INTOSAI

Risk management process
In Supreme Audit Institutions

Working Group
on Value and Benefits of SAIs

Risk management process
In the Supreme Audit Institutions

Introduction

According to ISSAI 12, "The Value and Benefits of Supreme Audit Institutions: making a difference in the lives of citizens", in order to perform its functions and ensure their potential value to citizens, SAIs needs to be seen as trustworthy.

This is only achieved if they are perceived as credible, competent, independent and accountable institutions that lead by example. Hence, it is necessary to implement an effective risk assessment process within SAIs, including integrity risks.

It is important to underline that risk self-assessment procedures contribute to reaching institutional goals and objectives.

Initial conditions to carry out a risk assessment process

- It is required to count on the support of the top management within the SAI to launch the process.
- Risk identification should be carried out by staff members with enough experience and occupying middle management positions, in order to ensure an effective detection of the threats and vulnerabilities in the institution.
- Risk identification can be done by conducting surveys and holding meetings with the selected staff.
- A report to the head of SAI should be prepared accordingly.
- As a complement of the process, it is advisable to undertake workshops with all the departments to enhance the risks detection mechanisms.

The workshops included the following steps:

Risk Management General Process

1. Identification of Strategic Goals and Institutional Processes

The strategic goals guide the achievement of the institutional mandate, mission and vision. From these strategic goals, the operational, information and compliance goals are established. Specific objectives for the different administrative units are thereafter defined, including internal regulations.

Once the processes performed by each unit are identified, it is necessary to match them with the strategic goals, objectives and actions set forth in the Strategic Plan.

2. Risk Identification

This step consists of determining the threats and vulnerabilities that may affect the activities carried out by each participating unit, and including the identification of internal and external factors that can trigger those risks.

The information gathered should be based on the experience and opinions of the participating staff.

3. Risk Classification

Since the tasks of SAIs have common features, it can be proposed to consider the risk self-assessment categorization, as follows:

- Strategic: Associated with matters relating to the mission and the achievement of strategic objectives.
- Financial: Related to the financial resources of the institution, especially the efficiency and transparency in the management of resources.
- Operating: This category considers the risks associated with failures in processes, systems or the structure of the institution.
- Legal: It affects the ability of the institution to comply with regulations and contractual obligations.
- Technology: Related to the ability of the institution's technological tools to support the achievement of strategic objectives.
- Integrity: Situations or events that, if they materialize, would affect the institution's ethical environment and principles.
- Reputation or image: Relating to events that, if materialized, could damage the way in which stakeholders perceive the institution.

4 and 5. Risk Evaluation and Prioritization

The risk evaluation consists of assessing the probability of occurrence and the impact of each risk. This evaluation is carried out using both, qualitative techniques (assessing the likelihood from the perspective of expert judgment), as well as quantitative techniques, using statistical models.

It is advisable to use a nominal scale rate (from 1 to 10) to evaluate risks, as well as an ordinal scale to establish the equivalent qualitative criteria (high, medium, low).

The probability of occurrence is evaluated based on the frequency; i.e. how many times the risk could occur; considering internal and external factors, while the impact was assessed by taking into account the consequences that may result for the institution if the risk materializes.

The following chart shows the scales used for risk assessment regarding impact and probability:

Assessment Scale – Risk Materialization Probability

Value	Category	Probability
10	Recurrent	Very high, there is full assurance that the risk will materialize, it tends to be between 90% and 100%.
9		
8	Very likely	High, the risk has 75% to 90% probability of materialization.
7		
6	Unlikely	Media, the risk has 51% to 74% probability of materialization.
5		
4	Unusual	Low, the risk has 25% to 50% probability of materialization.
3		
2	Rarely	Very low, the risk has 1% to 25% probability of materialization.
1		

Assessment Scale – Risk Impact in Case of Materialization

Value	Category	Impact
10	Catastrophic	Directly influences the attainment of the strategic goals, mission and vision of the institution; It may also involve monetary loss or damage to SAIs image, or interrupting for a significant period all or critical functions, resulting in institutional failure in providing services.
9		
8	Serious	Significant damage to the institutional monetary funds or to the image or affecting the achievement of some strategic objectives. A considerable period is also needed to restore correct operation or damage.
7		
6	Moderate	Causing a major loss to institutional funds or damage to its image.
5		
4	Low	Does not affect the attainment of strategic objectives, or may cause damage to property or image, which can be corrected quickly.
3		
2	Less	It may have very low effect on the institution.
1		

After developing the aforementioned two scales, it is necessary to prioritize risks, according to its final value and to determine which risks require immediate attention, by identifying the priority area in which each risk is located:

Risk Prioritization

Low risk 1 to 2.4	Tolerable risk area Determination is made regarding if the risks located here will be accepted, prevented or mitigated.
Moderate Risk 2.5 to 4.9	Moderate risk zone Determination is made regarding if the prevention and monitoring actions for risks located here will be shared or transferred to mitigate them properly.
High Risks 5 to 7.5	High risk area Determination is made regarding if the mitigation actions for risks located here will be shared or transferred to manage them properly.
Serious Risk 7.6 to 10	Significant risk area Steps are taken to mitigate risks located here, establishing a specific action plan to manage them.

The priority of the risks is concentrated in a General Risk Map, in which the risks are located to determine if their attention is needed immediately.

6. Evaluation of existing controls

Once the risks have been identified, evaluated and categorized, it is necessary to evaluate the existent controls to mitigate them and assess how effective is the operation and design of controls. It should be noted that the aim of the workshops is not to evaluate the effectiveness and adequacy of controls in place to respond to such threats. However, the technical opinions of the participants on the existence and operation of policies and procedures are contributions of high added value.

In order to address the deficiencies identified by participants, they themselves may suggest mitigation strategies, which are part of the response phase to the risks.

7. Risk response

After completing the stages of identification, evaluation, classification and prioritization of risks and evaluation of existing controls, public servants in each administrative unit may define, based on the priority of risk, the most appropriate response to address them according with the following determinations:

- Avoid risk: Eliminate the factors that are causing the risk. If a part of the process is at high risk, the entire process receives substantial changes for improvement, redesign or elimination, when applicable.

- Reduce the risk: The institution should establish actions to reduce the probability of occurrence (preventive actions) and the impact (contingency measures), such as specific measures for internal control and optimization procedures.

- Sharing: Transferring the risk to a third party who will assume the impacts or losses resulting from the materialization of risks present at the process with risks. It can also be understood as partial transfers, in which the goal is not be separated completely, but segmenting the process and channeling the segments to different administrative units or persons.

- Assuming the risk: Once the degree of impact the risk has on the strategic objectives is analyzed, a conclusion is made to establish no action or control and assume the consequences if the risk materializes, since mitigating it proves to be unreasonable due to its low impact and low probability of occurrence.

8. Reporting to the Head

After the identification, evaluation, assessment and prioritization of risks, a report on the workshops performed should be completed, in order to inform the head of the institution on the most relevant results. The report should include the following documents:

- **General Risk Inventory (GRI)**

  The list of all those events that the institution is exposed to and have been identified and categorized in the risk self-assessment workshops. In the inventory, each risk is traceable over time.

- **General Risk Map**

  Graphical representation of the value of each risk, according to their likelihood and impact, usually in the form of a heat map. The risks are represented so that the most significant ones (high impact and high probability) can be distinguished from the least significant.

- **Institutional Program for Risk Monitoring**

  Based on the risk matrix and the overall risk map, and in order to address areas of opportunity identified during the workshops, a Program of this kind can be developed and become a part of the activities to be carried out to address all risks, with a special emphasis on the top 15 risks. It should include administrative units responsible for implementation of controls, specific dates over a period of time for actions to be implemented, expected deliverables, and the expected effect on the institution's performance as a result of the action plans created to mitigate risks.

Risk management process
In the Supreme Audit Institutions