Appendix 4. Risk Management Methodology

Content

Glossary

Risk: incident that might happen and have an impact on the achievement of the objectives.

Cause: those actions, activities or situations that might give rise to the occurrence or materialization of one or several risks, they initiate the risk incident.

Control: action taken to prevent or mitigate the risk materialization.

- ✓ Prevent: to lower the likelihood of the risk materialization.
- ✓ Mitigate: to decrease the impact in case of risk materialization.

Likelihood: the chance of a risk happening or materialization.

Impact: effect or consequence of an incident.

Level of exposure: risk level that derives from the combination of likelihood and impact.

Introduction

Risk management is an iterative process that consists of several steps that, if executed in sequence, enables the continuous improvement of decision-making and it mainly ensures the achievement of the organization objectives.

GRAPH No. 3 RISK MANAGEMENT METHODOLOGY

1. Risk Identification

The following steps can be taken to identify the risks:

- Awareness of the **objective**, **scope** and **context** of the process or project under analysis using tools such as the following:
  - ✓ Interviews with the process or project owners and key personnel
  - ✓ Analysis of the evidence available for the process or project

  - ✓ Input-output review, KPI, technology that supports its execution and applicable regulations
  - ✓ Industry practices review and benchmarking.
  - ✓ Global and industry trends
- To identify the risks; i.e., relevant incidents that might have an impact on the achievement of the objectives
- To determine the origin of identified risks; i.e., their causes, failures or deficiencies
- To classify causes or failures that create the risk according to:
  - ✓ Internal incidents: situations that can be handled and managed by the organization, that is, are caused by internal factors such as the human resources available, processes being executed, technology or infrastructure used by the organization
  - ✓ External incidents: causes originated by external factors and are beyond the organization control, in terms of the cause and origin; for instance, social, political, regulatory, climate factors, inter alia.

2. Risk analysis and assessment

The purpose of this stage is to determine the level of exposure to the risk based on the occurrence likelihood and the impact it can have in case that it materializes. To do this, it is necessary to decide on the risk level through qualitative evaluations and quantitative evaluations, when required.

2.1. Identification of controls

To identify, for each risk, the controls or mitigation actions that are currently implemented specifying the following information:

- Name of the control
- Description of the control activity
- Frequency: how frequent is the control implemented
- Person responsible for implementing the control

2.2. Rating of the whole system of controls

It is carried out for each risk and it explains the way identified controls help to mitigate each risk and its causes. The following levels must be considered:

- Strong: controls apply to all the causes identified and their implementation is optimal (who, when and how are they implemented) based on the cost-benefit ratio
- Moderate: there are controls for every cause; however, they can be improved (who, when and how are they implemented).
- Weak: existing controls do not cover all causes
- Non-existent: there are no controls

2.3. Risk assessment

This stage involves the following activities:

- To assess the likelihood of risk occurrence considering the rating criteria outlined in Appendix 2 Criteria for measuring the likelihood of occurrence.

- ✓ Recurring / transaction activities: operations with a high volume of transactions that are carried out at least once a day
- ✓ Sporadic activities: operations that do not take place every day

- To assess the impact of the risk based on the rating criteria outlined in Appendix 3 Criteria for measuring the impact
  The impact of a risk incident can affect different business objectives and must be classified based on the following aspects:
  - ✓ Economic: it is a financial impact and it becomes materialized in the company as lower income, higher costs or expenses or loss in asset value, inter alia.
  - ✓ Reputational: impact that affects the organization's good standing before the stakeholders (shareholders, collaborators, suppliers, media, community, government and authorities).
  - ✓ OH&S: impact that causes employees or third parties' injuries, disabilities or death.
  - ✓ Information: the risk materialization causes the loss of the company information

  The risk may be assessed through any of the aspects related to these criteria and, the impact with the highest value should be selected and recorded if there are several potential effects.

The outcome of the risk analysis and assessment may be seen in the Risk Map, which illustrates the level of risk exposure.

Level of exposure = likelihood x impact

Likelihood						
	5 Very high	5	10	20	40	80
	4 High	4	8	16	32	64
	3 Moderate	3	6	12	24	48
	2 Low	2	4	8	16	32
	1 Very low	1	2	4	8	16
Low Moderate High Critical		1 Lower	2 Low	4 Important	8 Higher	16 Significant
		Impact				

The risk map is divided into four risk zones: low, moderate, high and critical.

- Low risks: acceptable risks since they are found within the level of risk taken by the organization and should be subject to permanent monitoring by the party responsible for the risk. It does not require additional control actions.
- Moderate risks: they are tolerable risks and additional actions could be implemented to take these risks to the green zone.
- High and critical risks: they are found outside the organization tolerance and control actions should be implemented and permanent monitoring needs to be ensured.

Note: Odinsa uses its risk assessment methodology in state contract projects set out by the Colombian Treasury Department or any other applicable body in other countries.

3. Risk treatment

After having considered the risk exposure, it is necessary to draw action plans to handle the risks at the critical, high or moderate level. In these cases, the mitigation options are assessed compared to the cost-benefit criteria and expected mitigation.

Below are the different treatment options that can be selected according to the type and level of exposure to the risk:

- To avoid the risk: stop the activity that might be causing the risk.
- To mitigate the risk:
  - ✓ Lower the likelihood: it aims at decreasing the probability of the risk occurrence, implementing additional activities or controls.
  - ✓ Lower the impact: it seeks to decrease the effects in case that a risk incident occurs, as with the execution of business continuity plans.
- To transfer the risk: it seeks to lower the risk exposure involving a third party to support and share the risk. Mechanisms include the use of contracts, insurance policies, financial coverage and organizational structures such as partnerships and joint ventures.
- To keep the risk: there might be residual risks that need to be kept or accepted at the level they are found, since it is more expensive to implement additional actions apart from risk monitoring.

Choosing the most adequate option involves the balance of the implementation cost of each option as compared to their benefits.

The following information should be explained to draw the action plan:

- Name and description of the action plan and activities that need to be conducted.
- Employee responsible for the tasks described in the action plan.
- Employee responsible for the review: is the one that determines if the action plan was implemented satisfactorily and if it complied with the objective for which it was created.
- Follow-up date to confirm progress and end date.

4. Monitoring

The risk properties change over time and there is a need for monitoring and reporting mechanisms to achieve a successful risk management. The following are among the most relevant monitoring and reporting activities:

4.1 Monitoring action plans

Progress and proper implementation of the action plans should be followed based on a schedule. Documentary evidence of this monitoring must be included in the activity risk matrix and, once these plans are implemented, it is required to assess the risks to confirm that there has been a decrease in the risk exposure as a result of the actions implemented.

4.2 Monitoring the risk profile

A risk assessment review should be carried out on an ongoing basis to confirm that is still in effect and it must be particularly conducted:

- ✓ When there are changes in the processes or projects, changes in the risk exposure or once a year if it is a critical process.
- ✓ At the implementation of the action plans established to mitigate the risks.
- ✓ At the materialization of a risk incident, in which case it is required to outline and implement action plans immediately.

4.3 Reporting mechanisms

The aim of reporting is to consolidate the risk management information relevant to the different stakeholders inside the organization. Regular and timely reports of risk warnings become essential to comply with the CRMS objective of anticipating the materialization of risks.

The risk reporting matrix determines the levels of responsibility to report and monitor risks associated with the operation. This matrix was approved by the Steering Committee. See Appendix 5. Risk reporting matrix of each company.