NT-025

INTERNAL CONTROL MANUAL

Company Standard

Approved by the Board of Directors on 23-10-2020

Contents

1. Object and scope of applicability

1.1. This manual sets out the general principles and requirements of the internal control components, as well as the organizational model associated to the integrated and uniform management of the internal control at Galp, defined as the series of processes implemented by the governing bodies, specialized committees, internal auditor and by Galp's personnel, with a view to conferring reasonable assurance of the achievement by Galp of its objectives related to the operations, reporting and compliance.

1.2. The present standard follows the COSO reference model - *Internal Control Integrated Framework*. Galp endorses the five components of this model as pillars of its internal control system: 1. Control environment; 2. Risk assessment; 3. Control activities; 4. Information and Communication; 5. Monitoring activities.

1.3. The design and implementation of process controls is ruled by the present manual and shall observe Galp's standards in force.

1.4. This manual applies to all the Organizational Units (OUs) of Galp and affiliates or other entities, regardless of their legal nature, in which Galp holds management control, encompassing all the locations where Galp operates.

1.5. In cases where Galp does not hold either directly or indirectly 100% of share capital in the company, the persons designated by it for management positions at these entities must ensure the approval and adoption of the standard herein by their respective management bodies.

1.6. The people appointed by Galp for management positions in subsidiaries in which Galp does not hold management control must endeavor to promote in those companies measures leading to the recognition and adoption of the rules and procedures established in the present manual or of equivalent rules.

2. Internal Control Components

The internal control components act and operate in an integrated and interdependent manner as a single system, so that they grant a reasonable assurance of compliance with Galp goals in relation to (i) the pursuit of its strategic objectives; (ii) the preparation and disclosure of financial and non-financial information to be provided to the internal and external stakeholders; (iii) compliance with applicable law and regulations; (iv) the safeguarding and protection of assets; and (v) efficiency and effectiveness in operations.

The five components are interdependent with a multiplicity of interrelations and links between one another, particularly in the way that the principles underlying each component interact.

Galp recognizes that its internal control is subject to limitations that fundamentally result from:

- potential lack of clarity of the defined strategic Galp objectives;
- the undertaking, by people, of tasks, control activities and decision-making, which are therefore subject to human errors, flaws or bias;
- characterization of fraudulent conduct, such as collusion and senior management's capacity to by-pass the existing controls;
- external events that might be beyond Galp's control span.

These limitations result in the impossibility for internal control to confer absolute assurance as to compliance with Galp's objectives, although it can confer reasonable assurance thereof.

2.1 Component 1: control environment

The control environment consists of a series of standards, processes and structures in place at Galp, which constitute the foundations of its internal control system.

The control environment is influenced by internal and external factors, such as Galp's values and the market in which it is integrated, reflecting the positioning of the management bodies with respect to the importance of the internal control system and guiding all the personnel in their decision-making, from a control perspective.

The control environment is supported by the organizational culture, which must ensure that expectations on behavior which reflect a commitment to ethical values, responsibilities, policies, standards and procedures are achieved. The senior management establishes and communicates the importance of internal control and the expected standards of conduct.

2.1.1 Principles

Galp's control environment is based on the following five principles:

1 - Demonstration of commitment in relation to ethical values

The Board of Directors, Audit Board, Executive Committee, Organizational Units and specialized committees at Galp demonstrate commitment to the ethical values through the issue of the following guidelines, actions, conduct and documents:

- Galp Vision and Values (available on Galp's intranet and official site at this link);
- Code of Ethics and Conduct (available on Galp's intranet and official site at this link);
- Policies, standards and procedures (disclosed and accessible at Galp's intranet at this link);
- Channel for communication of irregularities (via the address opentalk@galpenergia.com or form available on the intranet and on Galp's official website at this link);
- Existence of a process for the investigation of irregularities by the Ethics and Conduct Committee pursuant to the applicable procedure (available on Galp's intranet and official site at this link).

These guidelines, actions, conduct and documents are communicated internally at all levels in Galp,

and externally to the stakeholders, including service providers and business partners. Those responsible for the relations with these external stakeholders ensure obtainment of a formal commitment therefrom.

Galp requires, from all its employees and other players in the internal control system, attitudes of integrity, high ethical standards, leadership, critical thinking and problem-solving skills.

Any detected behavior that is inconsistent with the standards of conduct, policies, practices and responsibilities of internal control is assessed, and suitable corrective measures are taken in due time.

2 – Independence of the Board of Directors in relation to the Executive Committee, and supervision of the Internal Control's development and performance by the Board of Directors and Fiscal Council

The Board of Directors is responsible for approving the policy of the internal control system and definition of risk management strategy and supervision, monitoring and controlling performance of tasks delegated by the Executive Committee, in particular, the development and performance of internal controls.

The Company's current management is carried out by the Executive Committee pursuant to the delegation of powers conferred by the Board of Directors, available in the Regulation of this body (accessible on the intranet and at Galp's official website at this link), the latter supervising and monitoring the management, including through its independent members.

The Audit Board is responsible for supervising the effectiveness of the risk management, internal control and internal and independent audit systems, and proposing the necessary adjustments, as well as for annually appraising their functioning and their respective internal procedures, and issuing statements on work plans and resources allocated to internal control services, as established in their Regulation (available at Galp's official website and its intranet at this link).

The Executive Committee is responsible for issuing statements along with the Audit Board on the operational efficacy of internal controls, in particular on the ICFR, based on the conclusions of independent tests conducted by the internal audit feature.

3 – Definition by the Executive Committee, with supervision by the Board of Directors, of the structure, reporting lines, levels of competence and responsibility required to achieve Galp's objectives

Galp's organizational structure, on the one hand is based on business units and on the other, on a corporate center composed of support functions. Responsibilities and competencies are attributed by the Executive Committee through the approval of organizational standards, under the coordination of each one of the executive directors.

The corporate area responsible for Galp's organizational development is responsible for allocating individual competencies in accordance with the applicable internal standard, and also for optimizing and adjusting the organizational structures to the defined strategy, identifying opportunities and priorities for improvement in Galp's organizational structure, as defined in the organizational standard.

The corporate area responsible for Galp's *governance* formalizes the rules regarding management's decision-making, attribution of competencies and responsibilities, as defined in the organizational standard.

The rules and limits of competencies to be observed by employees and decision-making bodies and other personnel with decision-making and externally binding positions within Galp are defined in the internal standards (available at Galp's intranet at this link).

The corporate area responsible for Galp's internal controls sets out guidelines for the structure, reporting lines, level of competence and responsibility necessary for the development of an effective internal control system at Galp, in particular with regard to the ICFR, as defined by the organizational standard, integrating the governance model of internal control over financial reporting at Galp (which may be accessed here).

The efficiency and efficacy of reporting lines and levels of competencies and responsibility are periodically assessed, making the necessary revisions, in supporting the internal control system, considering the following variables:

- Type of business, size and geographic distribution of the organizational units;
- Risk related to Galp's objectives and business processes;
- Nature of the attribution of competencies and responsibility for the senior management, organizational units, functional units and local management; and
- Financial, legal, regulatory and tax requirements.

4 – Demonstration of commitment to attract, develop and retain skills, in line with Galp's objectives

The Executive Committee supervises the assessment of the existing set of skills at Galp in relation to the policies defined to achieve the objectives, conducting cost/benefit analysis of the different levels of competencies and experience.

The process of performance assessment in force at Galp ensures the validation of results by way of higher hierarchical levels, successively up to its executive directors.

The assessed competencies are technical (knowledge- based) and behavioral, as embodied in Galp's values, where the intended behaviors and scales of observation are described.

In addition to the assessment of competencies, performance assessment includes the achievement of results associated with company, team and individual metrics, directly linked to Galp's objectives and results.

The overall result of the performance assessment contributes to the calculation of the variable remuneration.

The corporate area responsible for the management of Galp's personnel directs the necessary processes to attract, develop and retain competent personnel, in sufficient number to support the pursuit of its objectives, in line with the defined policies and standards, namely the standard on

recruitment and mobility (which can be accessed here).

5 – Attribution of responsibilities to the participants in internal control aimed at the achievement of Galp's objectives

The Executive Committee attributes responsibilities for the performance of internal control to all the organization's levels by defining organizational standards for the respective areas. The attribution of these macro responsibilities is described in the responsibility matrix listed under point 5 of this manual.

2.2 Component 2: risk assessment

Risk assessment is a dynamic and iterative process, since it depends on Galp's objectives which may be modified and constitutes the basis for determining how risks are treated in order to accomplish these objectives.

2.2.1 Principles

Galp's risk assessment is based on the following principles:

a) Identification of the strategic objectives which are reported to the market (in particular, within the scope of the Capital Markets Day and via the Management & Accounts Report) and which enable the detection and assessment of the risks relative to compliance thereof;

b) Identification and analysis of the risks inherent to the achievement of Galp's objectives as a basis to determine the way that risks should be managed. The identification and assessment of risks is carried out by Galp's first and second lines of defense pursuant to Galp's Risk Management Policy (link), of the risk management governance model (link) and the internal standard on risk management in processes (link).

c) Contemplation of the possibility of fraud in risk assessment. The prevention of fraud must be subject to a specific programme in accordance with the principles established in chapter 4.2 of the present manual;

d) Identification and assessment of alterations that might significantly influence the internal control system, with this attribution having been conferred to the Risk Management Committee by organizational standard (available at Galp's intranet at this link).

2.2.2 Stages

Risk assessment at Galp, in the context of the internal control system, involves five stages:

a) Identification of objectives – Identification of the context and main objectives of the process relevant for the purposes of internal control;

b) Identification and analysis of risks – Identification and analysis of risks associated to the achievement of the main objectives and of the process;

c) Risk assessment – Assessment of the degree of severity of the identified risks, using criteria of impact (i.e. low, moderate, high or very high) and probability of occurrence (i.e. remote, improbable, probable or frequent);

d) Treatment of risks – Identification and implementation of the adopted option for the treatment of the risk according to the defined tolerance to risk. Tolerance of risks is proposed by the Risk Management Board and approved on an annual basis by the Board of Directors following the report by the Audit Board, incorporated into Galp's processes in compliance with the internal standard on risk management processes;

e) Monitoring of risks – Monitoring, via supervision conducted within the scope of the control activities specified, of risks regarding the effectiveness of the mitigation measures and the evolution of risk exposure.

2.2.3 Whenever risk assessment concludes on exposure higher than the tolerance defined by Galp, a decision must be taken on the need to create or intensify the use of control mechanisms to mitigate the risk identified**.**

2.2.4 The main risks and risk factors of the industry in which Galp is integrated as well as those specific to Galp are identified, in a systematic and organized form in Galp's Risk Dictionary (which may be consulted here).

2.3 Component 3 – control activities

Control activities (or "controls") consist of defined and implemented actions, which enable mitigating risks to a level considered acceptable, taking into account the outcome of the work carried out in the risk assessment component.

2.3.1 Principles

The principles of Galp's control activities are as follows:

a) Selection and development of control activities that contribute to mitigate the risks associated with achieving Galp's objectives up to a level considered acceptable;

b) Selection and development of control activities to be applied on the technology supporting the pursuit of its objectives;

c) Development of control activities defined in internal standards that establish expected conducts and procedures that accomplish them.

2.3.2 Classification

Control activities are classified into three major groups:

- **High level controls (Entity level controls)** – pervasive controls ("tone at the top") and that constitute the basis of Galp's internal control system (control environment). These controls were described in chapter 2.1 of the present Standard.

- **General IT controls (IT level controls)** – controls related to the technology supporting the pursuit of Galp's objectives and with its respective processes. The design, implementation and operation of these control activities is a responsibility of the corporate area of information systems ("IT & Digital"). The use of general information controls by Galp is described in point 3.5 of this Standard.

- **Process level controls** – controls implemented in business processes, both in terms of corporate areas and from business units. The design, implementation and operation of these control activities is a responsibility of the manager responsible for such processes.

  At Galp, the internal control activities must be documented in terms of processes, which are organized in accordance with Galp's Process Model, being supported by an information system platform, which classifies the processes and the respective risks and assures the association of the controls to the process flow. In addition, with regard to the ICFR, the risks of distortion with the impact on financial reporting and control activities designed to mitigate these risks, are to be documented in the risk and control matrix on the SI platform, characterizing high-level controls, general computing controls and procedural controls. The mapping of processes at Galp is carried out in accordance with the internal standard relating to the rules on process mapping (available here).

2.3.3 Guidelines and directives

The selection, definition and implementation of the control activities is framed under the following guidelines and directives, as well as their effects and limitations:

1. **Responsibility** – The control activities have a manager responsible for reporting (accountability) on its operation and effectiveness. The lack of definition assigning the responsibility for control could imply a reduction of its effectiveness.

2. **Traceability** – The keeping of adequate evidence of the implementation of controls, documentation or IT, is assured for a period of time not less than five years, without prejudice to the applicable policy of retaining information. The absence of traceability could prevent the undertaking of a subsequent control or the checking of its implementation by an independent third party.

3. **Preventive or corrective action** – The control activities are reflected in preventive or corrective actions aimed at limiting the probability of occurrence or the impact of the risk, respectively.

4. **Effectiveness** – A control only achieves its objective of mitigating the risk if it is effective, and the checking of this effectiveness is performed during the monitoring process. Greater weight should be given to control activities with higher inherent effectiveness. Thus, preventive and automatic control activities (carried out using technological/IT resources) should be given priority in relation to corrective and manual control activities. A cost/benefit analysis of the possible options should be taken into account.

5. **Complementarity between prevention and detection** – The higher effectiveness associated to the preventive activities should be complemented with specific control activities of detection and correction, in particular when situations that could transcend the effectiveness of prevention might result in high impacts.

6. **Segregation of duties** – An appropriate segregation should be assured between the preventive (e.g. approvals) and detective (e.g. review) control activities related to the same risk. Therefore, merely as an illustration, the reviews should be carried out by a third party that is "independent" from the person that carried out the preventive activity.

7. **Segregation of accesses** – The logical or physical accesses associated to mechanisms, systems or technologies that support the control activities should be differentiated in accordance with the defined segregation of duties.

8. **Periodicity** – A higher frequency in the implementation of a control will increase its effectiveness. However, this should not exceed the frequency with which the source associated to it occurs in the process (e.g. the control of review of issued invoices should have a maximum periodicity corresponding to the frequency of issue of the invoices).

9. **Technological dependence** – The higher the use of technology the higher the confidence level in the implemented control as it is less likely to be affected by human errors. However, the use of control activities based on technologies of information systems should be appropriately supported by specific IT controls that mitigate particular risks related to:

    a) Technological infrastructure and operations;

    b) Security;

    c) Life cycle of information and communication technologies; and

    d) Service providers.

2.3.4 Classification of control activities

At Galp the control activities are classified according to purpose, type, level of automation and periodicity.

Purpose – Classification regarding the objective of the control activity based on the assumptions (control activity goals):

- Authorization and approval – confirms the validity of a given transaction or operation;

- Verification – compares one or more elements with a given reference (defined, for example, in an internal standard or manual) aimed at identifying and treating exceptions. Verification normally considers the completeness, validity and precision of transactions processed. Information subject to verification is associated to one or more magnitudes of monetary, physical, chemical or other nature (e.g. monetary value, time, temperature).

- Physical Inventory - custody, protection or conservation of physical asset (e.g. equipment, inventories, money and other physical assets) and periodic counting thereof and comparison with the amounts shown in records.

- Safeguarding information – controls on the processing, updating and maintenance of the wholeness, validity and precision of data and information on which processing of transactions is based (e.g. master data).

- Reconciliation – comparison between two or more elements aimed at treating exceptions, in order to eliminate detected divergences and ensuring the wholeness and precision of transaction processing.

- Review and Supervision – confirmation as to how other transactional control activities are to be implemented, particularly authorizations/approvals, verifications, physical inventories, reconciliations and controls on safeguarding information, are to be conducted in full, correctly and in accordance with Galp's policies and procedures. These activities are particularly incident on activities with a higher associated risk level and normally involve critical appraisal during selection and implementation thereof.

Type – Classification regarding the timing of the control activity:

- Preventive – act before the risk event, being designed and implemented in order to prevent the occurrence of an event or outcome that is not intentional. These controls are able to reduce the probability of occurrence of a given event, by managing to eliminate or mitigate a source of risk;

- Detective – act during or after the occurrence of the risk, being designed and implemented to reveal an event after its occurrence, but before the main objective has been completed or compromised. These controls fundamentally act on one or more dimensions of impact, and should trigger one or more impact corrective or mitigation actions.

Level of automation – Classification as to the technology supporting the implementation of the control activity and in the case of automatic or semi-automatic controls, also identifies the systems intervening in their implementation:

- Manual – are implemented manually and do not require/depend on the support of technology/ information systems;

- Semi-automatic – are implemented manually, however require involvement/dependency on technology/ information systems;

- Automatic – are implemented entirely through the use of technology/ information systems.

Periodicity – classifies the controls regarding the frequency of their implementation (e.g. daily, weekly, monthly, quarterly, annually, on-event, i.e. controls implemented whenever necessary).

The responsible person may also classify the controls according to other aspects, such as the risk coverage level (e.g. high, medium, low).

2.4 Component 4 – information and communication

This component of internal control consists of the series of information required for the implementation of adequate internal control tasks to support the achievement of its objectives and their respective communication.

2.4.1 Principles

The information and communication within the scope of Galp's internal control is based on the following principles:

a) Obtaining, generation and use of quality and relevant information to support the operation of internal control;

b) Internal communication of information, including the objectives and responsibilities required for the operation of internal control;

c) Communication to the stakeholders of matters related to the functioning of internal control.

2.4.2 Information

All information necessary for the appropriate operation of Galp's internal control system must be available, permitting the responsibilities defined in each of the five components of internal control to be exercised in an effective manner, and it should be consistent with Galp's need to assess and respond to risk.

The information should be available for those who need it to exercise their duties in the context of internal control. This information includes Galp's strategic objectives to its policies, standards, specific procedures or data underlying the implementation of controls.

The quality of the information implies the observance of the following requirements:

- Completeness;
- Accuracy;
- Validity;
- Content appropriateness;
- Timing;
- Updated;
- Easily accessible.

On the other hand, the information should respect Galp's standards on information security (available at Galp's intranet at this link), personal data protection (available on Galp's intranet at this link) and other applicable standards or legislation throughout the entire life cycle of the information.

The control activities are described in documented information, which should be managed and kept in an appropriate condition of conservation and be accessible, in particular for purposes of the corresponding internal or external audit processes, and in order to assure compliance with the applicable company and sectorial standards and regulations.

The information relative to the internal control system is necessary to demonstrate its effectiveness, to enable appropriate monitoring and to substantiate the communication with stakeholders, and may exist in multiple formats and be supported by information systems or not.

The corporate areas responsible for internal control, governance and compliance, for risk management, for the security of information systems and for safety and sustainability, should be informed of the existence of any shortcomings in terms of the information required for the performance of the attributed internal control responsibilities or of a relevant limitation for the effectiveness of control, in order for appropriate measures to overcome these limitations to be able

to be adopted or proposed.

2.4.3 Communication

Communication in internal control seeks to effectively convey:

- Galp's objectives;
- the importance and pertinence of an effective internal control system;
- risk appetite and the respective tolerance;
- rules applicable to internal control;
- Galp's Risk dictionary;
- the duties and responsibilities of the participants in internal control.

Galp's communication principles are established in the Communication Policy (available at Galp's official website and on its intranet at this link), being the corporate area responsible for communication responsible for managing Galp's internal and external communication, according to the attributions conferred in the organizational standard.

All the participants in the internal control system should know their responsibilities and how their performance relates to the responsibilities of others, as well as know how to recognize a problem in due time, determine its cause and define an appropriate corrective measure.

The same should occur in the communication with external stakeholders, ensuring the necessary dynamics to understand the evolution of factors relevant for the internal control system.

2.5 Component 5 – monitoring activities

The monitoring of internal control consists of the verification, internal or independent, of the implementation and effectiveness of the defined controls.

2.5.1 Principles

Galp's internal control monitoring activities are based on two principles:

a) Definition, development and performance of current and/or occasional analyses to check whether the internal control components are working;

b) Assessment and communication, in due time, to the parties responsible for taking suitable corrective actions on any detected flaws of internal control, including corporate bodies.

2.5.2 Objectives

The monitoring activities should be carried out with a suitable periodicity vis-à-vis the level of risk that the controls intend to mitigate, and are aimed at the following objectives:

a) Assuring that the existing controls are effective and efficient, both in their design and

implementation and operational effectiveness;

b) Obtaining additional information that improves the existing risk assessment;

c) Analyzing past events or occurrences;

d) Detecting changes in the internal or external context, including modifications in the risk criteria and in the risk itself, which might require a review of the control measures;

e) Identifying emerging risks;

f) Detecting and communicating the results.

2.5.3 Classification

Continuous assessment – continuous assessment of the effectiveness of controls by the person responsible for the process (ultimately, the person in charge of the OU), enabling identification in real time and providing a rapid response to any flaws detected in the existing controls.

In this regard, the person responsible for the process should maintain an adequate level of monitoring of the control activities, in order to ensure the availability of the following information:

- Description, classification and context of the risk control;
- Any changes made to the control specifications (e.g. change of the periodicity of implementation);
- Documented evidence (electronic, paper or other format) of the implementation of the control.

This information should be available for the exercise of the monitoring activity in an independent form and documented on a specific SI platform for this purpose.

Independent or separate assessment – periodic assessment of the effectiveness of controls by internal auditing and/or by an entity that is independent. The scope and frequency of independent or separate assessment is a matter for critical appraisal by those in charge of these areas.

The independent and separate assessment activity should be carried out by an area or entity that is not involved in the design and implementation of the control.

The independent or separate assessment reviews in particular:

- The design of controls – review of the suitability of the controls *vis-à-vis* their intended purpose (specifications);
- The implementation of controls – verification that they are implemented in accordance with the specifications;
- The operational effectiveness of controls – review of the functioning of the controls, checking whether or not they are mitigating the risk as defined.

Without prejudice to other disclosure duties inherent to independent assessments, the person responsible for the control should be informed by the entity that carries out these assessments about:

- The scope of the monitoring;
- Period scheduled for the undertaking of the monitoring;
- Preliminary results for purposes of rebuttal;
- Final results.

The person responsible for the process subject to independent assessment assures that the monitoring activities do not affect the normal development of the process, consenting to it or warning against possible conflicts, which should be assessed together with the entity that carries out the independent review.

At Galp, independent assessment of internal control is carried out by the following areas:

- Internal Audit, in the context of its attributions as the area responsible for the independent and systematic assessment of Galp's activities through review of the risk management system, the optimization of management processes, internal control system (including ICRF) and governance systems;
- Corporate division responsible for safety and sustainability, in the context of its duties as the area responsible for the corporate audits on the environment, quality and safety at Galp;
- Corporate division responsible for legal affairs and governance, in the context of its duties of monitoring the internal control policies on matters of ethical, regulatory and governance compliance by Galp.
- Independent Auditors, within the scope of their ICRF certification attributions as soon as this is implemented.

2.6 Review and updating of internal control

The review and updating of internal control should occur at least whenever there are relevant changes to the level of processes relating to internal control, risks, control activity, regulatory aspects, information systems or the organizational structure of Galp, as well as the level of subsidiary companies, risks of material distortion on financial reporting and the recommendations from internal and independent audits.

Some examples of occurrences which justify the assessment of the need to review or update the internal control are:

- Change in Galp's strategic objectives;
- Relevant changes in Galp's organizational structure;

- Change of Galp's positioning;
- Entry of new personnel to key positions in the organizational structure;
- Replacement or implementation of a new information system;
- New legislation / internal standards and regulations;
- Creation of new sources of revenue, through the introduction of new products or services; and
- Modification of the existing processes and controls or introduction of new processes and controls.

The activities of review and updating of Galp's internal control should appraise (i) the persistence of the risk, (ii) the existence of new risks, (iii) the impact and probability of any risks that have changed, (iv) the effectiveness of the internal controls, (v) the need to redefine the controls and their periodicity, which should result in the establishment of management mechanisms for the new controls.

3. Specific Requirements

Due to the significant impact on the organization and the relevance and importance that the COSO reference model (Internal Control Integrated Framework) attributes to the reporting of financial and non-financial information, to the prevention of fraud, to the segregation of duties, to the use of service providers and technologies to support the activities, in this chapter specific applicable requirements are established in relation to these matters.

3.1 Preparation and reporting of financial and non-financial information

3.1.1 General aspects

The design, implementation and operation of the control activities in the preparation and disclosure of financial and non-financial information shall comply with specific requirements considering the relevance of its disclosure and impact on the decision-making of shareholders, investors and other stakeholders.

The main objectives related to the preparation and disclosure of financial and non-financial information are:

- Compliance with applicable standards and regulations, including that relating to accounting control and the capital market;
- The appropriate reporting of Galp's events, transactions and operations, in compliance with applicable accounting references;
- The appropriate reporting to its stakeholders of the material aspects of ESG.

The need for Galp to conduct critical appraisal, in particular subjective mensuration including estimates and assumptions, in events or complex transactions in order to draw up disclosures in a

reliable and transparent manner, is inherent to financial information and the application of accounting policies employed in the drafting of financial statements.

Accounting principles are periodically updated resulting from changes made to applicable standards and regulations.

The main risk associated to the reporting of financial and non-financial information consists of material omission or errors in the preparation and disclosure of information. The materiality of events expressed in financial statements determines the limit amount for defining whether a financial sum is of any relevance.

One of the key applicable requirements for Galp as a listed company consists of presenting a reliable financial report to the market, free of omissions or material distortions. In order to achieve this goal, Galp identifies and intervenes regarding risks that, individually or in conjunction, may result in omissions or material distortions of financial statements resulting in error or fraud.

In particular, with regard to fraud, the areas of fraudulent external financial reports and the incorrect appropriation of assets are considered within four focus points: 1) Types of possible fraud; 2) Assessment of incentives and pressures; and 3) Assessment of opportunities, always bearing in mind the probability of the incidence and magnitude of the impact.

The risks of omission or material distortion in financial statements are mitigated by control activities relevant to the financial report, which answer to assertions made on the information included in financial statements. Galp selects, develops and applies controls that affect the principles of each component of its financial statements and that respond to each risk assessed. Critical appraisal is conducted on the development of appropriate responses in order to mitigate the risks of omission or material distortion of financial statements, including among others, the materiality of the financial statements, business areas in which Galp operates, geographical markets, technological dependency, the scope and nature of the governance model and applicable standards and regulations.

3.1.2 Principles and assertions about the reporting of financial and non-financial information

The following assertions are included in the accounting, mensuration, presentation and disclosure of headings, transactions and events included in Galp's consolidated financial statements:

- Existence or occurrence – the recorded transactions correspond to events that occurred in a given period;
- Completeness – all the transactions and other events or circumstances that occurred in a given period and that shall be acknowledged in that period are recorded;
- Accuracy – values and other data related to the transactions or events are recorded appropriately;
- Shut-down of operations – the transactions or events are acknowledged and recorded in the period when they occurred;
- Presentation of disclosure – the information is duly placed, ordered and classified;
- Timeliness – the information is presented in due time for the corresponding decision-

making by stakeholders.

The preparation and presentation of financial information shall also take into consideration the following specific assertions:

- Rights and obligations – rights and obligations are acknowledged and recorded in the assets and liabilities, respectively, at any given moment;
- Valuation and classification – assets, liabilities, transactions, revenue and expenses are aggregated and recorded at their correct values in the accounting system in conformity with the relevant accounting principles;

The preparation and presentation of financial and non-financial information shall also take into consideration the following specific principles:

- Balance – The information reflects the organization's performance in an impartial manner, presenting positive and negative aspects which enable a balanced appraisal of its performance;
- Comparability – The information is consistent so as to enable the stakeholders to analyze the changes over time and to compare it with other similar organizations; and
- Clarity – The information is presented in a way that it is understood and is accessible to the stakeholders.

3.1.3 Approach to risk during drafting and disclosure of financial information to capital markets

In line with the key goals and principles listed above, drafting and disclosure of financial information for the purposes of reporting financial information must be conducted in accordance with the following approach:

- Assessment and definition of the materiality of disclosures and headings, subject to quantitative and qualitative factors;
- Identification of relevant disclosures and headings of financial statements, based on risk factors of material distortion and including materiality concerns;
- Identification of relevant assertions for each of these headings and disclosures, including the underlying transactions and events, as well as the processes that support these;
- Periodic review of the consistency of Galp accounting policies in light of accounting principles;
- For the relevant assertions of financial statements, to the level of each relevant heading and disclosure, identification of distortion risks in financial statements must be conducted, attentive to the qualitative factors of risk and probability criteria of these risks. This approach must be applied to business processes, business units, and on a more granular level, to the subsidiaries represented in the headings of the financial statements and disclosures defined as material. The identification process must involve the surveying and

discussion with the person in charge of each of these business processes, of these business units and these subsidiaries;

- Assessment of the risks of fraud and identification of approaches and circumstances in which these may occur.

3.1.4 Internal control during preparation and disclosure of financial information to the capital market

The internal control system for the preparation and disclosure of financial information to the capital market must be designed and function in an integrated manner with the approach to risk specified by Item 3.1.3 of this Manual.

Integration ensures a response to risk at the level of the relevant assertions of the financial statements and must occur through the selection and mapping of control activities that mitigate each risk identified.

The selection and implementation process of control activities typically includes the following methods and approaches:

- Involvement of those in charge of the identification of control activities, including those in charge of business processes and OUs, those in charge of the financial function and those in charge of the information systems that support the relevant business processes, among others.

- Use of matrixes to map out the control activities for the identified risks, either at the business process level or information systems' level;

- Holding of workshops to identify appropriate control activities for each risk;

- Use of walkthroughs in order to understand the business processes, existing controls as well as information systems and the interdependencies thereof;

- Use of examples of duly customized control activities in accordance with good practices;

- Assessment of existing control activities at service providers or implementation of control activities on activities developed or information processed by them, when these impact on financial statements, as well as the respective information support systems;

- Consideration of existing automatic control activities, as well as assessment of the possibility of use thereof, in line with the environment of the information systems in which these are inserted, and consideration of manual control activities;

- Use of a combination of preventative and detective control activities, which better respond to risk factors;

- Identification of incompatible functions and whenever there are constraints that render appropriate segregation of functions impossible and review control activities should be considered at a level of detail that enables errors to be identified.

The control activities for the reporting of financial and non-financial information shall follow the principles presented in this chapter, as well as the specific requirements for the prevention of fraud, segregation of duties, contracting of service providers and use of supporting technologies.

The internal control for the preparation and reporting of financial and non-financial information has also the following particularities:

- **Identification, design and implementation of control activities** – The process areas that contribute to the preparation and disclosure of financial and non-financial information must be reflected in Galp's Process Model. Additionally, the identification, design and implementation of control activities considers the main risks in the preparation of the financial and non-financial information, where the control activities are characterized as to the assertions to which they respond.

- **Relevant service providers for the reporting of financial information** – Without prejudice to the specific requirements for service providers specified by chapter 3.4 of this Manual, the contracting of service providers whose developed activities or processed information could influence Galp's financial statements shall consider the appraisal of the following aspects:

    - Risk of material omission or errors in the preparation and disclosure of financial information, including those related to the handling of assets susceptible to loss or undue appropriation;

    - The interdependence between the activities/tasks and the control activities carried out by the service provider and those carried out by Galp;

    - Control activities carried out by the relevant service provider for the reporting of financial information. In this context, whenever possible, an independent report shall be obtained from the service provider on the design, implementation and effectiveness of the control activities[1];

    - Control activities carried out by Galp to monitor and supervise the control activities carried out by the service provider.

- **Technologies supporting the reporting of financial and non-financial information** – The implementation of specific requirements related to supporting technologies established in chapter 3.5 of this Manual in the context of the reporting of financial and non-financial information is especially relevant at Galp due to the strong technological dependence of the respective procedural areas.

  Recognizing this dependence, Galp classifies the control activities for the reporting of financial and non-financial information as to the use of supporting technologies (application/information system) and identifies the control activities on these technologies.

[1] "*Assurance Reports on Controls at a Service Organization*" pursuant to the appropriate standard (e.g. ISAE3402, SSAE16)

Galp also recognizes the role of the use of productivity software, namely spreadsheet and database applications, in supporting the relevant activities and controls for the reporting of financial and non-financial information, assessing the underlying risks and identifying control activities for validation, monitoring and supervision over the use of these applications.

The control activities on supporting technologies carried out by service providers shall be included, whenever this can be provided, in an independent report on the design, implementation and effectiveness of the control activities.

- **Normative context** – Galp prepares its accounts in conformity with the international financial reporting standards IFRS, endorsed by the European Union. In order to remedy situations of non-existence or insufficiency in the international accounting standards IAS/IFRS or interpretations SIC/IFRIC, Galp has standards and procedures based on best market practices which it applies internally to supplement the IFRS.

  Galp reports its non-financial performance in the Management & Accounts Report in accordance with the requirements and guidelines of the Global Reporting Initiative standards and the guidelines for integrated reporting of the International Integrated Reporting Council, among other internationally recognized references.

  This reporting is made in line with the requirements on disclosure of financial and non-financial information required by Directive 2014/95/EU of the European Parliament and of the Council, of 22 October 2014, transposed by Decree-Law No. 89/2017, of July 8, with respect to the disclosure of financial and non-financial information on diversity and complies with the transposition of this Directive to national law.

  In its Management and Accounts Report, Galp also reports the company's governance system and practice, under the terms of the applicable regulations.

3.1.5 Information and communication

The process of disclosing mandatory financial and non-financial information must be monitored both by the management and audit bodies and by the OUs.

The documents presenting financial and non-financial information to the capital market are prepared by the area responsible for investor relations, based on the information provided by the areas responsible for the planning and control of the business units, by the area responsible for accounting, by the area responsible for corporate planning and control, and by the corporate area responsible for sustainability and governance, according to the attributions established in the organizational standard.

In particular, in what respects the provision of annual and semester accounts, the documents are sent to the board and audit board, which approve them prior to their disclosure.

3.2 Prevention of fraud

One of the focus points of the risk assessment component of the internal control system is the identification and assessment of the risk of fraud, as well as the detection of existing flaws in the control environment and control activities that enable situations of fraud.

The participants in the system shall create fraud prevention controls that consider the following aspects:

- Degree of the estimations in the disclosure of information;
- Common fraud schemes in the sector and industry market;
- Locations where Galp operates;
- Incentives that could motivate fraudulent behaviors;
- Nature of the technology used and capacity to manipulate the information;
- Complexity of relevant or unusual transactions subject to influence of the management;
- Vulnerability of the internal control system to management overlap and/or actions thereby that might circumvent the existing control activities.

The situations of fraud to be prevented are typically presented as follows:

- Fraudulent financial or non-financial reporting – Acts carried out with the intention of misleading the users of the financial or non-financial reports, and that might result in significant omissions or distortion of the information of these reports or even at a level of precision lower than that intended;
- Improper appropriation of assets – Appropriation of Galp's assets, which could result in significant omissions or distortion of the external financial reports' information;
- Illegal acts – Breach of laws or regulations with direct or indirect impact on the financial and non-financial reports.

The participants in the internal control shall also consider the three major factors that are at the core of fraudulent acts:

1. Incentives or pressures – existence of excessive pressure to comply with professional or personal objectives or obligations.

Only for illustration purposes, some examples of situations that might cause fraudulent disclosure of information are:

- threat to financial stability or profitability due to changes in the economy, industry or operating conditions;
- excessive pressure at the governing bodies level to achieve requirements or expectations of the stakeholders;
- existence of information that denotes threats to the financial situation of key personnel at the Company, which are a consequence of the Company's financial performance;
- excessive pressure on personnel to accomplish objectives.

Only for illustration purposes, some examples of situations that might cause improper appropriation of assets are:

- personal commitments or obligations that create pressure on personnel with access to cash or other assets that could be stolen;
- deterioration of the relation between the Company and personnel with access to cash or other assets that could be stolen.

2. Opportunity – existence of circumstances that favor acts of fraud, which influence the method by which the fraud is committed.

Only for illustration purposes, some examples of situations that might be at the root of fraudulent disclosure of information are:

- ineffectiveness or non-existence of supervision of the Management's activity;
- complex or unstable organizational structure;
- flaws in internal control derived from insufficient supervision, high personnel turnover in relevant areas for the reporting of financial information, or shortcomings in information systems.

Only for illustration purposes, some examples of situations that might cause improper appropriation of assets:

- handling of large volumes of cash, other values or assets that are easily convertible into cash;
- handling of inventory items (raw materials or finished product) of small size and high value;
- non-existence of an adequate segregation of duties.

3. Rationalization – self-justification by whoever commits fraud, thus making it acceptable from this person's point of view.

Only for illustration purposes, some examples of situations that could be at the root of fraudulent disclosure of information are:

- failures or ineffectiveness in the communication of the organization's values;
- excessive involvement of managers of non-financial areas in financial matters;
- justification or successive attempted justification of accounting errors based on relevance.

Only for illustration purposes, some examples of situations that could be at the root of improper appropriation of assets are:

- undervaluation of the need to monitor risks related to the improper appropriation of assets;
- undervaluation of the controls on improper appropriation of assets, not complying with the defined controls or not taking the corrective measures for known defects;

- behavior that suggests lack of consideration in relation to the Company or its form of treating its personnel;

- changes in behavior or life style.

Internal control thus plays a fundamental role in the prevention and detection of fraud, eliminating or mitigating its underlying causes, which is demonstrated as follows:

a) Control Environment – The prevention of fraud is mentioned in the Galp Code of Ethics and Conduct and the irregularity reporting channel (available at Galp's official website and its intranet at this link);

b) Risk assessment – Risk analyses aimed at detecting the risk of fraud are conducted by the second line of defense, which are considered in the preparation of internal audit programs present in the third line of defense;

c) Control activities – Control activities aimed at mitigating the risk of fraud shall be designed and implemented, in particular through:

    - Segregation of duties, described in further detail in chapter 4.3 of this Manual;

    - Supervision of the functions responsible for the handling and management of cash or assets susceptible to fraud (at the level of the corporate area responsible for treasury and corporate finance);

    - Design, implementation and conducting of control activities that mitigate the risk of fraud, at the level of business processes in which these may be manifested with a relevant impact on the headings of financial statements, or in a pervasive manner at the level of the financial statements as a whole;

    - Internal rules and procedures for approval of transactions in the process areas of expenses and revenue, as well as relevant, complex or non-usual transactions;

    - Rules and procedures for the custody of assets susceptible to fraud;

    - Reconciliations incident on assets susceptible to fraud;

    - Maintenance procedures of documented information on accounting estimates, on relevant, complex or non-usual transactions and on manual accounting entries and the control activities of review, authorization and approval thereof;

    - Rotation of personnel in positions susceptible to fraud;

    - Verification of candidate backgrounds for roles more susceptible to the committing of fraud, within the scope of Galps' recruitment and mobility processes;

    - Restriction of access to information systems according to duties and responsibilities.

d) Information and communication – existence of a channel for communication of irregularities (opentalk@galp.com) aimed at investigating the facts and timely definition of the

appropriate measures;

e) Monitoring activities – Supervision by the third line of defense of the internal control operation with respect to the risk of fraud.

3.3 Segregation of duties

3.3.1 Objectives

An appropriate segregation of duties shall be assured during the process of definition and implementation of control activities, in particular for transactions that represent a higher risk to the business.

The use of information technologies shall always be considered as it allows managing and monitoring of the duties that need to be segregated, although subject to cost/benefit analysis regarding their use.

The segregation of functions seeks to contribute to:

- Regulatory compliance – When required by law or by regulatory entities;
- Data security and management – When necessary to protect privacy and/or to prevent breach of security;
- Mitigation of the risk of material omission or errors in the reporting of financial information;
- Prevention of fraud – As a core control to prevent the execution of fraudulent actions derived from the undue accumulation of functions;
- Supervision and review of control activities;
- Timely detection of errors that might occur;
- Alignment between the business processes and controls in Galp's information systems. The participants in the internal control system shall:

1. Define the rules of segregation of duties, taking into account, in particular, the need for a correct management of accesses;
2. Identify the duties that shall be segregated in the relevant processes;
3. Ensure prior alignment with the managers responsible for the processes regarding the decisions on segregations of functions;
4. Define mitigation controls to respond to situations where it is not possible to segregate duties (compensatory controls);
5. Conduct periodic appraisals to Galp's personnel on compliance with the applicable standards and regulations.

At Galp, the segregation of duties is based on the principle of limitation of the accumulation of duties along the different stages of a process, namely those which involve distinct responsibilities for each of the following tasks:

- Responsible for the execution;
- Approver;
- Reviewer / Supervisor.

3.3.2 Main examples of conflicts in the preparation and disclosure of financial information

With respect to the preparation and disclosure of financial information, and in accordance with best practices, the segregation of duties shall at least consider the following main conflicts, in order to minimize the potential cover-up of fraud, concealment of errors, embezzlement of assets and concealment of their improper appropriation:

- Verifying, authorizing or approving payments conflicts with the respective preparation;
- Verifying/rectifying, authorizing or signing payments conflicts with the editing of master data on suppliers;
- Authorizing purchases of fixed assets conflicts with the editing of master data on fixed assets;
- Authorizing inventory or expenses related to purchases conflicts with the editing of master data on inventory;
- Editing master data on remuneration records conflicts with the approval of the processing or the authorization of the payment of remunerations;
- Editing master data on accounts receivables conflicts with access to funds/cash;
- Initiating transactions of investment, derivatives or credit conflicts with the recording of the respective transactions;
- Reconciling accounts conflicts with the preparation of deposits;
- Producing internal audits or financial reports conflicts with the review and approval of the financial statements.

3.3.3 Compensatory Controls

In case it is not possible or feasible to assure an adequate segregation of duties, particularly due to lack of sufficient resources, or a limitation on the information systems which precludes the reflection of the segregation of duties in the respective access permissions, compensatory controls shall be implemented.

Some activities, due to their critical nature, might justify the existence of additional risk mitigation measures, such as for example activities that involve the direct handling of cash, bank accounts or other high value assets.

In these circumstances, compensatory controls or alternative forms of risk mitigation shall be identified.

Only for illustration purposes, some examples of preventive compensatory controls are:

- Double authorization – the authorization/approval requires the intervention of two participants. Example: two signatures to authorize bank movements;
- Physical restriction – existence of physical access restrictions that prevent the occurrence of the risk. Example: control of access to zones of movement of goods in warehouses.

Only for illustration purposes, some examples of detective compensatory controls are:

- Independent review – independent review of the operations (for all the operations as a whole or based on sampling) subject to restrictions of segregation of duties. Example: monthly review of the recorded purchase orders;
- Automatic warning – warnings that are issued according to certain overlapping risk circumstances. Example: placement of orders for the purchase and receipt of goods for purchases of a value exceeding a specific amount;
- Report on exceptions – reports displaying the operations in which the principles of segregation of duties were breached, which shall be analyzed and validated. Example: list of alterations to the suppliers' master data.

3.4 Service providers

Prior to the decision to contract third parties for the implementation of processes or controls within Galp's responsibilities, the participants in the internal control system shall identify and assess the specific risks that this decision might bring to Galp.

The assessment and qualification system of Galp suppliers is conducted by the corporate area responsible for acquisitions of Galp's goods and services under the terms of the internal standard that regulates the purchasing process (available at Galp's intranet at this link), as well as the internal procedural standards on the integration of AQS requirements (available at Galp's intranet at this link) and the requirements of privacy and cybersecurity during the contracting process of suppliers (available at Galp's intranet at this link).

In order to determine the actions that shall be implemented to mitigate the identified risks, the importance of the services provided by third parties shall be defined, taking into account the following criteria:

- The relevance of the transactions and/or information processed for Galp's operational, reporting and compliance objectives;
- The nature and complexity of the services provided and the respective standardization level;
- The degree of responsibility granted to the service provider under the contractual terms; and

- The impact of penalties associated to non-compliance of the activity when the compliance with such is of legal or regulatory source.

Contracts between Galp and service providers are drawn up by the corporate area responsible for legal affairs, including elements that provide for and assure the requirements referred to above.

The design, implementation and operation of the controls to be implemented to mitigate the risks identified in this chapter is the responsibility of the corporate procurement area or equivalent area in the OUs, regarding purchasing processes that are not under the responsibility of the former, in coordination with the corporate areas responsible for legal affairs, governance and risk management.

3.5 Supporting technologies

Galp's use of technology requires the design and implementation of controls that mitigate specific associated risks and assure the proper functioning of the control processes, respective standards, procedures or activities supported by this technology.

The supporting technologies shall be used in accordance with the provisions established in standards and procedures.

Only for illustration purposes, supporting technologies include the following elements, to which specific risks are associated:

a) Technological infrastructure and operations – risks in the functioning of the supporting technologies, which depend on computer (e.g. servers), communication or energy resource infrastructures, belonging to Galp or contracted from third parties. The risks related to existing interdependencies between the supporting technologies shall be considered, namely in terms of the transfer of information through interfaces (automatic or manual);

   The contracts in force of fixed or mobile communication services, midrange services (operation, maintenance and management of Galp's servers, as well as the operative systems and databases underlying the various applications) and data center (accommodation of Galp's servers/hosting) define obligations for suppliers and rules for provision of the service (including service level agreements (SLAs) and penalties) that adequately mitigate the risks related to technological infrastructure and operations.

b) Security – security risks of the supporting technologies and information treated by them, in particular failures and accesses or usage that is improper, unauthorized or contrary to the objectives defined by Galp, coming from within or outside Galp, including Cybersecurity risks. Logical and physical security risks shall be considered.

   At Galp, the management of security risks is based on the information security management standard. The data center contracts and the fixed and mobile communication contracts in force at Galp also contribute to the management of the aforesaid risks.

c) Life cycle of the information and communication technologies – risks with impact on the functioning of processes, associated to the identification of business needs, adoption or

acquisition, development, maintenance and discontinuation of the supporting technologies and respective technological infrastructure. The management of this life cycle shall also assure an alignment of the technologies used with the objectives defined by Galp.

The internal standard that regulates the initiatives and projects of Galp's information systems and the sectorial standard on Galp's information architecture that establishes the architectures of integration of data between applications (internal and external) to be implemented embody Galp's concern with this issue. On the other hand, Galp uses "Information System Project Management Guides" (link) that guide and standardize the practices to be followed by information systems project managers in the development of projects.

d) Service providers –risks specific to the provision of services for supporting technologies, supplementing or replacing controls that are incident on the aspects referred to in the previous subparagraphs.

In addition, for the purposes of ICRF a control environment must be maintained over the information systems that support the relevant business processes and OUs for the disclosures and headings of financial statements and the interfaces thereof, following the approach of mapping out the risks associated with the information systems and General IT Controls (CGI) that seek to mitigate these, to be described in Risk and Control Matrixes for Information Systems to be adopted within the scope of the ICRF implementation project.

In order to strengthen the verification of compliance with the requirements of the projects carried out by its suppliers and outsourcers of information systems, Galp may use services provided by third parties (i.e. suppliers that are different from those carrying out the aforesaid projects) to conduct additional tests and to support/ supplement the conduct of acceptance tests, which are always the responsibility of Galp's OUs.

The extension, type and degree of automation of the General IT Controls (CGI) shall take into account the complexity of the technologies involved, the risks to which they are exposed, the use of service providers and the risks associated to the processes which they support.

The design of the CGIs, based on the business requirements defined by the organizational units, their implementation in the system and guarantee of their operation are the responsibility of the corporate area of IT & Digital.

These areas collaborate with the functional area of safety and sustainability with respect to the physical safety of the supporting technologies.

The area of IT & Digital and the CISO (*Chief Information Security Officer*) are also responsible for:

a) Identifying specific risks arising out of the use of certain technologies or from alterations made to the supporting technologies or underlying technological infrastructures, on the assumption that the technological options lie also within their responsibility; and

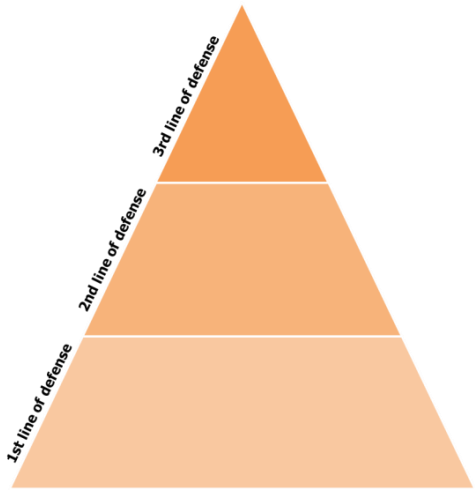
b) Defining the information requirements to be obtained from the organizational units, necessary for the design, implementation and operation of the CGI.

The internal standard relative to the process of recording information system (link) requests and incidents, which defines the necessary steps for the recording and treatment of incidents, assures the obtaining of information by the organizational units.

4. Governance Model

4.1 The three lines of defense of internal control

The governance model for internal control is structured according to the principle of three lines of defense.



The three lines of defense approach enables a consistent liaison between the daily risk management activities, the supervision of risk at the level of the Group's processes and the supervision of strategic and corporate risk.

The design of the defense lines should assure that functional areas and their participants do not accumulate duties in more than one line, except in the case of resources or organizational limitations, a situation in which compensatory controls should be assured.

Without prejudice to the observance of the principle established in the paragraph above, some organizational areas of the corporate center accumulate responsibilities in more than one line of defense, namely:

- The area of IT & Digital essentially performs a role as a first line of defense in being responsible for the identification and management of the risks of information systems and technologies. However, it also performs a role as a second line of defense in being responsible for the supervision and monitoring of the risks related to supporting systems and technologies.

- The area of safety and sustainability basically performs a role in the second line of defense in being responsible for supervising and monitoring their underlying risks. Nevertheless, it also performs a role in the third line of defense as a result of its responsibility in the conduct of independent audits concerning safety and sustainability;

- The accumulation of roles in the second and third line of defense also occurs in the corporate area of legal affairs and governance with respect to the compliance audits.

The definition of three lines of defense is specified in the Risk Management Governance Model, accessible via this (link).

5. Responsibilities Matrix

	External/Statutory Auditor	Audit Board	Board of Directors	Executive Committee	Business units	Information Systems	Financial	HR operations and reward	Purchasing	External communication	Investor Relations	Research and technology	Engineering and project management	Labour relations	Asset management	Insurance	Legal affairs and conflict resolution	Information systems	Tax	Environment, quality, safety and sustainability	Governance and Compliance	Management planning and control	Strategy	Risk management	Risk Management Committee	Sustainability Committee	Corporate EQS Committee	Ethics and Conduct Committee	Environment, quality, safety and sustainability	Internal Audit	Governance and Compliance
					1st Line													2nd Line												3rd Line		
Control Environment																															
Design and implement high level controls		I	A	R	I	I	I	I	I	I	I	I	I	I	I	I	I	C	C	C	C	C	C	C	C	C	C	C	I	I	I
Follow-up and supervision of the internal control system	I	R	A	I																									C	C	C
Promote organisational culture and commitment to internal control		I	A	R	I	I	I	I	I	I	I	I	I	I	I	I	I	C	C	C	C	C	C	C	C	C	C	C	I	I	I
Define reporting lines, competencies and responsibilities of internal control		I	A	R	I	I	I	I	I	I	I	I	I	I	I	I	I	C	C	C	C	C	C	C	C	C	C	C	I	I	I
Attribute responsibilities over internal control		I	A	R	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I
Risk Assessment																															
Identify and analyse risks				A	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R
Definition of risk tolerance levels			A	A	R	R	R	R	R	R	R	R	R	R	R	R	R	C	C	C	C	C	C	C	C	C	C	C			
Assess identified risks					R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R
Monitor risks		I	A	A	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R
Review risks		I	A	A	R	R	R	R	R	R	R	R	R	R	R	R	R	I	I	I	I	I	I	I	I	I	I	I			
Follow-up and supervise the risk management system	I	R	R	C	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	C	I	I	I	C	C	C
Control Activities																															
Design controls in processes				A	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R			
Implement controls in processes				A	R	R	R	R	R	R	R	R	R	R	R	R	R	C	C	C	C	C	C	C	C	C	C	C			
Design general IT controls				A	C	R	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C			
Implement general IT controls				A	I	R	I	I	I	I	I	I	I	I	I	I	I	C	C	C	C	C	C	C	C	C	C	C			
Execute control activities				A	R	R	R	R	R	R	R	R	R	R	R	R	R	C	C	C	C	C	C	C	C	C	C	C			
Develop control activities through standards and procedures					R	R	R	R	R	R	R	R	R	R	R	R	R	C	C	C	A	C	C							I	
Information and Communication																															
Identify and communicate relevant information shortcomings on internal control		I		I	R	R	R	R	R	R	R	R	R	R	R	R	R	A	A	A	A	A	A	A	A	A	A	A	I	I	I
Monitoring																															
Monitor the effectiveness of the implemented controls (Internal Monitoring)					R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R			
Assess the efficacy of internal control and its procedures (Independent Monitoring)	R	I	I	I	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	R	R	R
Review and update the internal control		I			R	R	R	R	R	R	R	R	R	R	R	R	R	A	A	A	A	A	A	A	A	A	A	A	I	I	I
Monitor and follow-up the development of the control system	I	I	I	I														C	C	C	C	C	C	C	C	C	C	C	R	R	R

R Responsible (execution) A Approver C Consulted I Informed

6. Periodic suitability checks

The Internal Control area and the department of Legal Affairs and Governance ensure the periodic monitoring of the present Manual with a view to verify its compliance with the most advanced standards of internal control.

This Manual is periodically subject to suitability verification, within a period of not more than 3 years.

7. Final and transitory provisions

This standard takes effect from the date of its publication.

Potential questions regarding application of this standard must be referred to Galp's Internal Control area.