

Corporate Policy

Grupo **Dia** 

Risk Management Policy

OBJECT

The purpose of this document is to define the DIA Enterprise Risk Management Policy and include the key principles as a basis for its adequate performance. On the other hand, it is briefly explained the taken methodology in order to achieve an effective Risk Management that helps to the attainment of business objectives set by the Management.

SCOPE

The Corporate Risk Management is a process that must be developed by the Board of Directors and be supervised by the Audit Committee. However, the correct implementation of a Risk Management and Control System requires the involvement of all Organization staff.

The Enterprise Risk Management Policy is applicable to all companies and territories where DIA operates.

The Management decisions in all of its activities have an influence in the creation of value, from the establishment of the strategy to the Company daily operations. The last one is maximised when strategy and objectives are established with an optimal balance between growth and profitability targets and the associated Risks.

In the implementation of the Corporate Risk Management System, DIA should consider all their activities at the different organizational levels, from those at Group level to the business units and processes. The System should be applicable at the following levels:



The entire Organization plays an important role in the objectives achievement related to the Risk Management System. The approach of Risk Management Model is therefore comprehensive, systematic and is applicable to all companies and territories where DIA operates.

METHODOLOGY APPROACH

A Risk Management Integrated Model improves the Organization's ability to manage uncertainty scenarios. It is a systematic and detailed approach that allows the Organization to identify events, assess, prioritize and respond to Risks associated with its main objectives, projects and operations.

The DIA Risk Management process is based on the methodological standard COSO II, Risk Management methodology generally accepted and adapted to DIA needs. This methodology allows DIA to identify, create, capture and sustain the value of Risk Management at the different levels of the Organization.

The methodology establishes three dimensions for analysis:

- / Organization **OBJECTIVES**.
- / **LEVELS OF THE ORGANIZATION** where the Risks may materialize and therefore need to be included in the Risk Management Model.
- / Risk Management **COMPONENTS** that allow the mitigation of Risks that affect the business objectives achievements.

COSO II

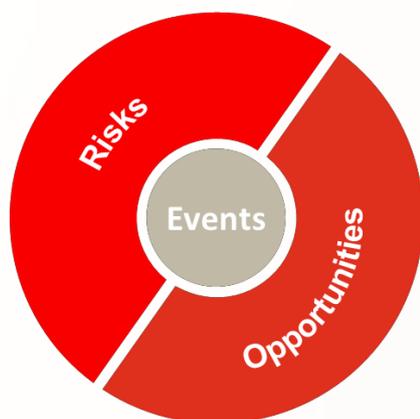


The components in the Management process of the Organization are:

1. **Internal environment:** Management establishes the Risk Management philosophy, determining the level of risk accepted.
2. **Setting objectives:** it is necessary to know the objectives of the Company in order to identify potential events that may affect their achievement.
3. **Event identification:** it must be identified potential events that may impact DIA. In this sense, it will be considered events, from internal and external sources, that may affect the achievement of the objectives, distinguishing between those that mean a Risk and those which represent an Opportunity.
4. **Risk assessment:** Risks are analysed by assessing their probability and potential impact on objectives achievement.
5. **Risks responses:** identify and evaluate possible responses to Risk: avoid, accept, reduce or share.
6. **Control activities:** based on Risk responses, establishing policies and procedures to ensure that they are carried out.
7. **Information and communication:** information obtained from the analysis must be communicated to the implementation responsible.

8. **Supervision:** Risk Management is supervised, so that they can be adapted in case of change of circumstances.

Definitions.



Event: Incident or occurrence derived from sources within or outside the Organization, which could affect the implementation of the strategy, or the achievement of business objectives.

Risk: Any situation or event, which may jeopardize the achievement of an objective.

Opportunity: Possibility that an event will occur and positively affect the achievement of business objectives.

CONCEPT OF RISK

DIA defines Risk as any contingency, internal or external that in case of materialisation would prevent or difficult the achievement of the objectives set by the Organization.

The DIA Risk Management identifies the different types of risk, financial and non-financial (including operational, technological, social, environmental, political and reputational) facing the Organization, including among the financial or economic risks, fiscal risks, contingent liabilities and other risks present off the balance sheet risks.

Depending on their nature can be classified into Inherent and Residual:

/ **Inherent Risks:** Risks related to the nature of business and the Company whose valuation does not take into account existing Organization Controls to mitigate them.

/ **Residual Risks:** Risks related to the nature of business and the Company that, remain after the existence Organization Controls to mitigate them.

Each Risk is assessed in terms of probability and impact. DIA considers that a Risk arises as lost Opportunities and / or strengths as well as a materialized threat and / or enhancement of a weakness.

Key principles

The five key principles of DIA Risk Management are:

1. In order to achieve the strategic goals, Risks must be managed throughout the all Organization with no exceptions. It is necessary all Organization involvement in the Risk Management System.
2. The Risk Management includes identification, assessment, response, follow up or monitoring and reporting according to the established procedures.
3. DIA Risk Management should ensure the existence of adequate measures to mitigate the impact of the identified risks, in the event of materialization. The Risk responses should be consistent and be widely adapted to the circumstances of the business and economic environment.
4. The Executive Committee (COMEX) will, among other things, evaluate annually the assessment of the main DIA Risks, including the fiscal risks, and review the Risk Tolerance level established.
5. Periodically, a monitoring and reporting will be done considering the identification activities, assessment, responses, follow up or monitoring and reporting according to DIA Risk Management Model.

The DIA Risk Management ensures the existence of adequate internal control systems to manage and control the aforesaid risks, including contingent liabilities and off balance sheet risks.

RESPONSIBILITIES

The Board of Directors, Audit Committee and DIA Management are responsible for the proper functioning of the Risk Management Model.

The **Board of Directors** is responsible for approving and setting the Enterprise Risk Management Policy. Management is responsible of its implementation, and for establishing the strategy, culture, people, processes and technology that make up the Risk Management Model.

The Executive Committee (COMEX) is responsible to set the level of risk that the organisation considered acceptable (risk appetite), to be approved by the Board of Directors ultimately.

The **Audit Committee** is responsible for monitoring and periodically reviewing the effectiveness of DIA Internal Control procedures, Internal Audit and Risk Management Systems, verifying the adequacy and completeness of them.

DIA has established a **Risk Committee** at Corporate level, and has designated a **Corporate Risk Coordinator** responsible for communication and coordination of

meetings and the collection of information and reporting of it. The Coordinator also acts as interlocutor with the countries in the field of Risk Management.

Each country must establish its own Risk Committee.

Each **Area Director** is responsible for managing (in his/her area) the Risks appropriately. In the case of a Risk occurrence (at one of the areas), the Area Director will be responsible for managing and implementing adequately the necessary mechanisms in order to minimize the impact as much as possible.

The **Risk Committee** will evaluate later, whether the response after the occurrence of Risk was correct or not, and whether it has been detected the necessity of implementing new Controls or response mechanisms.

Risk Committee

The Risk Committee is composed by the Risk Coordinator (at the quarterly meetings of the Corporate Risk Committee, the Corporate Risk Coordinator will act on behalf of Country Risk Coordinators, reporting to the Corporate Risk Committee the information received from them on Risk Management) and a responsible for each of the functional lines (Area Directors):

- / Franchise
- / Expansion
- / Master Franchises
- / Organization and Systems
- / Human Resources
- / Legal
- / Finance
- / Fiscal
- / Sales
- / Supply Chain
- / Quality Control
- / Technical Direction and Central Supply
- / Trade & Merchandise
- / Internal Audit
- / External Relations
- / Security
- / Strategic projects

In its task of Risk Management, the Risk Committee will held quarterly meetings and maintain, apart from the additional duties assigned by DIA, the following basic responsibilities:

- / Analysis of the environment and new projects that may directly or indirectly influence the Risks of DIA. Consideration of the inclusion of new Risks and / or disappearance of any of the existing ones.
- / Action plans recommendation, monitoring and continuity of existing Action Plans.

Additionally to the quarterly meetings, annually, the Risk Committee should conduct an assessment and detailed Key Risk Map analysis.

The findings and information from the analysis of the Risk Management Model must be reported to the Management regularly. Additionally, the Risk Committee shall inform to the Management, if relevant topics are detected in its analysis. Finally, Management may request the results report of the Risk Committee.

Supervision of key principles and Enterprise Risk Management Policy

The Audit Committee and Internal Audit, taking into account their responsibilities and independence, are the competent supervisors of Risk Management Control System.

Internal Audit will supervise the Control System and Risk Management. This supervision task involves the review of the entire process, including the performance of the Enterprise Risk Management Function and the effectiveness of Control activities. The results of this supervision will be reported to the Audit Committee.

Risk Appetite, Risk Tolerance

The DIA approach is based on three basic elements and its proper alignment with the Enterprise Risk Management process.

- / Business Objectives: Strategic & Operating goals of DIA.
- / Risks: Any situation or event, which may jeopardise the achievement of an objective.
- / Controls: Management actions and responses put in place for the Risks.
- / Proper alignment between Business objectives, Risks and Controls based on the level of Risk Tolerance and Risk Appetite of DIA.

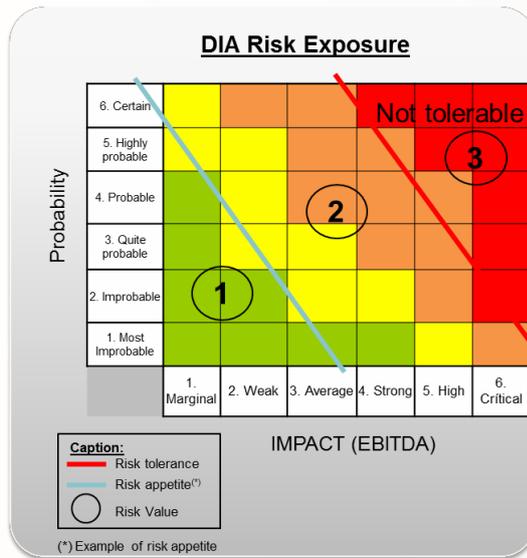
Risk Appetite is defined as the desired level of risk that DIA takes to achieve its objectives. It is considered in the strategy that has been defined by the Executive Committee and validated by the Board of Directors.

Risk Tolerance is defined as the acceptable level of variations is willing to accept regarding the pursuit of its objectives. It is the specific maximum risk that the Organization is willing to take. It is Management's responsibility to define the risk tolerance.

The risk appetite and the risk tolerance are annually reviewed and presented to the Board for approval.

Once the risk appetite and the risk tolerance are defined, these should be compared with the risk value. There are three different possible situations:

Example:



SITUATION 1:
Risk Value < Risk Appetite < Risk Tolerance
 The risk value is within the desirable and acceptable risk levels of the company.

Action Plans:
 Keep the present situation considering the possibility of taking more risk.

SITUATION 2:
Risk Appetite < Risk Value < Risk Tolerance
 The risk value is out of the desirable risk levels but within the acceptable risk levels of the company.

Action Plans:
 Take measures to mitigate risk adjusting it to the Organization risk appetite, otherwise approve to maintain the risk value out of the risk appetite in order to achieve the business objective.

SITUATION 3:
Risk Appetite < Risk Tolerance < Risk Value
 The risk value is out of the desirable and acceptable risk levels of the company.

Action Plans:
 Management must analyze the situation and the necessary action plans to reduce the risk value at least within the acceptable risk levels.

Regarding the risk appetite, the Board of Directors must continuously have sufficient information of the entire Organization for a proper decision-making.