures to address the risks. At the same time, the whole process is subject to continuous 'monitoring and review' in order to take into account new threats and opportunities arising from the constant changes in the internal and external environment of the organisation.

Step 1: Establish the context



The objective of this step is to analyse the internal and external factors that affect the operation of the entity and determine the range of risks to which it is exposed.

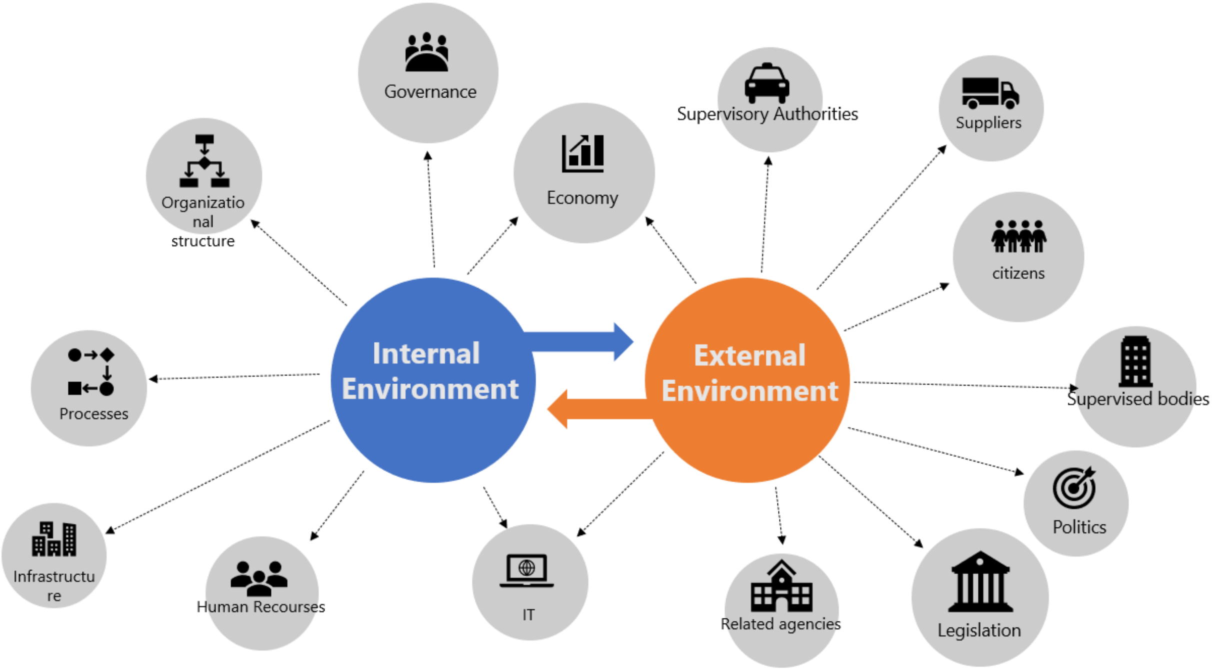


Figure 5: Environment of the operator

The group conducts a broad overview of the ways in which corruption can affect any public body. The table below sets out the common types of corruption risks to which all public bodies are vulnerable, which are divided into vulnerabilities arising outside or inside the body. Addressing some of these, as a result of external factors, is considered useful to start the process, as it mitigates the concerns of specific individuals within the body about their potential involvement in corruption. As team members become more comfortable with identifying risk stemming from the external environment, the risks arising from the internal environment of theoperator can then be introduced into the process.

***Table 1**: Examples of vulnerabilities of public sector bodies to corruption*

	REASONS FOR CONTACT	**EXAMPLES OF VULNERABILITIES**
EXTERNAL VULNERABILITIES They concern relations withthe private sector or the public Possible incidents ofcorruption could be trafficking influence, personal favouritism or briberyaffecting the Decisions	Receipt of money	Exemption / low collectability of taxes,licensing fees, import duties
	Matters relating tocontracts	Favor to a supplier at the stage of itspreparation tender or contract award, photographicspecifications
	Payme nt supplier s	Preferential treatment of a particular supplier (non-compliance with the orderof priority)
	Issuance of licence /Report	Issuing passports, building permits, inspection reports, driving licences in anillegal manner
	Application of law orrules	Risk of not reporting violations and other incorrect incidents, investigationor prosecution of a person without strong evidence
INTERNAL VULNERABILITIES They concern the management of publicassets Possible incidents of corruption could be embezzlement, fraud ortheft	**TYPE OF ASSET**	**EXAMPLES OF VULNERABILITIES**
	Money	Non-issuance of collection receipts /fictitious overtime
	Permanent	Removal of fixed assets or stocks of theentity
	Information	Theft/sale of confidential informationabout an individual tender or future acquisitions of the operator, national data or nationalsecurity, etc.

External context (external context)

At this stage, the group should reflect on the external factors that shape the agency's action, the behaviour of its employees, the powers the agency has vis-à-vis of these factors (for example, it cannot modify the legislation governing contracts). Therefore, a wide range of factors affecting the operator such aslegal, political, regulatory, financial must be considered, technological, economic, physical and others.

> "It's no good leaving a living dragon out of your calculations when you live next door to it."
>
> J.R.R. Tolkien

Box 3: *Assessment of how external factors affect the operator*

- What are the laws governing the body's operations and what powers are granted to the body over them?
- Which government bodies supervise the body; Parliament, the Court of Auditors, another supervisory authority?
- How do these institutions react to reports of corruption?
- Who investigates allegations of corruption? (An internal inspector, the police, the National Transparency Authority?)
- Who are the parties involved (citizens, suppliers, others?)
- Do the interests of the parties involved coincide with those of the operator?
- What is the degree of media coverage the institution receives?

Internal context (internal context)

With regard to the internal environment of the entity, the team should take into account the framework governing its governance, its organisational structure, its responsibilities and horizontal functions, as well as specific processes that are a significant source of risk.

The current internal audit guidelines from INTOSAI[4] for public sector entities identify five factors that form the foundation of each entity's internal audit system, as detailed in Box 4. The guidance demonstrates how these five factors affect the overall internal climate of the entity, which in turn affects the internal Audit system. Any weaknesses in any of these factors, or deficiencies in their implementation, place the organisation at significant risk of any form of fraud or corruption.

Box 4: *Factors to consider in an organisation's internal Audit system*

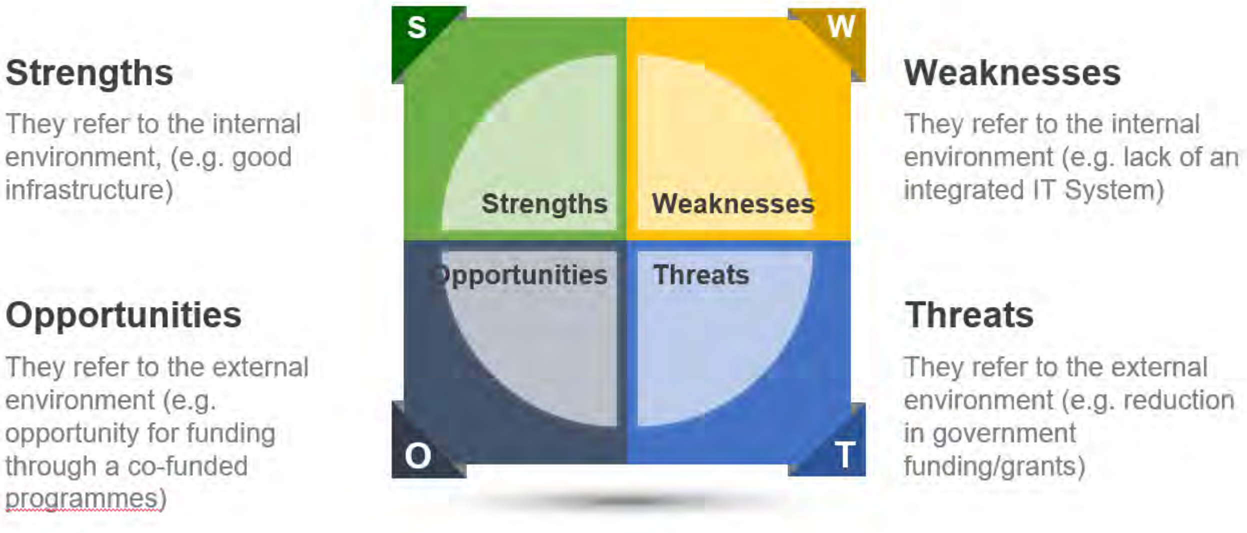
1. Personal and professional integrity of staff
2. Commitment to maintaining and improving staff expertise
3. Philosophy (tone at the top) of the management of the organisation
4. Organisational structure of the body
5. Policies and procedures in human resources management

Source.
PUBLIC SECTOR

Using Boxes 3 and 4 above, it is important to ensure that team members have a common and sound understanding of the environment in which the institution operates, as well as knowledge about the opportunities they have to influence that environment. Thepreparation of a memorandum summarising this information is an effective way of ensuring a good process for identifying corruption risks.

[4] INTOSAI, INTOSAIGOV 9100: GUIDELINES FOR INTERNAL AUDIT STANDARDS FOR THE PUBLIC SECTOR

Furthermore, according to the international literature, a good practice for capturing all this information is in the form of a SWOT table, as illustrated in the figure below:



Strengths

They refer to the internal environment, (e.g. good infrastructure)

Weaknesses

They refer to the internal environment (e.g. lack of an integrated IT System)

Opportunities

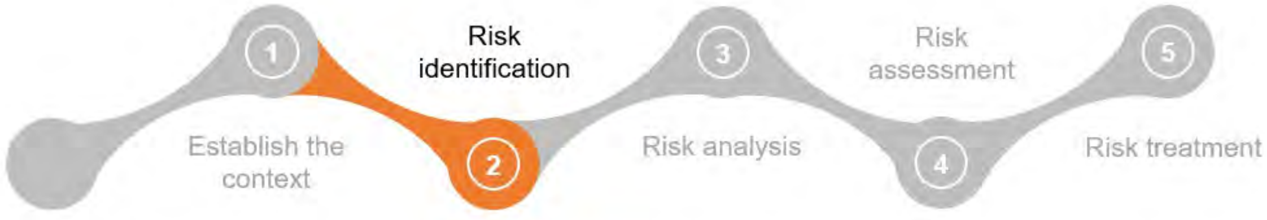
They refer to the external environment (e.g. opportunity for funding through a co-funded programmes)

Threats

They refer to the external environment (e.g. reduction in government funding/grants)

Figure 6: *SWOT analysis*

Step 2: Risk identification



The aim of this step is to identify the risk of corruption and fraud. Team members should make use of any information they know about their organisation's operations.

A key feature of this process is the participation of the competent executives of the relevant service units of the organisation (at the level of Director General, Director or even Head of Department). These managers are confronted on a daily basis with risks of corruption and fraud in their area of responsibility. They are therefore best placed to assist the team in identifying and assessing risks more accurately.

It is suggested that the process of identifying corruption and fraud risks should take the form of brainstorming sessions, where members of the working group freely exchange ideas to draw up a list of corruption/fraud scenarios to which the institution is potentially vulnerable. One way to do this is to ask the group to "think like a thief", i.e., like someone who wishes to gain an advantage by avoiding procedures or legal requirements.

During the exchange of ideas, one way to start the identification process is to ask the group to identify specific corruption and fraud risks and scenarios that they believe could harm the organisation in the future, starting with those that are already harming it. It is particularly important, where corruption scenarios are based on incidents that have already occurred within the organisation, that they are analysed independently of the outcome of any disciplinary or other proceedings.

All possible information that can help the team to identify weaknesses and risks of corruption and fraud should then be collected and analysed.

Common sources of relevant information:

α. **Conducting interviews** with supervisors and employees of the organization is the most important method of obtaining information. During the interviews, a good practice is to **fill in a questionnaire, which** will help to frame the discussion and cover all the parameters to be taken into account to identify the risk and its causes. An indicative questionnaire basedon the Corruption Risk Management Guide is provided in the Annex: '*IPA Twinning Project, Support to Efficient Prevention and Fight against Corruption, Corruption Risk Management: Addendum to the RiskManagement Guidelines, 2016*".

b. The **collection of statistical data** from which the team can draw conclusions, for example on the workload of officials by department or regional office, in order to justify or not justify possible delays or lower collections.

c. A **review of the forms** used to carry out certain tasks, whereby the team can identify issues of inadequacy of the system of supervision, approvals and accountability, sufficient automation and standardisation of the process, etc. For example, the form can be used to draw conclusions as to whether the execution of a procedure requires the signature of only one official and/or his/her superior.

Methods of data analysis:

- Conducting interviews with management and staff
- Completion of questionnaires
- Collecting statistical data (published or not)
- Review of the standardized documents used
- Review of IT systems
- Identifying and analyzing any past audit findings of internal and external auditors, public records and/or complaints from citizens

d. The **review of information systems.** The overview of information systems. The team can on the one hand capture to what extent the processes followed are automated and on the other hand, if these systems are sufficiently supported, so that they are available at all times and the operator is not at risk of possible data losses or leaks.

e. The **analysis of publications, complaints** and previous **audit findings,** that can help the team to identify the vulnerabilities, which exploited, or that could be exploited, in the course of committing incidents of corruption or fraud.

In order to identify the risk of corruption and fraud, an important element is the examination of the behaviour of the person committing illegal acts. In this context, the fraudtriangle analysis mentioned in **Figure 2** is a good practice.

The following box lists six common ways in which assets and public money can be misappropriated. It is suggested that these possible ways of committing corruption be shared during the exchange of ideas meeting in order to encourage discussion. In the event that the group identifies any of these risks in its organisation, the relevance of the identified risks on the list to its objectives should be determined, as members should focus only on those types of corruption that have a realistic likelihood of occurring within the normal operations of their organisation.

Box 5: *Some common forms of asset fraud and corruption*

1. Theft of small amounts of money (skimming). Cash is removed from the entity before it is recorded in the entity's financial statements. For example, an employee of the institution collects the entrance fee to a museum, either without issuing the legal document or by issuing a false receipt.
2. Theft of large sums of money (Larceny). Cash is removed after it has been entered in the financial statements of the entity. More complicated than skimming. May involve entry in a different account or incorrect entry to conceal the theft. At least two persons are involved in the illegal process in the case where the responsibility of collecting and recording the amount of money is assigned to two or more employees of the entity.
3. Fraudulent disbursements. Money is paid for goods that are not delivered to the organisation or for services that are not performed. An employee assigns a friend to do cleaning work on weekends. The employee's friend does not perform the work but nevertheless submits a bill for services not performed.
4. Payroll. Included in payroll are individuals who never show up for work or who may no longer work for the organization. Employees request overtime pay even though they did not work overtime.
5. Travel expenses. Employees claim expenses for trips they have not taken or overpay for expenses of a trip taken. The

hotel employees, in some cases, provide false or overcharged invoices for a fee.

6. Theft of fixed assets. Office supplies, furniture and other items that can be easily sold are not properly recorded at the stage of their receipt by the institution's employees or the entries are falsified after the receipt of their invoices.

Source: Singh and Bussen, Management Compliance: a how-to guide (2015).

It should be noted that the purpose of this stage is not to simply list every form of corruption risk to which the entity may theoretically be exposed, but instead to create a realistic, manageable list of risks that can then be prioritised according to their importance.

The size of the list will depend, first and foremost, on the number of functions carried out by an institution. For example, the list of potential corruption risks for an entity that collects fees, issues operating licences and procures goods and services will be longer than the listfor an entity whose sole function is to issue licences. As the group develops the list, it shouldlook for ways to consolidate individual vulnerabilities into broader categories. For example, an entity's employees in more than one department may be responsible for collecting cash payments from the public for providing different services. Rather than listing cash collection as a separate vulnerability for each department, all of these could, instead, be included in a risk titled "Likelihood of Cash Theft or Money Security Risk".

It is important, when the team identifies corruption risks, to avoid the following failures:

- ➔ The "illusion of the checks and balances". The existence of a safety net gives the impression that the risk is no longer possible and, therefore, it should not to be included in the list. However, in most cases, incidents of corruption/fraud take place when individuals circumvent the existing checks and balances and, therefore, their existence alone does not guarantee the elimination of the risk they are called upon to address.
- ➔ The "rule of the ancients". Often the opinion of the most senior employees overlaps with that of the younger ones, resulting in a lack of appropriate an environment of critical thinking and that not all views are freely expressed. This may be due to the fact that younger employees do not want to be confronted by older or more senior colleagues.

To avoid this, the team leader should encourage all members to express their views through various techniques, such as creating two groups, one for junior and one for senior employees, so that their views can be discussed in a single debate later. Another technique is for group members to submit their views anonymously and then discuss them in the group.

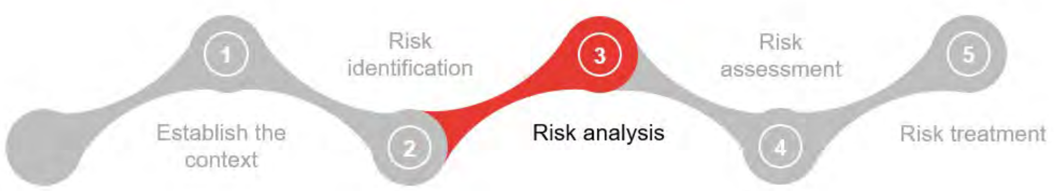
In general, at this stage, it is advisable to include as many risks as possible. Besides, the exclusion of certain risks can be carried out in subsequent stages.

In order to record the identified corruption and fraud risks, it is proposed to complete the table below:

Table 2: *Identification of corruption and fraud risks*

Identifying risks of corruption and fraud				
Procedure / Function	**Objective of the process/operation**	**Danger**	**Source of risk**	**Consequences**

Step 3: Risk analysis



The identified potential risks from the previous step are grouped into categories and an attempt is made to identify the cause of the potential risks, as shown in the table below:

Table 3: *Indicative corruption and fraud risks and possible sources*

Risk category	Danger	Potential sources of risk
Governance	Insufficient or inadequate functioning of reporting mechanisms problems and complaints	Lack of a strategy and mechanism to prevent, detect and respond to incidents of corruption and fraud
	Internal or external interventions	Lack of a strategy and mechanism to prevent, detect and respond to incidents of corruption and fraud
Regulatory framework	Non-compliance with legal/regulatory framework	The regulatory framework is complex, unclear and contradictory

Organization & operation	Limited resources and infrastructure	The structure of the organism is not functional
	Money / file / asset security	The structure of the organism is not functional Lack of security measures Lack of monitoring systems
	Inadequate or inefficient procedures	Complexity of procedures, lack of documentation
Supervision	Insufficient guidance	Ineffective instructions and guidance from management
	Incorrect information provided by management	Lack of monitoring systems
	Ineffective provision of delegation, oversight, approvals and accountability	Lack of authorisation and approvals policy
	Inadequate or ineffective procedures for allocating and charging for work	Inadequate or ineffective instructions and guidance from management
Information systems	Inadequate information systems	The information system does not provide sufficient automation of all procedures and approvals The information system is not interoperable with other systems The information system does not

		is adequately supported The information system does not provide electronic document handling The information system does not offer the possibility of digitising documents
	Not ensuring the confidentiality and access to information systems	Lack of political access to the information system
	Loss or misuse of personal data	Lack of political access to the information system
	Failure to ensure the authenticity of supporting documents	Lack of interoperability between information systems
Human resources	Insufficient training of human resources	Lack of policy human resources training
	Inadequate human resources management	Lack of planning policies for staffing, deployment and movement of staff
Information and communication	Insufficient information to the stakeholder and lack of communication rules	Lack of political communication with the public

Note that the above table is indicative, for the convenience of the group. In any case, it may be modified according to the identification of the environment and the results of the risk identification process as carried out in the previous steps.

This phase is designed to enhance the understanding of the nature of each identified risk. As can be seen in the table above, it should be noted that all corruption risks are not only financial. In addition to financial risks, there is also reputational risk, as well as the risk that can cause problems in the ability of the entity to carry out its own mission. Categorising risk in this way is considered particularly useful at the impact analysis stage.

Box 6: *Example of a corruption risk impact assessment*

A body whose mission is focused on ensuring the quality of food products by meeting specific hygiene standards to maintain public health is a good example of riskcategorisation. A relatively small bribe could potentially lead an inspector to ignore compliance with hygiene standards, thus allowing a contaminated product to reach the public, causing harm to the health of large numbers of people. The economic impact onthe operator is negligible. However, the impact on the reputation and ability of the operator to fulfil its mission is enormous.

The analysis and categorisation of risks will help the organisation to understand the areas where it has weaknesses and facilitate the process of identifying the factors that contribute to causing them.

Risk register (risk register)

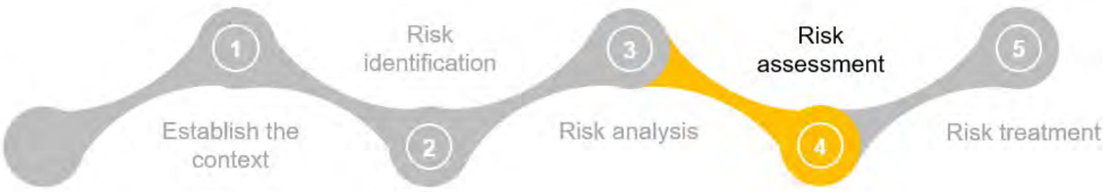
A good practice is to create **a risk register,** in which the categories of risks, as shown in **Table 4, and the** results of the assessment and response process, which will be carried out in the next steps, will be recorded in detail.

With the register, the operator will be able to gather, in a systematic approach, all the information on the potential risks to which he is exposed, analyse them and at the same time draw conclusions about the level of overall risk it is at.

Table 4: *Corruption & fraud risk register*

Risk category	Danger	Potential sources of risk	Units involved	Existing safeguar dsAudit	Risk assessment	Respon se actions (in summ ary)		

Step 4: Risk evaluation



At this stage, the potential risks identified in the previous step are prioritised in order to be included in a response plan based on their severity. Where the number of potential risks is relatively small, prioritisation is not necessary.

> "Risk assessment is mainly based on subjective perceptions. However, perceptions of some people can be prove to be quite accurate even from a quantitative point of view."
>
> Ad Hoc Risk Assessment Review Group, Risk Assessment: Review Group Report to the United States Nuclear Regulatory Commission (September 1978)

The identification and treatment of any risk of corruption that occurs in an organisation and becomes apparent, for example from a falsification in the date of an invoice, to a bribery scheme involving several employees and external parties, is considered difficult or even impossible. Also, assuming that the institution aims to eliminate all possible corruption and fraud risks that threaten it, unlimited resources would be required to deal with them. Therefore, any plan must be realistic in terms of prioritising potential risks of corruption and fraud.

It is also important to note that the identification and analysis carried out in the previous steps relates to inherent risk, i.e. without taking into account any positive effects of specific procedures and Audits that have been designed and are in place. This was done in order to avoid the 'illusion of the Audit loop' as discussed in the risk identification step. The effectof the Audit loopholes will be examined using the method discussed below, so that ultimately the residual risk of corruption and fraud can be assessed.

Review existing Audits (review existing Audits)

In order to assess the risk, the team should analyse any existing risk Audit mechanisms(Audits) in place that contribute to mitigating the risk.

Audits relate to policies and procedures used by the entity to address identified risks.

Examples of checks and balances include:

- ➔ Fiscal Audits (e.g. separation of duties when taking over expenditure, clearance and payment).
- ➔ Management Audits (e.g. business planning, methods and procedures adopted by managementto ensure that its objectives are achieved, including measurement systems, reporting and monitoring of plan performance).
- ➔ Physical checks (e.g. stock counting).
- ➔ Information technology systems audits (e.g. access Audits, issuing reports and statistics, etc.).

> The **Audit of compliance with procedures** is a core responsibility of theInternal Audit Function and is carried outby a specific methodology in accordance with international internal Audit standards. AtIn the context of corruption and fraud risk management, a general risk assessment is carried out.
> a review of the adequacy of the Auditsin relation to the risks identified.

Examining the adequacy of the Audits will help the team to identify any weaknesses in risk management and ultimately calculate the residual risk, i.e. the residual probability of the risk occurring. This will help to decide whether or not to take additional measures to address the risk. The higher the residual risk, the more urgent the need to improve existing Audits or introduce new ones. The adequacy of existing Audits depends on the nature of the risk they are designed to adderss and their characteristics as shown in the following figure:

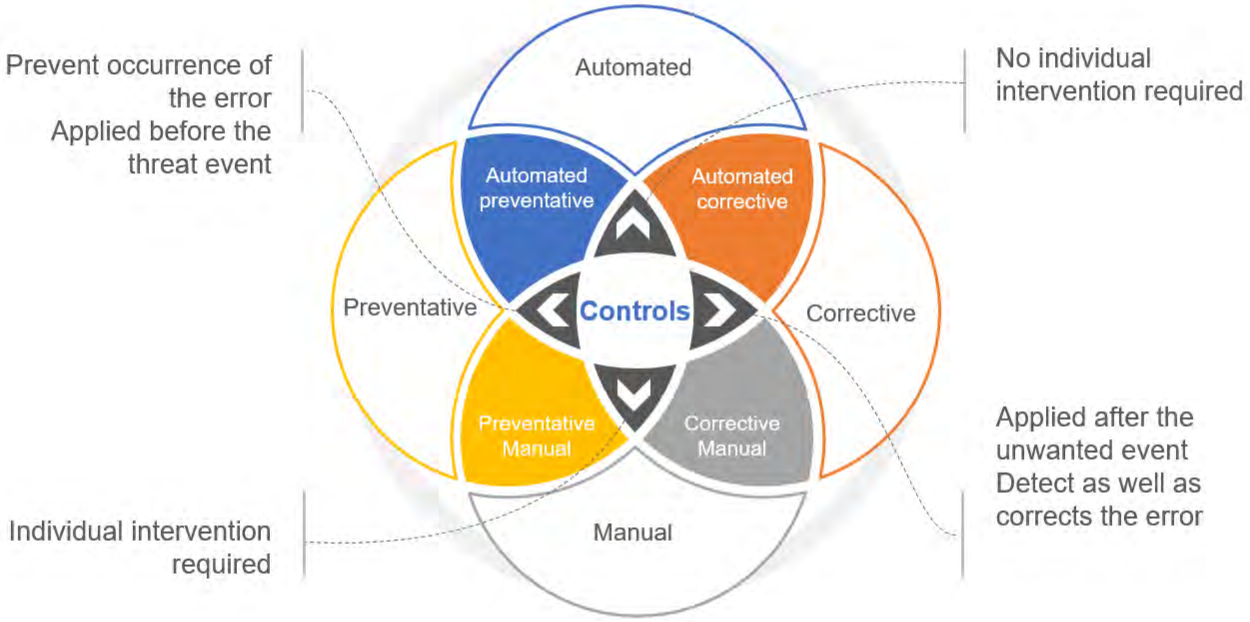

Prevent occurrence of the error
Applied before the threat event
Automated
No individual intervention required
Automated preventative
Automated corrective
Preventative
Controls
Corrective
Preventative Manual
Corrective Manual
Manual
Applied after the unwanted event
Detect as well as corrects the error
Individual intervention required

Figure 7: *Types of Audit nets*

To facilitate the process of analysing the adequacy of the Audit mechanisms, the organisation may define specific assessment criteria as described in the table below:

Table 5: *Analysis of the adequacy of the Audit network*[5]

Analysis of the adequacy of the Audit network				
Description of risk				
Description of the Audit network				
Type of Audit net	**Preventive**	**Suppressive**		
Criter ion			**Yes**	**No**
Have the persons responsible for monitoring the Audit network been designated?				
Is the frequency of operation of the Audit valve satisfactory?				
Is the monitoring of the Audit network measured by specific data?				

[5] Adapted from Guide for Corruption Risk Management, 2015, Presidency of the Republic of Colombia

<table>
<tr><td colspan="2">Is the check valve automatic?</td><td></td><td></td></tr>
<tr><td colspan="2">Is there any indication or any evidence that the safeguard has been breached in the past?</td><td></td><td></td></tr>
<tr><td colspan="4"><b>The check valve is estimated to reduce the inherent risk in terms of:</b></td></tr>
<tr><td><b>POSSIBILITY</b></td><td><b>CONTACT</b></td><td colspan="2"><b>NEITHER.</b></td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
</table>

Residual risk evaluation

The team, having now identified its operating environment and having identified the relevant risks faced by the entity, as well as the existing Audits, is asked to assess the significance of each risk on the basis of two parameters:

- the likelihood **of** the risk occurring, and
- the impact that its implementation may have.

In particular, probability relates to how often a particular risk is considered to occur (occur) within a given period of time. Impact refers to the assessment of the consequences that the occurrence of the risk may have on the operations, reputation and financial results of the entity.

The scoring of the risk in terms of the parameters of likelihood and impact is largely based on the experience and professional judgement of the team. In making this decision, a variety of characteristics of the area under assessment are taken into account, which may be both quantitative and qualitative.

In particular, the **analysis of the probability of occurrence of** each risk can be carried out on the basis of the following classification:

Not at all likely (1)	It happens in exceptional cases. The risk has not occurred in the last five years.
Rare (2)	It can happen. The risk occurred once in the last five years.
Possibl e (3)	It is possible to happen. The risk has occurred once in the last two years.
Very likely (4)	The risk occurs in the majority of cases. The phenomenon occurred once in the last year.
Almost certainly (5)	The risk is expected to occur in the majority of cases. It is certain to happen and occurred more than once a year.

Working group members should take a number of factors into account when determining assessments of the likelihood of corruption risks. The questions outlined in **Box 7** may serve as an appropriate starting point for this process.

***Box 7**: Questions to assess the likelihood of corruption risks occurring*

1. How complex is a possible corruption scenario and how many people are needed to commit it?
2. Have similar corruption scenarios occurred in the institution or in other public bodies?
3. To what extent could those involved in such a corruption scenario benefit?
4. How many officials or executives of other agencies could be involved in the procedures to carry out the corruption scenario?

Research shows that when people are asked to make probability assessments, they overestimate the occurrence of events with which they are familiar or which can easily remember, on the one hand, underestimating or ignoring, on the other hand, their past experiences. According to Cognitive Psychology[6] , this cognitive bias is called "selective memory". For example, if a recent bribery incident has taken place, or if the media and political debates focus on issues related to corruption in the country, such as bribery, there is a much greater likelihood that individuals will identify bribery as more likely to occur and assess it as more destructive than other forms of corruption. However, less obvious types of corruption, such as concealing the interests of an entity's employees in a competitive process for a public contract award, where it is in fact more likely to occur, are not assessed accordingly.

Questions that can be asked in interviews and group discussions to minimise this negative impact are:

➔ Why does a respondent believe, in the context of an interview, that one type of corruption is more likely to occur in the organisation than another?

➔ What factors are behind this crisis?

➔ Are there any current corruption cases or corruption issues that are currently being highlighted in the media that may affect the working group discussions in the institution;

The analysis of the **potential impact of** each risk can be carried out on the basis of the following rating:

[6] Tversky, Amos; Kahneman, Daniel (1973).
Cognitive Psychology. 5(2): 207-232. DOI: 10.1016/0010-0285(73)90033-9. ISSN 0010-0285.

Insignificant	• Possibly cause some additional work but without delay in achieving the objectives of the organisation and impact on its reputation
Limited	• Slight delay in achieving its objectives operator without impact on its reputation
Medium	• Delay in achieving the objectives of the body by little impact on his reputation
Important	• Very significant delay in achieving the objectives with a major impact on its reputation
Critical	• Inability to achieve the mission of the body, with as a result of which the reputation of the

Since determining impact involves several subjective judgements, it is suggested that the following questionnaire be used:

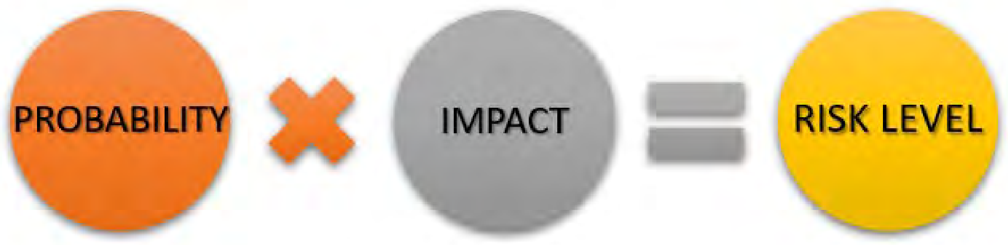


***Table 6**: Determining the impact of a corruption risk*[7]

A/N	The risk could	YES	NO
1	affect all of the agency staff involved in the process;		
2	affect the achievement of the entity's objectives;		
3	affect the achievement of the agency's mission;		
4	affect the achievement of the mission of the sector of activity to which the entity belongs in general;		
5	cause a loss of credibility to the operator, affecting its reputation;		
6	cause a significant economic impact;		

[7] Adapted from Guide for Corruption Risk Management, 2015, Presidency of the Republic of Colombia

7	affect the delivery of services to citizens;		
8	be detrimental to the quality of life of society, due to the loss of goods or services or public resources;		
9	cause loss of carrier data;		
10	cause the Audit bodies or the police to intervene?		
11	impose administrative sanctions;		
12	to trigger the initiation of disciplinary proceedings (CDR);		
13	to impose tax penalties?		
14	bring criminal sanctions?		
15	cause a loss of credibility in the operator's field of activity;		
16	cause bodily injury or loss of life;		
17	affect the reputation in the place where the operator operates;		
18	to affect the reputation of the operator across the country;		
Total number of affirmative answers		**Total negative Answers**	
Categorisation of impact:			

Insignificant		Limited		Medium		Important		Critical	

Based on the number of positive responses in the table above, the impact is graded as follows:

Table 7: *Rating of the impact of a corruption risk*[8]

Number of positive responses	Description	Level
0-2	Insignificant	1
3-5	Limited	2
6-8	Medium	3
9-10	Important	4
11-18	Critical	5

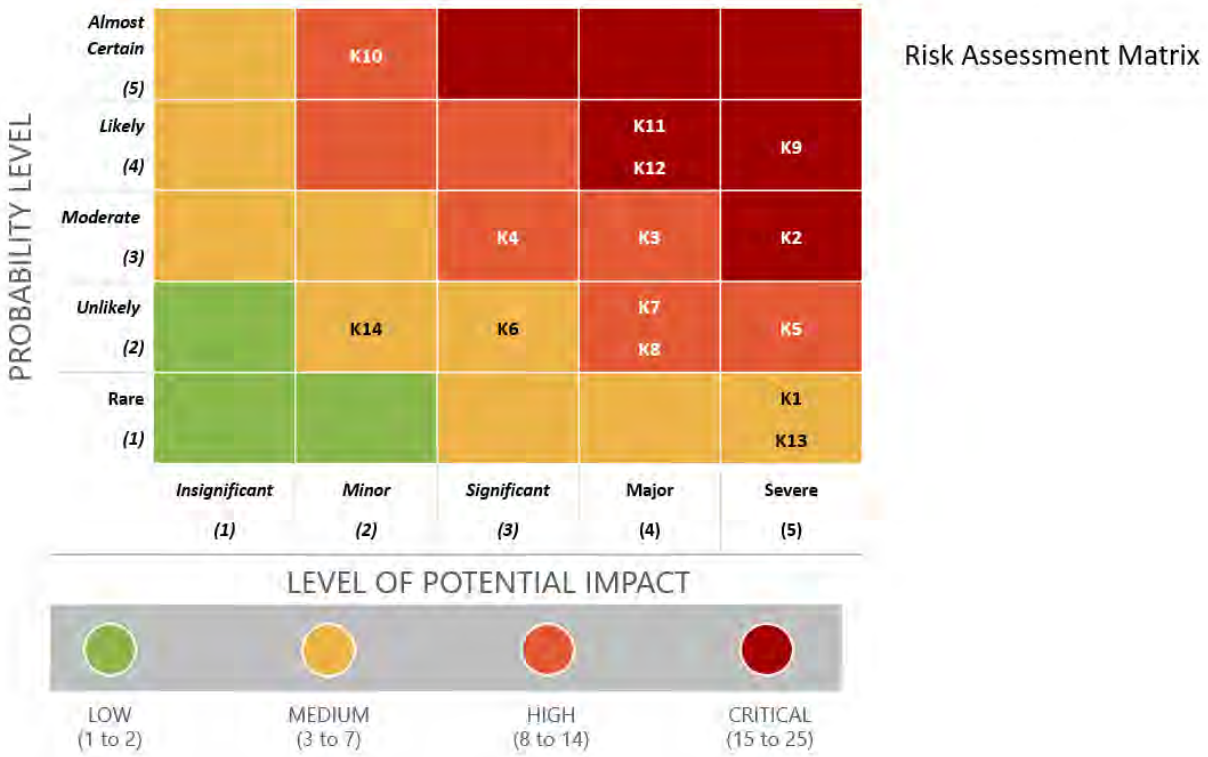
Then, the following function is used to calculate the importance of a risk:

Figure 8: *Risk level calculation function*

According to this function, risk is graded on four (4) scales, as shown in the table (risk map) below:

[8] Adapted from Guide for Corruption Risk Management, 2015, Presidency of the Republic of Colombia

***Table 8:** Corruption & fraud risk ranking (heat map)*



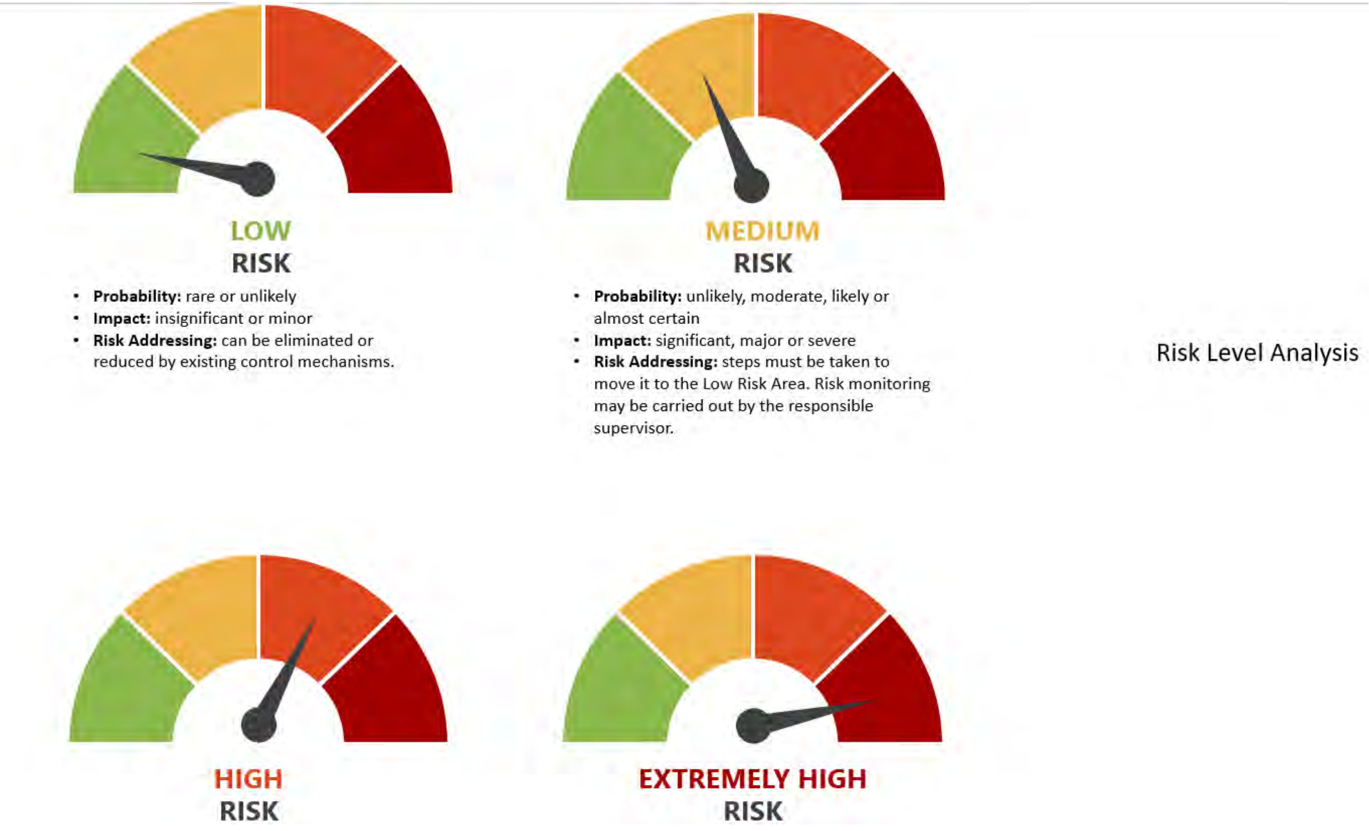
Risk Assessment Matrix

PROBABILITY LEVEL	Insignificant (1)	Minor (2)	Significant (3)	Major (4)	Severe (5)
Almost Certain (5)		K10			
Likely (4)				K11 K12	K9
Moderate (3)			K4	K3	K2
Unlikely (2)		K14	K6	K7 K8	K5
Rare (1)					K1 K13

LEVEL OF POTENTIAL IMPACT

LOW	MEDIUM	HIGH	CRITICAL
(1 to 2)	(3 to 7)	(8 to 14)	(15 to 25)

Note that the proposed rating scale is indicative and is provided for the convenience of the operator. The above table shows:



Risk Level Analysis

LOW
RISK

- **Probability:** rare or unlikely
- **Impact:** insignificant or minor
- **Risk Addressing:** can be eliminated or reduced by existing control mechanisms.

MEDIUM
RISK

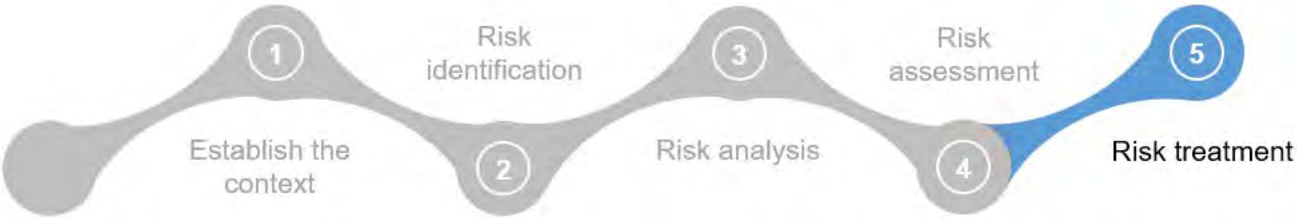
- **Probability:** unlikely, moderate, likely or almost certain
- **Impact:** significant, major or severe
- **Risk Addressing:** steps must be taken to move it to the Low Risk Area. Risk monitoring may be carried out by the responsible supervisor.

HIGH
RISK

EXTREMELY HIGH
RISK

Figure 9: *Risk level analysis*

Step 5: Risk treatment



The final step of risk management is the selection of appropriate corrective measures to effectively address the risk of fraud and corruption identified, analysed and assessed in the previous steps of the process.

Attitude towards risk (Risk Attitude)

The management of the entity should first decide what actions it is willing to take for each of the risks, and ultimately determine its level of **risk** tolerance as follows:

Risk Treatment Options

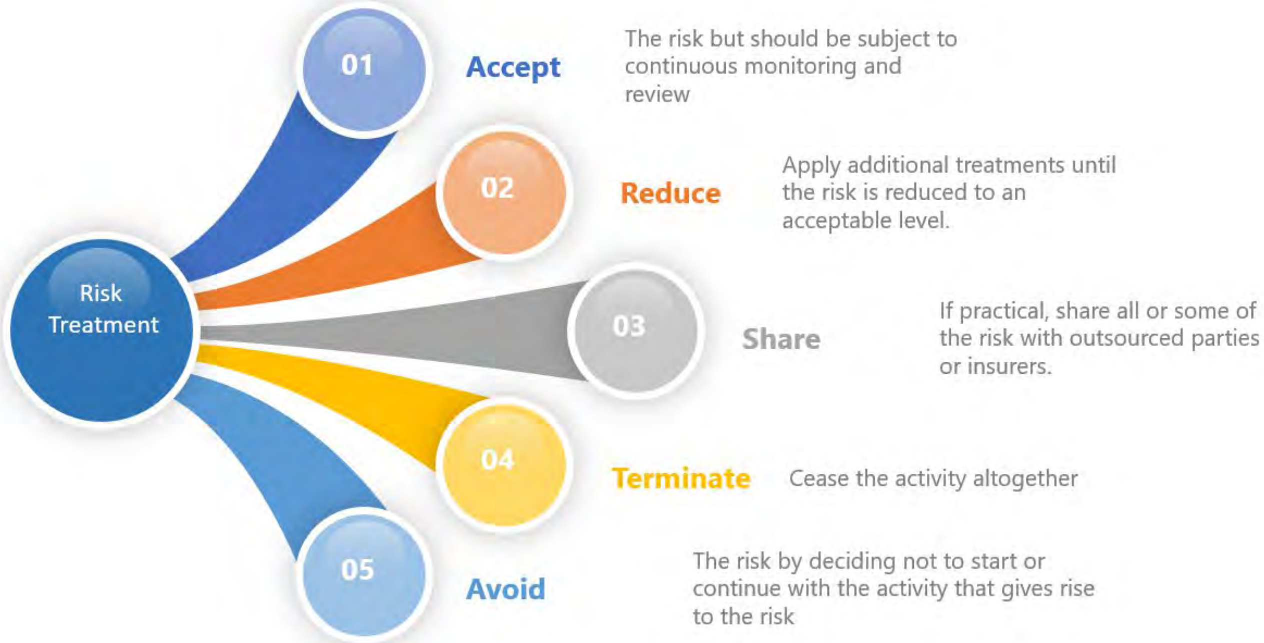

Risk Treatment
01
Accept
The risk but should be subject to continuous monitoring and review
02
Reduce
Apply additional treatments until the risk is reduced to an acceptable level.
03
Share
If practical, share all or some of the risk with outsourced parties or insurers.
04
Terminate
Cease the activity altogether
05
Avoid
The risk by deciding not to start or continue with the activity that gives rise to the risk

Figure 10: *Attitude towards risk*

It should be noted that it is not possible to eliminate all the potential risks identified in an operator. No system is perfect, as often individuals who commit corruption or fraud will find new methods to circumvent existing Audit systems.

Designing measures to address the risk of corruption and fraud

Based on the attitude towards the risk of corruption and fraud decided by management, the corresponding actions should be designed and implemented to address the risk.

Response actions may include policies, procedures and management systems to prevent, detect and respond to incidents of corruption and fraud (see **Figure 3**).

In the table below it is proposed that the team should fill in for each risk, the actions and activities they intend to develop, the indicator by which implementation will be monitored, the resources required, the deadlines for their implementation and the person responsible for monitoring them:

Table 9: *Actions to address corruption & fraud risks*[9]

Actions to address a risk of corruption & fraud					
Description of risk					
Level of risk	**Low**	**Medium**	**High**	**Extreme**	
Existing checks and balances	1. 2.				
Attitude towards risk	E.g. Acceptance, probability reduction, impact reduction, rollover, source elimination				
Response actions (in detail)		**Resources**	**Observation index bathing**	**Deadline for implementation**	**Implementation Manager**
1					
2					

[9] Adapted from Guide for Corruption Risk Management, 2015, Presidency of the Republic of Colombia

Identifying the existing Audits that need strengthening will not always be easy. The team should assess the effectiveness of existing Audits individually (see **Table 5**) and collectively (see **Table 9**).

In this way, areas where excessive and/or overlapping Audits exist can be revealed, so thatby eliminating them, resources can be saved without increasing the overall risk of corruption.

Box 8: *Example of identifying redundant Audits in the context of risk assessment*

The assessment of the fraud risks and existing Audits in one organisation revealed that there were three separate Audits in place to ensure that the organisation's office equipment was not stolen. Firstly, detailed weekly inventories of all office equipment in the organisation's headquarters building were carried out by auditors. Secondly, the organisation's security department placed guards at each exit of the building, who inspected all staff and packages mailed from the building. Third, the guards were monitored by closed circuit cameras supervised by a third party. The agency concluded that, given these multiple and independent audits, the frequency and intensity of office equipment audits could be reduced and the audit resources freed up could be allocated toauditing other agency functions.

Most institutions have limited resources and should therefore consider the need to design and activate additional Audits to address specific corruption and fraud risks in a cost- benefit perspective. In particular, the group should consider whether the proposed new Audits are affordable and feasible to implement. For example, assigning additional tasks toan employee and subsequently moving him/her to perform them may not be particularly costly, but it is not inexpensive either. The institution should weigh both the cost of the employee's travel and the time away from his or her normal duties. If the travel requires an absence of one or more days, in case the institution has limited financial resources, the cost of transport, accommodation and daily allowance for its staff member may be considered particularly onerous.

In addition to ensuring the cost-benefit ratio in the operation of the Audits, the team should also consider the feasibility of their implementation. For

For example, if an audit trail involves a major policy or institutional reform or legislative change it is considered particularly time-consuming and complex. Therefore, although the above measures may address a specific risk, they are nevertheless so burdensome for the body (time, staffing, modification of information systems, political processes) that theycould potentially affect the body's ability to fulfil even its institutional mission.

Therefore, the checks and balances must be specific and clear and no more costly than the damage that will be caused by the risk of corruption and fraud they are trying to prevent.

Action response plan and monitoring of progress

In order to implement the actions decided upon, the organisation shall develop a corruption and fraud risk management plan, which shall be monitored and reviewed at least annually.

For this reason, specific indicators should be developed for each action, through which the team monitors and assesses their adequacy in relation to the risk of corruption and fraud.

Continuous monitoring with periodic evaluations of the degree of implementation ensure that the
the risks to which the person is exposed
operator are under Audit.

In addition, the results from the monitoring activities are used to improve the design and implementation of the process itself. management the design and implementation of the corruption and fraud risk management process, which should

shall be carried out at regular intervals, taking into account changes that have occurred in the internal and external environment of the entity.

"He who fails to plan, plans to fail."

Winston Churchill

In order to ensure that the funding and staffing needs for the anti-corruption and anti-fraud plan are met, it is proposed to integrate its activities into the operational and strategic plan of the organisation.

Epilogue

A public body cannot stop providing a service to avoid risks as a measure to address them. This, however, makes it more imperative that the body be able to identify the risk - in this case of corruption and fraud, and manage it appropriately to mitigate the risk of putting the success of its objectives at risk.

The Council of Europe (CoE 2010) recommends that corruption risk assessments should not focus directly on corruption but on *"specific practices within an institution that jeopardise the ability of that institution to perform public service tasks in an impartial and accountable manner".* Such an approach includes illegal practices, such as bribery or embezzlement, but also practices such as those in which employees act in ways that serve their own interests rather than those of the institution they work for (unethical behaviour).

An appropriate policy for managing the risk of corruption and fraud requires, first of all, **the existence of an adequate internal Audit system**

(internal Audit system). Risk management is an integral part of an organisation's internal Audit system. It isa dynamic and an iterative process to identify and assess risks that could affect the achievement of objectives and to determine how to address them. Management is responsible for establishing and maintaining an effective system of internal Audit. In this context, an **adequate system of corruption and fraud risk management** is essential and should target:

Strong values and reliable management **practices of** an organisation, through the enforcement of clear rules, are the foundation of
on which a Corruption and Fraud Risk Management System should be based.

✓ **prevention/deterrence**, by designing checkpoints/Audit lines to reduce the risk of corruption and fraud and unethical behaviour,

✓ in **detection**, designing checkpoints to uncover incidents of corruption, fraud and unethical behaviour,

✓ in **addressing**, by designing checkpoints that will address the impact that corruption, fraud or unprofessionalism can have
behavior in the carrier, and even cure the effect of these.

The governance system and the risk management system of an entity must be aligned for best effectiveness.

It is necessary to establish a **specific and standardised process for risk management that is** dynamic and iterative, ensuring that risk is continuously assessed, taking into account changes in the internal and external environment of the organisation.

Annex I - Definitions

Risk Identification: the process of finding, identifying and describing the risk ***(second stage of the risk assessment process)***. Note that risk identification:

- consists of identifying the sources of risks and incidents, and identifying their causes and possible consequences.
- may require knowledge of historical data, theoretical analyses, expert opinions and may be based on the needs of stakeholders.

Risk Analysis: the process that takes place to clarify the nature and level of risk **(the third stage of the risk assessment process)**. The analysis forms the basis of both the assessment and the response to the risk.

Risk Tolerance: the percentage of risk that the organisation has decided to take in order to achieve its objectives, after any mitigation actions.

Impact: the result of an event. It is noted that:

- for an outcome to be considered an impact it must affect the objectives of the organisation.
- an impact can be certain or uncertain, as well as positive or negative.

Risk Treatment: the process of Auditing - modifying risk ***(the fifth stage of the risk management process)***. Risk treatment can create a new risk or modify an existing risk.

Risk Assessment: the overall process of (a) identification, (b) analysis and (c) assessment of risk.

Fraud: Any illegal act of fraud, concealment or abuse of trust. These acts do not depend on the use of the threat of force or physical force. Fraud is committed by individuals and entities to obtain money, assets or services, to avoid payment or loss of services, to secure individual or business interests.

Threat: A threat is defined as:

- the potential source of danger, harm or other undesirable effect.
- a negative situation in which a loss is considered likely to occur and in which a low level of Audit is maintained.

Moreover, a threat to one operator can be an opportunity for another.

Risk Evaluation: the process of comparing the outcome of the risk analysis with the risk criteria to clarify whether the risk is acceptable or tolerable, based on its magnitude or severity ***(the fourth stage of the risk assessment process)***. The risk assessment facilitates any response decisions.

Corruption: any form of unethical use or abuse of public power for personal or private gain. Corruption includes the exercise of influence and/or abuse of public power through the giving or receiving of incentives or illegal rewards for improper personal or private interests.

Risk Management: the ongoing process of identifying and evaluating internal and external risks that may adversely affect the achievement of the entity's objectives and implementing the necessary measures to maintain risk exposure at an acceptable level or to reduce the impact of potential risk to a level acceptable to the entity.

Audit: A measure that limits or modifies the risk. A Audit can include any procedure, policy, practice or other action that limits or modifies the risk.

Inherent Risk: The risk that exists before any measure is taken to mitigate it.

Review: an activity undertaken to determine the suitability, adequacy and effectiveness of an item.

Opportunity: an opportunity is defined as:

- the combination of situations that is expected to be favourable to the achievement of the entity's objectives.
- a positive situation in which a profit is considered probable and in which a fair level of Audit is maintained.

An opportunity for one institution can be a threat to another. Moreover, the exploitation or non-exploitation of an opportunity is considered both sources of risk.

Risk: The positive or negative effect of uncertainty on the achievement of the organisation's objectives. It should be noted that risk is characterised by the concepts of an event and its consequences, and is often referred to as the combination of the consequences of an event and the possibility of its occurrence. It also refers to the internal or external weaknesses of an entity that may provide an opportunity for an event to occur.

Corruption Risk: Any type of internal or external weakness or process that may provide an opportunity for corruption within the public body.

Risk Criteria: Reference data against which the significance of the risk is assessed. Note that risk criteria:

- are based on the objectives of the organisation, as well as its external and internal environment.
- may result from standards, laws, policies or other regulations.

Risk Register: a specific record of information on identified risks.

Likelihood: In risk management terminology, the term "probability" is used to refer to the likelihood of something happening. It is also distinguished from the term 'frequency', which describes the number of occurrences of an event in a given period of time.

Level of Risk: The magnitude or severity of risk as a result of the combination of impact and probability.

Risk Attitude: the approach of the operator to accepting, avoiding, reducing or passing on risk.

Risk Management Plan: a plan that defines the approach, specific management elements and resources to be allocated to manage risk.

Vulnerability: Intrinsic properties of an entity that result in its susceptibility to specificsources of risk and/or that may lead to the occurrence of an event with consequences.

Residual Risk: A risk that remains after mitigation methods have been implemented.

Annex II - Questionnaire

I. Vulnerable areas

1. Can you identify which areas or activities of your organisation are most vulnerable to breaches?
2. Has a risk analysis been carried out in your organisation to identify areas vulnerable to serious misconduct?

II. Organisational structure

3. What is the organisational structure of the body (e.g. ministry, directorates within the ministry)?
4. Does the institution have a vision/mission of its role? Does the staff know it?
5. Do the main units/directorates of the organisation have a "vision/mission"? Are the staff aware of them?
6. Does the institution have staff job descriptions and are staff aware of them?
7. Is there monitoring and/or statistics kept on the achievement of the organisation's objectives?

III. Financial management

8. What is the budget of the body?
9. What is the average expenditure on supplies of the organisation: Is there a significant number of very large procurements within the year (or in the previous year)?
10. What percentage of the body's procurement was carried out by open tendering?

IV. Human resources management

11. How many employees does the body employ?
12. How many of them are employed centrally (e.g. in a ministry) and how many decentralised?
13. What percentage of the body's staff have civil servant status, what percentage arewithin a two-year probationary period and what percentage are employed on fixed-term contracts?
14. Is there an internal recruitment process for the institution through its own advertisements, other than the Supreme Personnel Selection Board (ASEP)?
15. The Staff understands clearly which situations are conflictsof interest;
16. Are new staff subject to training at the operator?

17. If so, does the training cover integrity issues? Is this possibly repeated with more specific procedures at the stage of promotion or movement of staff to new positions within the organisation?
18. Do employees consider their training to be sufficient to manage the situations they face?
19. Who is designated as the person to whom the staff is referred for counselling?
20. To what extent do employees consider their salaries to be sufficient, marginally sufficient or insufficient to ensure a decent standard of living?
21. To what extent do employees feel that they are valued on the basis of their skills by (i) the organisation, (ii) their immediate supervisor? (scale 1 to 5)?

V. Procedures and decision-making

22. Are there standardised procedures and criteria for providing certificates or other documents, providing benefits or other economic benefits to citizens and/or collecting payments?
23. Where are these procedures and criteria described?
24. Where employees have discretion to make such decisions, are there clear instructions on how they should exercise that discretion (e.g. that it must serve a particular purpose)?
25. Are there specific deadlines for the completion of the above procedures?
26. If the body cannot take a decision due to lack of the required supporting documents (e.g. for a permit) within the deadline, is the citizen informed so that the procedure can proceed?
27. Are the body's procedures designed to minimise the number of contacts that citizens have to have with officials?
28. Are there alternative points from which citizens can be served (e.g. different branches of the same institution, post office, etc.)?

VI. Information systems

29. Are the information systems used by the institution effective in supporting the operation of critical processes?
30. Is there an access policy for information systems with user profiles, read, modify, delete, etc.?
31. Do the information systems interoperate with other public sector systems?
32. Do the information systems provide the possibility of extracting reports t o monitor processes?

33. Do the information systems contain the necessary checks to ensure that data are correctly recorded?
34. Are information systems capable of electronic document exchange?
35. Are the information systems adequately supported?

VII. Record keeping

36. Does the institution have clear rules for the management of its records?
37. Are the decisions of the body recorded and filed according to clear rules and within a specific time limit?
38. Who has access to the operator's records, who is authorized to manage them?

VIII. Access to documents

39. How many citizens' requests for access to documents were made last year?
40. How many of the above requests were rejected and how many were accepted?

IX. Transparency

41. Does the body have a communication policy to publicise its activities?
42. Are the following provided on the entity's online website?

a) organisational structure of the body and contact persons

b) body policies and policy documents

(c) laws and regulatory acts

(e) procedures for serving citizens and businesses

X. Ethics and integrity framework

43. Does the institution have its own Code of Conduct or Code of Ethics?
44. If there is a Code, are new staff informed of its existence when they take up their duties?
45. How often do staff receive ethics training?
46. Are there provisions, either in the Code, guidelines or other staff regulations or rules, informing staff of the actions to be taken in the event of a conflict of interest?
47. Which official has formal and specific responsibility for the development, implementation, monitoring and coordination of the anti-corruption policy within your organisation?
48. Is this responsibility stated in the job description of the employee in question?
49. Is there a Working Group within the institution in charge of formulating, coordinating, monitoring and reporting on the anti-corruption policy?

XI. Accountability mechanisms

50. Are procedures in place for employees to communicate on a regular basis with their supervisors (e.g. weekly unit meeting) to discuss issues related to the performance of their duties?
51. Is there an internal inspection service in the organisation?
52. How many audits did the Internal Audit Service carry out last year?
53. Is there an Internal Audit Unit in the organisation?
54. What were the most significant findings of the Internal Audit Unit in the past year?
55. Has the organisation been subject to an external audit in the last two years (e.g. by the Court of Auditors, the National Audit Office, the Ministry of Finance, etc.)?
56. What were the most significant findings of the external audit?

XII. Internal Complaints Mechanisms

57. Is there an internal complaints mechanism to which staff can report incidents of corruption or breaches of integrity?
58. Are agency staff aware of the internal complaints mechanism?
59. Has a provision been included in the complaints mechanism to protect employees who make complaints from retaliation?
60. How many complaints were lodged last year and what was the outcome?

XIII. Complaint mechanisms for citizens

61. Are there any complaints mechanisms to which citizens can submit complaints against acts of the institution or its employees?
62. Under the complaints mechanism, who examines complaints and to whom are the results of their investigation submitted?
63. How many complaints has the institution received in the previous year?
64. How many complaints were substantiated and upheld?

XIV. Disciplinary procedures and sanctions

65. How many disciplinary proceedings were carried out in the past year in your organisation?
66. How many of these proceedings concerned cases of corruption?
67. What is the result of these procedures?

Bibliography

1. ISO 31000:2018, Risk Management - Principles and Guidelines
2. ISO/IEC 31010, Risk management - Risk assessment techniques
3. COSO's Enterprise Risk Management Framework standard/methodology, 2013
4. International Professional Practices Framework (IPPF) https://global.theiia.org/translations/PublicDocuments/IPPF-Standards-2017-Greek.pdf
5. ELOT, Risk management and communication - Vocabulary
6. Presidency of the Republic of Colombia, Guide to Corruption Risk Management, 2015
7. United Nations Office on Drugs and Crime, State of Integrity, A guide on conducting corruption risk assessments in public organizations, 2020
8. U.S. Government Accountability Office, A framework for managing fraud risks in federal programs, 2015
9. Publication of the Regional Anti-Corruption Initiative: Corruption Risk Assessment in Public Institutions in South Eastern Europe: Comparative Study and Methodology. Available at: http://rai- see.org/focus/corruption-risk-assessment-in-publicinstitutions-in-south-east-europe- comparative-study-and-mMethodology/
10. INTOSAI, Audit of International Institutions, Guidance for Supreme Audit Institutions (SAIs), 2004
11. IPA Twinning Project, Support to Efficient Prevention and Fight against Corruption, Corruption Risk Management: Addendum to the Risk Management Guidelines, 2016
12. Chartered Institute of Management Accountants Report, Fraud Risk Management, A guide to good practice, 2012
13. Chartered Institute of Management Accountants, Fraud risk management, A guide to good practice, 2009
14. Office of the Auditor General of British Columbia, Guidelines for managing the risk of fraud in government, 2010

NTA
NATIONAL TRANSPARENCY AUTHORITY

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

ISBN 978-618-84622-3-6