GreenVolt

Integrated Risk Management Policy

Shaped
by Nature

Integrated Risk Management Policy

1. Policy introduction

1.1. The Board of Directors of GreenVolt considers risk management a central theme and an integral part of the strategic management of organization, contributing for the creation of value for shareholders and other stakeholders.

1.2. By defining and implementing a risk management system in the organization, this process will allow all existing risks, both internal and external, in GreenVolt's activity to be identified, evaluated, monitored, as well as to ensure that residual risks remain at acceptable levels by the management and management body, and that any changes do not significantly and negatively affect the financial situation, reputation and image of the company.

1.3. It is important to note that the risk management process is a continuous activity, in constant development and that it runs through the entire strategy of the organization. It should be applied assertively in all risks, both in the past and in the present, so that we can learn from them and thus be prepared to ensure the future sustainability of the business.

1.4. Thus, this Policy aims to establish principles, guidelines and responsibilities to be observed in the risk management process, in order to enable an adequate, assessment, treatment, monitoring and communication of risks or potentials in GreenVolt's business and that constitute threats that may affect the achievement of strategic and business objectives.

1.5. The Policy also has the purpose of providing employees in the GreenVolt's universe of companies with skills to apply a risk management methodology in a disciplined, systematized, consistent and comprehensive manner, enabling the efficient and effective implementation of the risk management system.

1.6. The risk management process presented in this document follows the principles and guidelines established in the international framework on internal control and risk management matters, namely COSO Internal Control Integrated Framework, COSO Enterprise Risk Management Framework and ISO 31000 – Risk Management.

1.7. The application of the methodology presented in this document will support the Board of Directors and management bodies in optimizing the decision-making process to minimize losses and maximize results.

2. Scope

The Policy applies to the entire GreenVolt Group, in compliance with the following rules:

a) in the case of companies wholly dominated by GreenVolt, their management bodies shall carry out the local transposition of this Policy;

b) in the case of companies in which GreenVolt exercises control, co-control (Joint Ventures) or significant influence (Associates), GreenVolt representatives present at the management body shall, by effect of the exercise of control, co-control, or significant influence, support the adoption of the measures necessary for the local transposition of this Policy;

c) in the case of companies in which GreenVolt does not exercise control or significant influence, GreenVolt representatives shall observe the guidelines of this Policy in the performance of their duties and, as far as possible, encourage the adoption of the rules and procedures consistent with this Policy.

3. Definition of terms

3.1. Risk Management

It is the culture, processes, procedure and government structure implemented to manage risks, enabling the identification, assessment, treatment, monitoring, reporting and taking decision risk based.

3.2. Risks

It is the effect of uncertainties on the company's objectives. It is the possibility that an event will occur and affect the achievement of the objectives.

3.3. Uncertainty

It is the situation of insufficient information associated with a given event, including its understanding, its knowledge, its consequence or its probability. Uncertainty can turn into a threat or an opportunity for the company.

3.4. Event

It is the occurrence, changing or non-existence of a specific set of circumstances. An event can consist of one or more occurrences and can have multiple causes. It may also consist of the non-occurrence of something.

3.5. Risk Profile

It is an organized view of the risk assumed by the company and that allows the management body to be able to decide the several types of risk that it is willing to take in the development of its activity.

3.6. Risk appetite

It is the level of risk that GreenVolt is willing to accept and manage to achieve its strategic and business objectives, with the aim of creating and preserving value for its shareholders and other stakeholders.

3.7. Risk tolerance

It is the definition of the level of uncertainty that GreenVolt is willing to assume to achieve strategic and business objectives.

3.8. Risk treatment
It is the action or set of actions selected and implemented, with the objective of managing and/or changing the behaviour of the risk.

3.9. Impact or Consequence
It is the result of an event stated qualitatively and/or quantitatively, which affect the defined objectives. There may be diverse results associated with the event that can lead to positive or negative impacts on the goal.

3.10. Inherent risk
It is the risk associated with the existence of the operation, process, transaction, or activity. It is the situation in which response and treatment actions have not yet been applied to change the probability of occurrence and/or impact at acceptable levels.

3.11. Residual risk
It is the portion of risk that remains after the implementation of response and treatment actions by those responsible.

3.12. Internal Control
It is the process carried out by all of employees of the company, with the aim to provide a reasonable assurance in achieving the objectives associated with effectiveness and efficiency of operations, reliability in the preparation and disclosure of financial and non-financial information and compliance with established laws, standards and regulations.

3.13. Control mechanism
It is the method or measure implemented that must be performed and that leads to a given result, with the aim of managing and/or changing the behaviour of the risk.

3.14. Process Owner
It is the function in charge for managing the process end-to-end.

3.15. Risk Owner
It is the function in charge to ensure the risk management on a timely basis in the area which it belongs. It is also who defines or supports the selection of risk treatment or the implementation of the control mechanism.

3.16. Control Owner
It is the function in charge for defining the design of the control and ensuring the implementation and execution of the control mechanism for risk management. The control owner is not always the risk owner.

3.17. Employees
Employees (including Directors and Directors), interns, temporary workers, business partners and service providers.

3.18. Organic Unit
Any business unit, department or supporting function belonging to the universe of GreenVolt companies.

4. Functions and Responsibilities

The proper risk management depends on a well established government structure, as well as the clear and objective definition of functions and responsibilities.

It is important that each party involved in the process understands its responsibilities and its individual and collective role, since it is not a matter of having a defined process and procedures, but also of the behaviour of each party to include the culture of risk management in all activities.

4.1. Board of Directors

- Establish the government structure for risk management;
- Define the level of risk appetite and risk tolerance;
- Regularly approve and review the integrated risk management policy and ensure its implementation;
- Regularly approve and review the risk management appetite, defining situations and boundaries that are clearly unacceptable in the business;
- Know and monitor risks classified as very critical, critical and elevated;
- Manage the risk appetite regarding to the behaviour in search of opportunities in the development of new products, fresh solutions and new markets;
- Ensure and get comfort that control mechanisms and assessments are in place in critical areas.

4.2. Supervisory Board

- Monitor the risk management process and the fulfilment of its objectives;
- Regularly assess and check the effectiveness and sufficiency of the internal control and risk management system;
- Monitor the necessary control mechanisms for risk management are in place;
- Review and suggest adjustments to the policy that it deems necessary;
- Monitor the levels of risk appetite and risk tolerance for critical areas;
- Monitor risks classified as very critical, critical and elevated;
- Suggest improvements to the risk management process and information.

4.3. Chief Executive Officer (CEO)

- In conjunction with Board of Directors create an environment for the risk management process to work effectively;
- Support priorities in the implementation of the risk management process;
- Monitor the risk management process, the performance of the system and the fulfilment of its objectives;

- Ensure the necessary control mechanisms for risk management are in place;
- Monitor risks classified as very critical, critical and elevated, and the effectiveness of their control mechanisms.

4.4. Risk Management Department

- Provide the risk management methodology;
- Develop, implement and review the risk management process;
- Develop and implement the strategy and the necessary resources for the risk management process;
- Advise the business units, departments and supporting functions in identifying and assessing the likelihood and impact of the various categories and types of risks;
- Advise the business units, departments and supporting functions in defining the risk treatment strategy, suggesting improvements or alternatives as needed;
- Consolidate and communicate relevant risk to the Board of Directors and Supervisory Board, as needed;
- Support the annual risk assessment risk process;
- Take actions that allow the conscious dissemination of the culture of risk management;
- Disclose risk indicators, implementation status, effectiveness of corrective measures and risk maturity to the Board of Directors and Supervisory Board, and other bodies as needed.

4.5. Businesses Units and Supporting Functions Officers

- Put forward the integration of risk management culture into the planning of activities;
- Disseminate the risk management culture among its teams;
- Ensure the implementation of an efficient model of identification, assessment of likelihood and impact, and risk treatment aligned with this Policy;
- Ensure the implementation of risk treatment mechanisms necessary for risk management;
- Proactively assess the efficiency, effectiveness and sufficiency of the implement risk treatment mechanisms and make the necessary adjustments;
- Review, complete and keep updated the management tool that allows the organization of the identified risks, the response strategy and the treatment of defined risks in a clear and objective manner;
- Share the risk management tool with Risk Management Department for information consolidation.

4.6. Businesses Units and Supporting Functions Employees

- Ensure the effective execution of the internal control system and risk management system in its activities;
- Actively act in risk identification, risk assessment and suggest the implementation of risk management procedures;
- Support the Business Units and Supporting Functions Officers in completing and updating the management tool that allows to organize clearly and objectively the identified risk, the response strategy and the treatment of defined risks in a clear and objective manner
- Carry out the control mechanisms, according to the treatment model defined for risk management;
- Collaborate in actions that allow the conscious dissemination of the culture of risk management.

4.7. Internal Audit Function

- Prepare the Annual Audit Plan (based on the outcome of the risk assessment), with the aim to verify the effectiveness of the internal control system and the risk management system;
- Identify and suggest improvements in the risk management process, in the operationalization of mechanisms for the risk treatment and compliance with associated standards and regulations;
- Regularly report the audit results on the effectiveness of the internal control system and risk management system to the Board of Directors and/or Supervisory Board.

4.8. External Assurance Providers

- Review internal control system and risk management system implemented, as well as the internal control mechanisms implemented with potential impact on the financial statements preparation process.

5. Integrated Risk Management System

Based on the guidelines of the Board of Directors and principles defined in the COSO and ISO 31000 frameworks, the methodology established for risk management should be carried out according to the following sections.

5.1. General information

The risk management is an essential pilar on how we conduct our activities, thus present in the culture of GreenVolt and in the various existing processes, with all employees having the initial responsibility to looking for solutions that allow managing risk events, reducing their impact and/or likelihood.

The risk management system should correspond an integrated set of permanent processes that ensure an adequate comprehension of the nature and magnitude of risks underlying the activity carried out, allowing an appropriate implementation of the strategy and the fulfilment of objectives.

5.2. Risk Categories and Risk Types

To support the risk management process and establish a common risk language to all stakeholders, GreenVolt establish a risk management structure model, composed by 4 risk categories, 12 risk subcategories and 46 risk types.

5.2.1. Strategic Risk

- External Environment: Country, Sector regulation, Sector taxes and chargers, Climate changes, and Technological disruption.
- Internal Environment: Energy planning, Investment strategy, Corporate Governance, Socio-Environmental, and Reputation & Image.

5.2.2. Business Risk

- Energy Market: Energy price, Renewable energy production, Commodity price, Equipment or Material supply, Project development, Project execution, and Project operation.

5.2.3. Financial Risk

- Financial Market: Foreign exchange rate, Interest rate, Inflation, and Financial asset valuation.
- Credit: Clients (B2B & B2C) and Counterparties (Energy & Financial).
- Liquidity: Treasury, Access to capital & Capital cost and Rating notation.

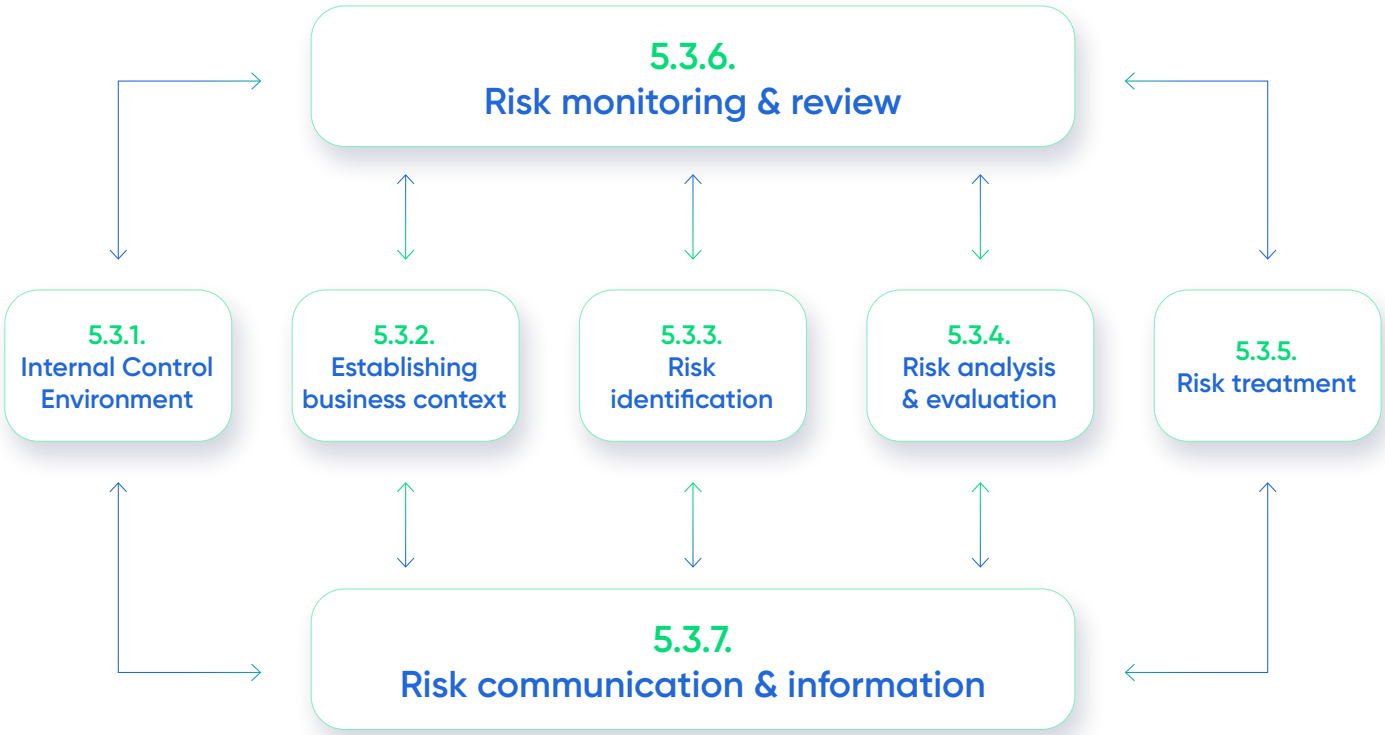
5.2.4. Operational Risk

- Processes: Execution process, Sales process, Suppliers & Outsourcing process, Billing, Collections & Payments process, Management control & Budget process, and Business Continuity Process.
- Asset Management: Assets under development, Damage to assets in operation, and Technical & Non-technical losses.
- Reporting Standards: Accounting standards and Environmental standards.
- Legal: Fiscal, Civil, Administrative and Labour, Litigation and Compliance.
- Human Resources: Talent & Knowledge management, Security & Health, and Ethical conduct & Fraud.
- Information Systems and Technologies: Availability, Security & Integrity.

5.3. Risk management process stages

The risk management is a continuous and regular process that requires reviewing and updating risk profiles for the entire group. To ensure the updating and the integrity of data, a formal review process is carried out once a year by Risk Management Department.

The risk management system is composed by a set of components, split by processes, single and integrated actions. The risk management system engages the components presented in the following figure.



Adapted from ISO 31000 – Risk Management

5.3.1. Internal control environment

The internal control environment of the risk management process reflects the philosophy and attitude of the company through the guidelines of the Board of Directors and the CEO. It can be achieved, but not limited, through the following activities:

- Definition of the government structure of risk management, including the clear definition of the authority and responsibility of risk management throughout the group;
- Existence of an Integrated Risk Management Policy, established in line with the guidelines of the Board of Directors;
- Existence of the Risk Appetite Statement, with the definition of risk appetite levels and risk tolerance in relevant matters, with potential impact on the achievement of strategic and business objectives.

5.3.2. Establishing business context

The business context is defined as trends, relationships and other factors that can influence the current and future strategy of the group and the achievement of its strategic and business objectives.

The business context can be:

- Dynamic: where new risks can arise at any time and change the pattern of activity behaviour.
- Complex: where there are many interconnections and interdependencies.
- Unpredictable: where changes occur quickly and without means of identifying events in a timely manner.

In this process is essential that the objectives are clearly defined and identified, and that they are aligned with the vision, mission and values of the company, as well as consistent with the definition of risk appetite and risk tolerance.

At this stage it is important to consider the factors of internal and external environment that have potential to influence the strategy and the achievement of the objectives. The following table presents some categories and characteristics of internal and external environment to be considered.

Environment	Category	Characteristics
Internal	Capital	Assets, including cash, equipment, property, patents.
	People	Knowledge, skills, attitudes, relationship, values, culture
	Processes	Activities, tasks, policies, procedures, changes in management, operational and supporting processes
	Technology	Evolutive and corrective developments, new adopted technologies
External	Political	Govern intervention and influence, including tax policies, labour laws, environmental laws, trade restrictions, tariffs and political stability.
	Economic	Interest rates, inflation, foreign Exchange rates, availability of credit, GDP growth.
	Social	Customer needs or expectations, population demographics, such as age distribution, educational level, distribution of wealth.
	Technological	Research and Development activities, automation, technology incentives, technological changes or disruption.
	Legal	Laws (e.g., employment, personal data protection, consumer, health and safety), regulations, industry standards.
	Environmental	Natural or human-caused catastrophes, climate changes, changes in energy consumption, attitudes towards the environment.

5.3.3. Risk identification process

At this stage, the main purpose is to identify and generate a comprehensive listing of inherent risks and opportunities based on events that can create, increase, prevent, reduce, accelerate or delay the achievement of the objectives.

The approach to identifying risks can be varied, and can occur in daily activities, such as budget preparation, business planning, performance monitoring, process understanding, data analysis and team meetings, with customers, suppliers, regulators and external assurance providers.

When identifying the risk, it is necessary to describe it precisely, which will allow:

- Manage risk listing more effectively and understand the relationship with strategy, business objectives and performance;
- Assess the severity of the risk in the business context;
- Identify the events that cause the risk and impacts, allowing to select the proper risk treatment;
- Understand the interdependencies between risks and business objectives.

5.3.4. Risk analysis and evaluation process

In the risk assessment process, it is essential that the origins and consequences that may exist and the probability that these consequences may occur are identified and analysed. The impact assessment is measured according to the potential magnitude of loss or gain if the risk or opportunity materializes. Probability assessment is measured according to the number of occurrences of the event, that is, its frequency. This assessment is based on past experiences and relevant knowledge.

To support the process of analysis and evaluation of probability and impact and establish a comprehensive spectrum of situations that can impact the areas, processes and activities by all parties involved, GreenVolt establishes the criterion to be used at this stage of the process, and risks can be classified as: Reduced, Moderate, High, Critical and Very Critical.

The purpose of the risk assessment is to assist those responsible in decision-making to define a better risk response, according to the potential impact on the business, and to identify the most relevant and priority to monitor stakeholders in business management.

5.3.5. Risk treatment

The risk treatment process involves the analysis of possible response strategies to decide the proper treatment to manage risk. Possible risk response strategies include: Avoid, Pursue, Control (Prevent, Mitigate, and Transfer) and Accept.

When determining the risk response option, should be performed a cost-return analysis to compare the cost of risk treatment with the result of the risk reduction.

Inherent risks classified as Reduced usually do not require continuous monitoring, except the recording and monitoring of its evolution. However, these risks may be subject to the implementation of control mechanisms and in these circumstances, it is necessary to assess the cost-return of risk management.

For inherent risks classified as Moderate, Elevated, Critical and Very Critical, the Organic Unit should determine the risk response, aligned with risk appetite and risk tolerance, and the treatment required for risk management.

The risk management process involves the implementation of control mechanisms, which aim to keep risks within the acceptable levels established.

Thus, to ensure the effectiveness of the control mechanisms it is necessary to understand the content of the control and the supporting documentation.

Control mechanisms can be classified into two categories:

- Preventive: It is a control mechanism implemented in the process with the aim of avoiding or reducing the impact of the incidence of the risk event; and
- Detective: It is a control mechanism implemented in the process with the objective of responding to the incidence of the risk event and reducing the potential impact.

The type of control mechanism to be used depends on the classification of risk and cost- return to be obtained with the implementation of such mechanisms. The Control Owner shall conduct a self-assessment to ensure that the treatment strategy defined in risk management is capable to produce the desired effect and that it effectively produces the desired result.

The risk assessment process is carried out initially for the identified (inherent) risks. After the treatment measures have been applied to these risks, the assessment and treatment process should continue until the residual risk becomes acceptable in accordance with the defined risk appetite and risk tolerance.

5.3.6. Risk monitoring and review process

The risk information requires regular monitoring and review to ensure risk are up to date. The environment in which GreenVolt operates is constantly changing, as are the risks exposed. If the risk information is not precise, inappropriate decisions may occur and otherwise could be avoided or better managed.

Thus, the Businesses Units and Supporting Functions Officers, as well as the teams, are the first guarantors that the risk information is up to date. Thus, all existing information on risks is reviewed at least on an annual basis, with the participation of governing bodies.

This process is relevant for the continuous development of risk management and to allow the continuous improvement of the entire process.

5.3.7. Risk communication and information process

The communication and distribution of risk information to stakeholders is a key element of the risk management process. Communication and information must be disclosed clearly and objectively disseminated, in an appropriate model, with the necessary level of detail, at the right time, respecting the best management practices and information security.

6. Risk register

The risk register is an important activity to characterise risk in the risk management process. This action will allow to know in a systematized way all the factors that originate the risk, as consequences if it occurs, as treatment measures implemented and as improvements that are still necessary.

The risk register shall document in a disciplined, structured and organized manner the results of the business context, risk identification, risk assessment carried out and as risk response and risk treatment actions necessary to make residual risk at an acceptable level. If the Organic Unit that is recording the risk identifies a risk in its process but is not responsible for managing the risk, then it should indicate the most appropriate Risk Owner. The risk register activity should be carried out in the implementation of new processes, in the acquisition or development of new businesses.

The information of the risk register is reviewed annually and may be reviewed in other circumstances as indicated by the management body or Board of Directors.

7. Policy review

The appropriateness of the Policy to its purpose is ensured by the Risk Management Department every 2 (two) years. However, the revision of the Policy may be suggested at a shorter period, as necessary.

8. Final notes

8.1 This Policy takes effect on the date of approval by the Board of Directors.

8.2 Any changes to this Policy shall be approved by the Board of Directors.