DOMINION

CONTROL AND RISK MANAGEMENT POLICY

CONTENTS

1. PURPOSE

The purpose of this document is to define the Control and Risk Management policy of Global Dominion Access, S.A., in order to establish the general framework in which to act and the procedures and responsibilities required to control and manage the risks confronted by Dominion efficiently and effectively.

Dominion uses its risk management system (hereinafter, the "RMS") to reasonably ensure that all material strategic, operational, financial (see the Internal Control over Financial Reporting (ICFR)) and compliance risks are anticipated, identified, assessed, monitored on an ongoing basis and lowered to the risk appetite and tolerance levels approved by the Board of Directors.

Senior Management and the Management Team are strongly committed to managing risks and have implemented a rigorous strategic programme in order to establish an environment in which it is possible to operate with the existence of controlled risks by actively managing them and taking advantage of new opportunities.

The principles the policy is based on are essentially as follows:

- Strengthen a constructive view of the concept of risk.
- Commitment and capabilities of the individuals involved.
- Use of plain language.
- Transparent communication throughout the organisation.

Dominion personnel with RMS responsibilities shall be equipped with the material and human resources required to perform their duties.

2. SCOPE OF APPLICATION

This policy applies to DOMINION's RMS with respect to all its centres and investees and the areas in which it operates and covers all financial reporting risks that may impact on Dominion, irrespective of whether such risk is the result of its environment or activities. To this end, the RMS covers the risks that threaten strategic, operational, financial, non-financial and compliance objectives.

3. RESPONSIBILITIES

The different functions involved in the RMS can be grouped into three lines of defence against the risks that threaten compliance with strategic, operational, financial, non-financial and compliance objectives. The first line of defence reports directly to Senior Management and the Management Team, while the second and third lines of defence report to the Compliance department.

As shown in the attached diagram, the three lines of defence within the RMS all fall under the supervision of the Board of Directors:

BOARD OF DIRECTORS	
CORPORATE SOCIAL RESPONSIBILITY COMMITTEE	AUDIT AND COMPLIANCE COMMITTEE
COMPLIANCE DEPARTMENT	

1ST LINE OF DEFENCE	2nd LINE OF DEFENCE			3rd LINE OF DEFENCE
Operational management	Risk Management	Internal Control (ICFR, IT, operational, etc.)	Compliance (regulations and policies)	Internal Audit

The Operational Management Unit must assess, control and mitigate risks and implement effective internal controls.	Internal control, risk management and compliance functions facilitate and supervise the Operational Management Unit's implementation of effective internal control and risk management effective practices.	The function of the Internal Audit Unit is to prove the effectiveness of internal control and risk management mechanisms to government agencies, including how the 1st and 2nd line defences work.

In this context, the roles and responsibilities of each member of the organisation involved in the RMS are as follows:

Body	Functions/Responsibilities
Board of Directors	✓ Most senior group accountable to shareholders with respect to the existence and performance of the RMS. ✓ Monitors the RMS through the activities performed by the Audit and Compliance Committee.
Audit and Compliance Committee	✓ Assessment and supervision of Dominion's RMS. ✓ Report to the Board of Directors with respect to the results of the assessments performed and schedule assigned to the measures proposed to combat detected weaknesses.
Senior Management and Management Team	✓ Responsible for identifying and assessing risk. ✓ Establish and convey a risk-focused culture within the company. ✓ Define, establish and/or modify risk appetite. ✓ Approve the plans, programmes and actions proposed by the Compliance department that may be considered necessary to address identified risks.
Compliance Department	✓ Define Dominion's methodology, procedures and criteria with respect to identifying, measuring, classifying, approving and responding to risks. ✓ Regularly report to the Audit and Compliance Committee with respect to the progression of risk and the general performance of the RMS. ✓ Responsible for designing and implementing the RMS. ✓ Coordinate and assess strategic, operational, financial and compliance risks to be included in the Risk Map.
Internal Audit Team	✓ Assess the effectiveness of the RMS and issue regular information on detected weaknesses and the schedule assigned to the correction methods proposed.

Other employees	✓ Responsible for identifying risks threatening objectives and communicating them to the area manager. ✓ Collaborate with area managers to measure and classify risks, propose action plans to address the risks identified and collaborate in the performance thereof.

Chart showing the assignment of RMS functions:

	Board of Directors	Audit and Compliance Committee	Senior Management and Management Team	Compliance Department	Internal Audit Team	Other employees
Establishing context	X					
Identifying risks		X	X	X		X
Risk analysis				X		
Risk assessment		X	X			
Addressing risks			X	X		
Monitoring and reviewing risks				X		
Monitoring risks				X	X	
Updates				X		
Non-performance actions					X	X

4. DESCRIPTION OF THE PROCESS

The RMS is based on ISO 31000 (international risk management standard) methodology and adapted to Dominion's requirements. It comprises the following main components:

4.1. Communication

Effective external and internal communication and enquiries in order to ensure that those responsible for implementing the RMS and the group's stakeholders understand how decisions have been made and the reasons why certain actions are deemed necessary.

To this end, Dominion submits an official report to Senior Management and the Management Team in order that they may update the Risk Map.

4.2. Establishing context

Dominion analyses external and internal parameters to ensure the full context is understood.

understand the **external context** (through collaboration with the Communication and Marketing department) to ensure that the objectives and concerns of the company's external stakeholders are taken into account when risk criteria are established. The external context may include, but is not restricted to:

a) The social, cultural, political, financial/legal, technological, economic, natural and competition environment at international, national, regional and local level.
b) The factors and trends that impact on the organisation's objectives.
c) Relations with and the opinions and values of the company's external stakeholders.

The **internal context** refers to any area within the organisation that may impact on operations and cause it to have to manage risk. The risk management process must be consistent with the culture, processes, structure and strategy of the organisation.

4.3. Identifying risks

Any risks that may impact on business objectives must be identified using existing business objectives, which are primarily obtained from the Strategic Plan and Budget.

The process used to identify risks involves looking for events (associated with internal or external factors) that may give rise to risks or opportunities, thus identifying the business objectives that may be affected.

Once the Risk List has been created, it shall be reviewed on a regular basis to align identified risks with business objectives.

Risk categories are as follows:

- **Strategic:** those that impact on high-ranking objectives that are directly related to the Strategic Plan.
- **Operational:** those that impact on objectives associated with the effective and efficient use of resources.
- **Financial:** those that impact on financial objectives.
- **Compliance:** those that impact on objectives relating to compliance with applicable laws and regulations.

4.4. Risk analysis

Risk analysis provides data that can be used to assess risk and make decisions about whether or not it is necessary to address the risks at issue. It also indicates the best risk strategies and methods to use.

In order to define uniform criteria to measure risks prior to their identification and thereafter prioritise them in a consistent manner, a scale has been designed to measure each risk variable: probability of occurrence and impact. These scales can be used to locate each risk on the Risk Map, which is the main tool employed to assess risks.

In addition to defining scales to measure each risk, the following areas will be defined:

a) Finding the origin of the risk.
b) Identifying areas impacted by risk.
c) Identifying the individuals responsible for managing risks.
d) Identifying the risks associated with the entity's activity, that is, defining how risks would impact on the company, were they to occur.

4.5. Risk assessment

In Dominion's RMS, the procedure used to assess risks is performed by Senior Management and the Management Team, who must assess the risks identified. The Compliance department will instruct the above individuals to complete assessments within the established timeframe.

Once assessments have been obtained from each of the above individuals, they will be consolidated in order to design the corresponding risk maps. Risk consolidation takes into account the specific weight of each of the assessments performed and the geographical area for each type of risk in order to obtain a global perspective of the matter at hand and prioritise risks accordingly.

4.6. Addressing risks

Once risks have been identified, assessed and consolidated, responses must be prepared so as to reach an acceptable level of risk for the organisation at a reasonable cost. Thus, based on the risks and controls identified, action plans must be determined in order to reach the risk level accepted by the organisation.

Management of these risks can be classified into four categories, as per the following Probability/Impact binomial:

a) **Avoid:** performance of actions designed to avoid events that present a risk.
b) **Mitigate:** reduce the probability of occurrence, potential impact or both.
c) **Accept:** decide to accept the probability level and impact of the identified risk. This decision must be communicated and supported.
d) **Share:** identify actions intended to reduce or partially combat the detected risk.

The Compliance department is responsible for analysing risks and designing responses, which it must submit to the Audit and Compliance Committee. This process involves a control system comprising two types of parameters:

a) **Lowering impact:** Measures used to reduce risk consequences.
b) **Reducing probability:** Measures used to reduce the probability of the risk occurring or increase the probability of detecting it before it occurs.

4.7. Monitoring and reviewing risks

In order to ensure that risk responses are viable and efficient, a monitoring process is performed on an annual basis to obtain the following objectives:

- ✓ Ensure risks continue to be managed as provided for by Senior Management.
- ✓ Assess the efficiency of responses. Provide feedback to those responsible for said responses and implement action plans where necessary.
- ✓ Determine whether or not the Risk List anticipates and reflects changes in business circumstances and new economic conditions.

In order to carry out this monitoring procedure, the Compliance department includes priority action plans in its annual review programme to monitor whether or not the controls used to lower impact and reduce probability are being implemented as provided for and that they are effectively mitigating the risks they are intended to combat. The individuals responsible for each individual risk within the corresponding business areas are also in charge of monitoring said risks.

In addition, the Compliance department must check whether or not a risk has occurred and, where applicable, indicate what measures need to be adopted in order to mitigate it.

To facilitate monitoring activities, the following two reporting levels are used:

a) **Internal reporting:** two-way reporting from Senior Management and the different business units to the Compliance department and vice versa. The Risk Map is used for this purpose. As a minimum requirement, it includes the list of Dominion's risks and graphs indicating the main risks by geographical area and type of risk, including a breakdown of the same, the high-ranking controls implemented to combat the top 15 risks and the action plans agreed to mitigate them.

   The Compliance department will coordinate annually with Senior Management and the Management Team to update the Risk Map.

b) **External reporting:** this mainly comprises information about the risk management actions to be included in the Dominion Corporate Governance Annual Report, which is prepared by the Compliance department and the section included in the Non Financial Information Report, which indicates the main risks affecting DOMINION and the agreed actions to be taken in respect of the main risks identified.

The monitoring and reviews performed by the Board of Directors and Senior Management with respect to the impacts, risks and opportunities of economic, social and environmental issues complies with the GRI G4-47 index.

4.8. Updates

Business risks change over time and, as such, generate changes in the RMS. To this end, risks that were previously critical may become less important, while others become more critical.

The Compliance department applies a model to update the RMS on an annual basis in order to ensure it remains effective and is kept up to date.

The procedure followed to update the system is described below:

1. Communicate the start of the procedure.
2. Obtain the following information:

- Senior Management and Management Team: check the current risk situation and compare it to the risk management system in operation. In order to do this, the individuals responsible for the risks at hand will be interviewed.
- Analysis of Dominion Strategic Plan.
- Meetings with the Audit and Compliance Committee.

3. Update and identify risks.
4. Prepare a Risk Map proposal for subsequent validation by the Audit and Compliance Committee and approval of the Board of Directors.
5. Update the Risk Map and system documents.
6. Communicate the new Risk Map and, where necessary, indicate how it should be used.

4.9. Non-compliance

Employees who have evidence of or are concerned about improper behaviour and/or conduct that may cause risk must report their concerns immediately to Dominion through the ethics channel, which is available on the corporate website.