SIGMA
Creating Change Together

A joint initiative of the OECD and the EU, principally financed by the EU

COVID-19 RISK ASSESSMENT

Guidelines

March 2021

2 Rue André Pascal
75775 Paris Cedex 16
France

mailto:sigmaweb@oecd.org
Tel: +33 (0) 1 45 24 82 00

www.sigmaweb.org

This document has been produced with the financial assistance of the European Union (EU). It should not be reported as representing the official views of the EU, the OECD or its member countries, or of partners participating in the SIGMA Programme. The opinions expressed and arguments employed are those of the authors.

Table of contents

1. INTRODUCTION

CONTEXT

The crisis caused by coronavirus (COVID-19) has revealed the vulnerabilities and deficiencies of the conception of management systems in all areas of society (political, health, social, economic, industrial, educational). The full impact of the pandemic, and its magnitude, is still unknown. However, the first consequences can already be recognised in the increasing debt of individuals and states, as well as the serious damage to business, the rising unemployment rate and the potential risk of poverty for a large part of the population.

Faced with this scenario, the European Union has planned an increase in public contracts and investments in the different Member States in order to alleviate the consequences of the crisis. These investments should be planned on the basis of a risk analysis that would contribute to making appropriate decisions, taking into account uncertainty, the possibility of future problems and effects on strategic objectives.

There are important differences in the extent to which public administrations throughout the world base their management on risk analysis. Few Member States of the European Union base their management on an adequate risk analysis system. In general, the public sector has considered this type of tool as typical of the business sector and those states that have initiated the implementation of a risk management system have done so in a purely testimonial manner, often limited to developing a risk register. The crisis, however, has highlighted the enormous importance of anticipating and managing any threat or risk that endangers the achievement of the objectives of any organisation, whether public or private.

In fact, over the last few years, several pandemics have put public management systems in difficulty (type A influenza, Ebola, avian flu, the Zika virus). The different national security strategies of the last three years have not been unaffected by these and warnings have accumulated. An adequate risk analysis would have considered the pandemic as a risk, with a very low probability of occurrence but with a catastrophic impact, both in the public and private spheres and, therefore, sufficiently important to carry out preventive actions. The notion of risk management as common to the private sector or as merely bureaucratic has meant that little or no preventive action was taken in relation to the current pandemic, so the impact of COVID-19 has been critical.

This crisis has highlighted the importance of implementing an effective risk management system and not merely a token one. It has also proved the need to develop such a system from the bottom up, taking into account the risks over which managers have control, and from top to bottom, assessing strategic risks that can have a huge impact on an organisation as a whole.

It is necessary then to establish a system for the management of the risks generated by the pandemic, working in parallel on the preparation of contingency plans to cover existing and additional risks that an organisation may face, and to be prepared for future similar events. On the other hand, and once the risk has materialised, it will be necessary to address and foresee more risks as a result of this materialisation. In addition to health risks, the economic support packages and the relaxation of financial controls required by the immediacy of the needs to be met will expose governments to greater risks of fraud, corruption and financial mismanagement.

OBJECTIVES

The COVID-19 crisis, due to its significant impact and its longevity, has revealed itself not as a short-term emergency but as a systemic crisis. The effects of this crisis, both on health and on the economy, will take a long time to disappear. Countries have reacted by adopting and implementing measures to combat the effects of the crisis, including immediate and urgent measures to respond promptly to the impact of the pandemic. However, it is also essential to carry out adequate planning in all areas, using as a reference the fulfillment of the organisational objectives and those factors that may put their achievement at risk. From this point of view, the four main objectives of these guidelines are as follows:

- Illustrate the importance of the implementation of a risk management system in the public sphere, emphasising that it is not a goal in itself, but a means to increase the chances of achieving objectives.
- Provide a basic manual for the implementation of a risk management system in any organisation or institution.
- Provide managers with a tool that helps them to assess the development of their internal control system and identify those areas in which improvements need to be made. This will facilitate the identification of risks in the internal control area.

- Identify risks in the key fields of public financial management: public procurement, internal control, internal audit and budgeting.

2. THE IMPORTANCE OF IMPLEMENTING A RISK MANAGEMENT SYSTEM

According to the International Standard ISO 31000 on Risk Management[1], a risk is *the effect of uncertainty on objectives* and an effect is *a positive or negative deviation from what is expected*. On the other hand, risk management consists of co-ordinated activities to direct and control an organisation with regard to risk.

Risk assessment and management is one of the components of the Committee of Sponsoring Organisations of the Treadway Commission (COSO) integrated internal control framework. Therefore, it is a key part of the internal control system of any organisation, which is defined as[2] "a *process effected by an entity's board of directors, management and other personnel designed to provide reasonable assurance of the achievement of objectives in the following categories: operational effectiveness and efficiency, financial reporting reliability, applicable laws and regulations compliance".*

Interest in the creation and implementation of an adequate internal control system based on risk management has been common for many years in the business sector, but it is relatively new for the public sector. The numerous cases of fraud and corruption, as well as the scarcity of resources and the increasing demand for transparency and efficiency from institutions, have caused concern in administrations about establishing systems to improve their public governance. The European Union has established[3] that the European Fund Management Authorities must implement effective and proportionate measures against fraud, taking into account the risks that have been detected.

An adequate internal control system and, therefore, an adequate risk management system, has innumerable advantages for any organisation, whether public or private, but in a context such as the current pandemic it becomes a crucial tool to be able to plan, allocate resources and anticipate potential threats appropriately. The numerous needs, the immediacy of the responses required by this emergency and the relaxation of controls in order to allow more agility of management, make it necessary to consider restructuring public internal control systems, starting with a risk analysis and assessment.

3. BASIC METHODOLOGY FOR THE IMPLEMENTATION OF A RISK MANAGEMENT SYSTEM

The objective of this section is to develop a risk management guide that may be used by any type of organisation as a reference for developing and implementing its own risk management system.

There are numerous manuals and methods that study risk assessment. This guide is primarily based on the five components of the COSO Internal Control Framework, which is currently the most widely accepted worldwide. However, it is also compatible with other internal control models or standards such as ISO 31000, CoCo in Canada or Cadbury in the United Kingdom.

According to this model, "*internal control is a process carried out by the Board of Directors, management and other staff of an entity, designed in order to provide a reasonable degree of security regarding the achievement of the objectives in terms of operations, reporting and compliance".* This process consists of five components:

- Control environment
- Risk assessment
- Control activities

[1] Issued by the International Organisation for Standardisation.

[2] Internal control – Integrated framework. COSO, 2013.

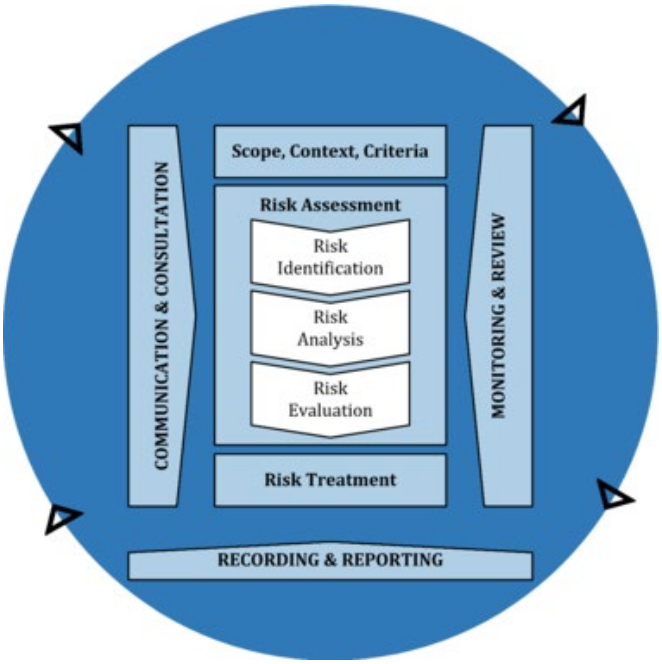
[3] Regulation (EU) No 1303/2013 of the European Parliament and of the Council of 17 December 2013 laying down common provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund, the European Agricultural Fund for Rural Development and the European Maritime and Fisheries Fund and laying down general provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund and the European Maritime and Fisheries Fund and repealing Council Regulation (EC), Article 125, paragraph 4, letter c.

- Information and communication
- Monitoring activities.

This manual focuses specifically on the second component; however, it is important to note that all five components must exist, function and interact with each other.

Before proceeding to study the risk analysis process, it is necessary to emphasise the importance of a demonstration of durable commitment from senior management to risk management through a statement that clearly expresses the objectives and the commitment of the organisation to risk management. This commitment should also be communicated appropriately within the organisation and to stakeholders.

The following figure shows the process that an organisation must follow to properly identify and manage its risks:



Source: ISO 31000.

OBJECTIVE IDENTIFICATION

An organisation has four types of objectives according to COSO:

- STRATEGIC: Related to the fulfillment of the entity's mission and vision.
- OPERATIONAL: Referring to the effectiveness and efficiency of the entity's operations, processes and resource allocation to achieve the strategic objectives.
- INFORMATION: Referring to the preparation of reports to be used by the organisation and other interested parties, taking into account the veracity, opportunity and transparency. These reports relate to financial and non-financial, internal and external information and also cover aspects of trust, opportunity, transparency and other concepts established by recognised bodies or entity policies.
- COMPLIANCE: Related to compliance with laws and regulations to which the entity is subject.

The strategic objectives should guide the organisation in achieving its mission and vision. The operational, information and compliance objectives are established using the strategic objectives as a basis, as are the specific targets for the different administrative units.

At this stage of the process, it is important to have a good understanding of the general functioning of the institution, as well as its strategic goals and objectives. To accomplish the above, it is recommended to review:

- All national and international regulations that affect the organisation, as well as all internal documentation, with the purpose of knowing the mission, vision, values and general guidelines of the institution.

- The organic structure of the institution, as well as its specific competences (such as an organisation manual, if any).
- The particular goals and objectives of each administrative unit in the organisation.

The organisation should identify its objectives properly and these should be achievable, clear, measurable and realistic. If the entity does not have defined objectives, this can be considered as a risk in itself, since it is impossible to measure the degree of their execution, or to define indicators for their improvement.

SETTING CONTEXT

According to ISO 31000, an organisation should analyse and understand its external and internal context when designing the framework of risk management.

The analysis of external factors should consider the institutional environment, from a social, economic, cultural, political, legal or technological point of view. The study of internal factors implies the understanding of the institution itself through the examination of its organisational structure, operational model, compliance with plans and programmes, information systems, documentation of processes and procedures and financial resources, among the most relevant.

To carry out this analysis, it is necessary to use tools such as interviews, questionnaires and brainstorming with public servants of different hierarchical levels, who are familiar with the performance of the organisation's processes. It is also important to conduct interviews with people outside the entity; develop flow charts to locate possible risks in processes; analyse different scenarios and periodically review economic, technological and regulatory factors, among others, that may affect how the institution operates.

Additionally, historical records of risks that materialised or were close to materialising, opinions of specialists and experts, evaluation reports from previous years and indicators generated in the institution should be considered.

IDENTIFYING RISKS

Once a thorough understanding of the entity is achieved and its objectives and processes have been understood, the process of identifying risks that may jeopardise these objectives can begin.

This process consists of determining the types of risk that exist and their influence on the institutional activities. Identification is one of the key activities within the risk management process, as without proper risk identification it is very difficult to achieve successful management. Thus, carrying out a risk inventory and analysing the causes of the events that generate them is key to understanding the sources of risk.

There are different categories of risk, including strategic, financial, operational, legal, technological, reputational or image.

There are different techniques in order to identify risks correctly, such as:

- Process mapping
- Self-assessment workshops
- Brainstorming
- Analysis of performance indicators
- Interviews and questionnaires
- Materialised risk records.

RISK ASSESSMENT: SEVERITY CALCULATION (PROBABILITY X IMPACT)

The assessment of the identified risks consists of calculating the severity of the risk, which is a magnitude expressed by the product of the probability that a risk will materialise, multiplied by the impact it would produce if it materialised:

RISK SEVERITY = PROBABILITY * IMPACT

The calculation can be carried out using qualitative or quantitative techniques:

- Qualitative: through the judgment of experts, who know precisely the activities, processes and environment in which the institution operates.
- Quantitative: determining the value of a risk using statistical models and calculating the expected loss due to its materialisation. Ideally, the institution has records of materialised risks for at least the last five years. If not, the calculation can be carried out through questionnaires, interviews, checklists, etc.

PROBABILITY

The probability of occurrence consists of calculating the possibilities that the risk materialises. Once the probability is measured, a value is assigned taking into account a scale such as the following:

Category	Value	Description
Very Likely	**5**	Risk probability is very high, that is, equal to or greater than 90% certainty that it occurs.
Likely	**4**	Risk probability is high, that is, there is between 66% to 89% certainty that it occurs.
Possible	**3**	Risk probability is medium, that is, there is between 31% to 65% certainty that it occurs.
Unlikely	**2**	Risk probability is low, that is, there is between 11% to 30% certainty that it occurs.
Very unlikely	**1**	Risk probability is very low, that is, there is between 1% and 10% certainty that it occurs.

Source: SIGMA.

IMPACT

The impact is evaluated by taking into account the consequences that risk materialisation can have on the institution. Calculating the impact quantitatively is very difficult, as it is necessary to have records of the value of the consequences of the materialisation of a risk for the organisation, not only financially, but also for the image or for the efficiency of the institution. Therefore, the impact is usually estimated qualitatively through expert judgment.

The impact is usually calculated according to the following categories:

Category	Value	Description
Catastrophic	**5**	Risk materialisation seriously influences the development of the process and the fulfillment of its objectives, ultimately preventing it from developing.
Major	**4**	Risk materialisation would significantly damage the development of the process and the fulfillment of its objectives, preventing it from developing normally.
Moderate	**3**	Risk materialisation would cause a deterioration in the development of the process by hindering or delaying the fulfillment of its objectives, preventing it from developing properly.
Minor	**2**	Risk that causes minor damage to the development of the process and does not majorly affect the fulfillment of its strategic objectives.
Insignificant	**1**	Risk that may have a small or no effect on the development of the process and does not affect the fulfillment of its strategic objectives

Source: SIGMA.

EVALUATION OF EXISTING CONTROLS

Once the risks have been identified and evaluated, it is necessary to review the control activities that already exist in the organisation to mitigate them. However, these controls not only have to exist, they also have to be well designed and effective.

Measurement of the effectiveness of controls can be done by taking into account their characteristics (design), their use and efficacy (effectiveness) or both. For a risk management system that is still under development, only the design of the controls can be evaluated by examining their characteristics, as historical data would be needed to measure the level of effectiveness.

The following is the basic valuation matrix of the controls associated with the identified and evaluated risks:

CHARACTERISTICS CONTROL DESIGN		CLASIFICATION	VALUE CONTROL DESIGN
PERIODICITY	OPORTUNITY		
PERMANENT	PREVENTIVE	OPTIMAL	5
PERMANENT	CORRECTIVE		
PERMANENT	DETECTIVE	WELL	4
PERIODICAL	PREVENTIVE		
PERIODICAL	CORRECTIVE	MODERATE	3
PERIODICAL	DETECTIVE		
OCCASIONAL	PREVENTIVE	POOR	2
OCCASIONAL	CORRECTIVE		
OCCASIONAL	DETECTIVE	VERY POOR	1
NOT DETERMINED	NOT DETERMINED	NON EXISTENT	-

Source: SIGMA.

LEVEL OF RISK EXPOSURE

The level of risk exposure is determined by the division between the severity value and the existing controls value:

$$\text{RISK EXPOSURE} = \frac{\text{RISK SEVERITY}}{\text{CONTROL VALUE}}$$

The values resulting from this formula will allow the classification of the risk according to the level of exposure, as can be seen in the following table:

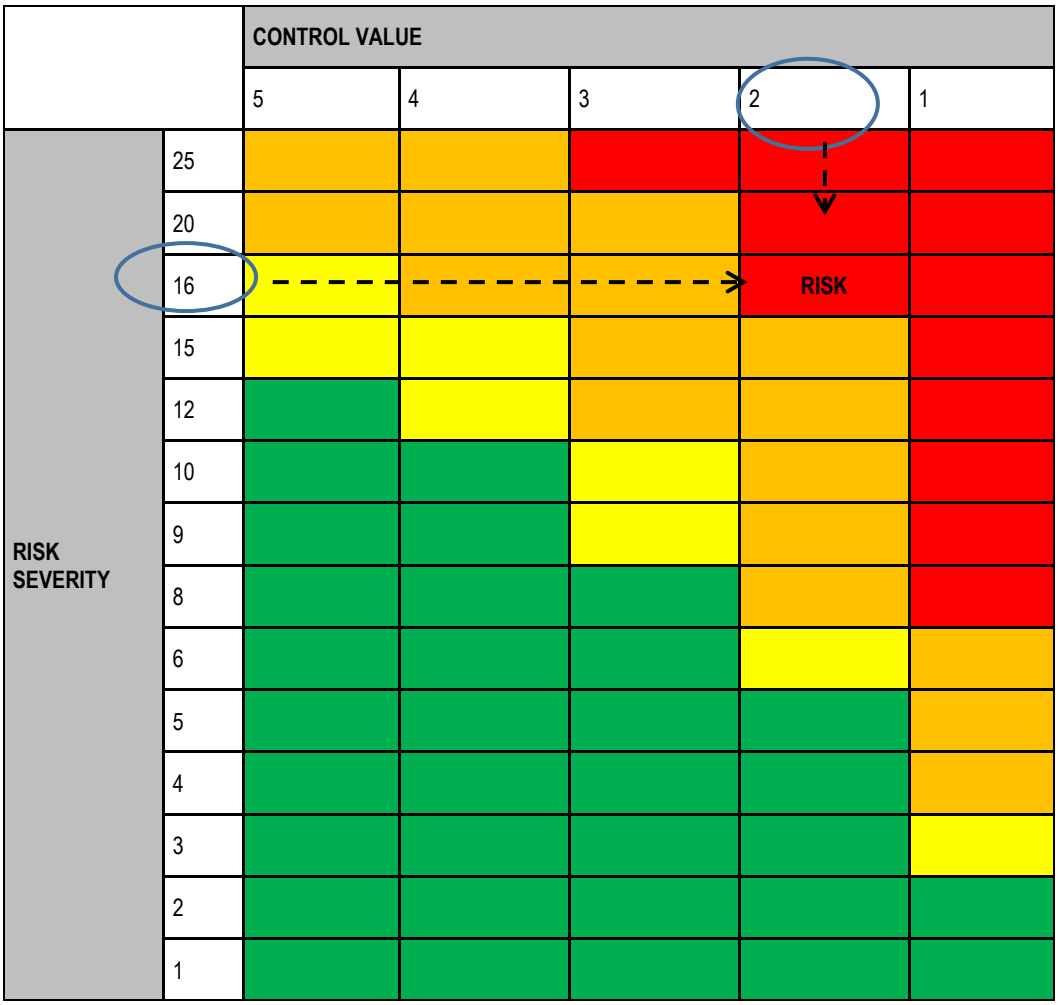
RISK EXPOSURE INDICATOR	VALUE	LEVEL OF EXPOSURE TO RISK
RISK SEVERITY / CONTROL VALUE	8.0 – 25.0	UNACCEPTABLE
	4.0 – 7.99	MAJOR
	3.0 – 3.99	MEDIUM
	0.2 - 2.99	MINOR

Source: SIGMA.

With these results, the organisation will be able to prioritise the risks to which it is exposed and select the most appropriate responses.

HEAT MAP

Another, visual, way of looking at the level of risk exposure is to develop a heat map. A heat map enables us to visualise which risks have the highest degree of frequency and impact. Decisions must then be taken on the responses to the risks located in the higher levels.



Source: SIGMA.

The risks in the red boxes are those with unacceptable levels of exposure and actions must be taken to mitigate them.

RISK RESPONSE

To respond to the assessed risks, the institution analyses and determines the actions to be taken in order to align the assessed risks with its strategy and objectives. There are different responses to the assessed risks that must be considered based, among other factors, on the ratio between the expected benefit and the cost of the action to be taken:

1. **Assume risk**: Once the impact the risk has on strategic objectives has been analysed, it is concluded that it cannot be reasonably mitigated, and it is decided not to take any action. This strategy should be used only for risks with low impact and low probability of occurrence.
2. **Monitor risk**: In this case, a periodic monitoring of the risk should be done to check if the probability of occurrence increases. In this case, those responsible for managing risks must act immediately by implementing actions to mitigate it. This type of strategy is applicable for risks with high impact and low probability of occurrence.

3. **Avoid risk**: This type of response refers to eliminating the factor or factors that are causing the risk; that is, if a part of the process is at high risk, the entire segment receives substantial changes for improvement, redesign or elimination.
4. **Transfer risk**: This response consists of transferring the risk to a third party. The third party must have experience of performing the work safely or under permanent risk. The responsibility will be of the third party and this party will assume the impacts or losses derived from its materialisation. The risk transfer strategy is currently one of the most used, for example, taking out insurance.
5. **Reduce risk**: This strategy applies when a risk has been identified and represents a threat to the fulfillment of the strategic objectives. The institution must establish actions aimed at reducing the probability of occurrence (prevention actions) and the impact (contingency actions), such as specific internal control measures and optimisation of procedures.
6. **Share risk**: This refers to distributing the risk and the possible consequences through partial transfers, in which the objective is not to be completely disengaged, but to segment the risk and distribute it to different administrative units or people, who will be responsible for one part of the risk.

The adoption of one of these strategies or the combination of several of them will result in a residual risk, which must be assumed responsibly by the heads of the administrative units in question.

However, the risk management process does not end there. Each risk must be monitored and controlled by its owner. Tt would also be beneficial to have a section in the organisation dedicated to internal control that carries out general monitoring of the entire system, including risk management.

4. IDENTIFICATION OF COVID RISKS IN KEY FIELDS OF FINANCIAL MANAGEMENT

As the general methodology to design an adequate risk management in an entity of any type and size has been defined, this section of the guide focuses on making an initial identification of risks in the most important areas of financial management: public procurement, budgeting, internal control and internal audit. It is not exhaustive and each body must analyse its needs, objectives and risks, which may or may not coincide with those related in this guide. It is not the objective of this guide to assess and prioritise specific risks, nor to identify their 'owner'. These categories will be different in each institution and, therefore, each one should carry out this work individually.

The COVID-19 crisis is the determining and cross-cutting factor that will condition the context for all the fields analysed. SIGMA has studied the consequences and risks that this crisis has implied. A cross-sectional study has been carried out regarding all the fields analysed (public procurement, budgeting, internal control and internal audit), selecting risks that have been repeated in different Member States and adding others that may occur.

PUBLIC PROCUREMENT

When grouping the risks, SIGMA started by identifying the objectives of the public procurement process, divided into COSO categories: strategic, operational, informational and compliance. Simple and very general objectives have been selected, since this list of risks is not addressed to any particular institution, but rather seeks to frame almost any public body. In this sense, the stated objectives are the following:

- **STRATEGIC OBJECTIVE:** Delivery of goods and provision of services necessary for the fulfillment of the functions of the public authority in a punctual, economic and efficient manner.
- **PERFORMANCE OBJECTIVE:** Resource optimization. Fast, agile and reliable acquisitions.
- **INFORMATION OBJECTIVE:** Transparency.
- **COMPLIANCE OBJECTIVE:** Comply with the current legislation.

SIGMA has identified some of the most recurrent risks that endanger the fulfillment of these objectives, particularly in the context of the coronavirus crisis. They are listed in ANNEX III.

INTERNAL CONTROL

Before identifying risks that affect the entity's internal control, it is necessary to make a first assessment of the internal control system itself. It is very common for organisations not to have an internal control system as such, but they do have control activities that can be evaluated. In this way, the very idea of internal control as a system and its importance is also transmitted to the entity.

Attached to this work is a basic tool for the evaluation of the internal control system of any entity (ANNEX I), based on the integrated COSO framework. Instructions for its use are developed in ANNEX II. The result will be the confidence level of the entity's system and of each COSO component, ranging from nonexistent to high.

Once the organisation's internal control system has been evaluated, it is easier to detect its risks. The list of risks identified by SIGMA in the COVID context is found in ANNEX III.

INTERNAL AUDIT

Although internal audit can be considered a part of internal control, it has been considered appropriate to analyse it separately due to its importance in the current context. Both internal control and internal audit itself must make a great effort to adapt to the current conditions in which the urgency of needs, teleworking and the use of IT tools pose challenges to carry out their objectives in an optimal way. Under these circumstances, a series of risks for internal audit in the COVID environment are identified in ANNEX III.

BUDGETING[4]

Based on the categorisation of objectives according to COSO, the following have been identified for the budgeting area:

- **STRATEGIC OBJECTIVE:** Adequate estimation of the financial resources and the expenditures in order to accomplish the strategic objectives of the organisation.
- **PERFORMANCE OBJECTIVE:** Optimisation of resources.
- **INFORMATION OBJECTIVE:** Offer complete and reliable information regarding income and expenditures.
- **COMPLIANCE OBJECTIVE:** Comply with the budgetary regulations.

In an environment such as the current one, budgetary activity is complicated by unforeseen expenses to meet the most urgent needs, which must be covered by increasing borrowing and/or by reducing other less urgent but necessary expenses. A list of risks can be found in ANNEX III.

[4] In this section, we do not attempt to address fiscal risk management in detail. Fiscal risks tends to describe large deviations from fiscal forecasts. Fiscal risk management is about monitoring, mitigating and managing these risks so that the public finances remain on a sound footing. The central budget authority normally manages them centrally, although each line ministry and agency must comply with the requirements and guidelines of sound budgetary practice. For more information on fiscal risk management, see OECD [GOV/PGC/SBO(2020)6] *Best Practices for Managing Fiscal Risks*
http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=GOV/PGC/SBO(2020)6&docLanguage=En

ANNEX I. INTERNAL CONTROL EVALUATION TOOL (EXTERNAL LINK)

The internal control evaluation tool (Annex I) is available online: www.sigmaweb.org/publications/COVID-risk-assessment-guidelines-Annex-1-internal-control-evaluation-tool-SIGMA-March-2021.xlsx.

ANNEX II. INSTRUCTIONS FOR USE OF THE INTERNAL CONTROL EVALUATION TOOL

The internal control evaluation tool is in Excel format. It is based on the integrated COSO framework and consists of seven tabs as described below:

1. TOTAL EVALUATION

This tab shows the final result of the evaluation. In it, the level of confidence of the entity's internal control system can be seen through a color code.

The tool also shows the system confidence level for each COSO component. In this way, the entity can quickly locate the component that requires immediate improvement actions.

2-6. COSO COMPONENTS EVALUATION

Tabs 2 to 6 correspond to each of the five components of internal control according to COSO: control environment, risk assessment, control activities, information and communication and monitoring activities.

Each tab includes a series of questions related to each of the components and criteria that make up the internal control system according to the COSO Framework, taken as a reference for the development of this work.

Each questionnaire should be completed as follows:

- Affirmative answer: The corresponding box is filled with the value 1.
- Negative answer: The corresponding box is filled with the value 0.
- Answer “in process”: The corresponding box is filled with the value 0.5.

At the end of each tab, the final result for each component can be seen once the questionnaire has been completed. Each answer should be accompanied by supporting evidence.

This tool can be used both by an organisation to assess itself and by the internal audit team, to have an initial approximation of the level of confidence of the internal control system. Therefore, two more columns are included (auditee comments and auditor comments) so that both the auditee and the auditor can add their comments.

7. VALUES

This tab shows the values necessary to interpret the results that the tool returns, according to the following table:

RANGE TABLE FOR THE EVALUATION OF THE INTERNAL CONTROL SYSTEM			
TOTAL	**BY COMPONENT**	**CONTROL CONFIDENCE LEVEL**	**MEANING**
HIGHER THAN 75%	HIGHER THAN 75%	**HIGH**	Reasonably defined and implemented internal control system. It is important to strengthen your self-assessment and continuous improvement.
HIGHER THAN 50% AND LESS THAN OR EQUAL TO 75%	HIGHER THAN 10% AND LESS THAN OR EQUAL TO 15%	**MEDIUM**	Internal control system with aspects that require better development and must be identified to be corrected.
HIGHER THAN 25% AND LESS THAN OR EQUAL TO 50%	HIGHER THAN 5% AND LESS THAN OR EQUAL TO 10%	**LOW**	Internal control system with serious limitations to correct. It requires the execution of an improvement plan.
LESS THAN OR EQUAL TO 25%	LESS THAN OR EQUAL TO 5%	**NON EXISTENT**	Internal control system non-existent or with serious deficiencies.

Source: SIGMA.

ANNEX III. RISK ASSESSMENT TOOL FOR PFM IN THE CONTEXT OF COVID-19 (EXTERNAL LINK)

The risk assessment tool for PFM in the context of COVID-19 (Annex III) is available online: www.sigmaweb.org/publications/COVID-risk-assessment-guidelines-Annex-3-public-financial-management-risk-assessment-tool-SIGMA-March-2021.xlsx.