
# Risk Management Policy

## 1. Purpose

The primary goal of risk management is to ensure that the outcomes of risk-taking activities are consistent with the
Firm's strategies and risk appetite, and that there is an appropriate balance between risk and reward in order to maximize stakeholder value and returns. The Firm's enterprise-wide risk management framework provides the foundation for achieving these goals.

Effective risk management is fundamental to the success of the Firm and is recognized as one of the Firm's strategic priorities. Firm has a strong, disciplined risk management culture where risk management is a responsibility shared by all of the Firm's employees. The Firm's approach to risk management is holistic in nature recognizing the interplay of many factors affecting the overall risk profile and interplay in recognizable risks.

## 2. Scope

The Firm's risk management framework is applied on an enterprise-wide basis and consists of three key elements Risk governance, Risk appetite and Risk management techniques which are explained respectively.

## 3. Definitions:

**CEO:** Chief Executive Officer

**RM:** Risk Manager

**RCSA:** Risk control self-assessments

**CMB:** Capital Markets Board

**AML:** Anti-Money Laundering

**MASAK:** Financial Crimes Investigation Board of Turkey

## 4. Risk Governance

The Firm has in place a risk governance structure, with an active and engaged Board of Directors supported by an experienced senior management team and a risk management function that is independent of the business lines.
Decision-making is highly centralized through the Chief Executive Officer and the Board of Directors.

## 4.1 Board of Directors

The Board of Directors, either directly ensures that decision-making is aligned with the Firm's strategies and risk appetite. The Board receives regular updates on the key risks of the Firm and approves key risk policies, limits, strategies, and risk appetite. It also establishes executive-level lines of authority and responsibility for managing the Firm's risks by prescribing mechanisms to identify, measure, monitor, and manage these risks.

## 4.2 Senior Management

The Risk Management is responsible for risk management under the oversight of the Board and is responsible for the design and application of the Firm's risk management framework.

## 4.3 Risk Manager

The Risk Management Function of the Firm is headed by the RM who provides an independent oversight of the risk management framework and its execution. The core responsibilities of the RM are:

- To work with all functional areas of the Firm and assemble information to build an overall risk profile, ● To prepare, analyse changes/trends and submit the risk profile reports to the Senior Management.
- To function as the custodian of the Firm's Risk Management policies and the risk register;
- Monitor the risk indicators and limits and report breaches to the Senior Management on a monthly basis;
- To facilitate the development of Firm's risk strategy;
- To conduct a risk control self-assessments (RCSA) and present results to the Senior Management on a quarterly basis; and
- To work closely with Internal Audit to plan assessments and discuss concerns about risks in the Firm.

The RM has a direct reporting line to the reports to the Head of Internal Systems from a functional perspective. The RM has direct communication with the Board of Directors regarding concerns where specific risk developments affect or may affect the Firm.

## 4.4 Risk Governance Framework

Our risk management structure is based on the '3 lines of defense' model:

- The First line (Management) is responsible and accountable for identifying, assessing and managing risk;

- The Second line (Risk Management and Compliance) is responsible for defining the Risk Management process and policy framework, providing challenge to the first line on Risk Management activities, assessing risks and reporting to the Board; and
- The Third line (Internal Audit) provides independent assurance to the Board and other key stakeholders over the effectiveness of the systems of controls.

### 4.5 Business/Functional Heads

The CEO and functional heads are responsible for risk taking, related controls and mitigations as set out in this document and other relevant policies and procedures.

The CEO and functional heads are ultimately responsible for:

- **Risk management practices**
  Implementation of sound risk management practices and any resulting impact for losses
- **Risk ownership**
  Ownership of the risks faced in their areas of responsibility
- **Understanding**
  Understanding the risk profile of their area of responsibility and communicating that to the RM as and when changes to the profile are expected or have occurred.
- **Self-Assessment**
  Responsible for the periodic completion of self-assessments of the respective functional area, incoordination with the RM

## 5. Risk Appetite

The Firm’s risk appetite framework governs risk taking activities on an enterprise-wide basis and consists of four components and combines qualitative as well as quantitative terms of reference to guide the Firm in determining the amount and types of risk it wishes to prudently undertake.


## 5.1 Risk Management Principles

Our risk management principles are as follows:

- Promotion of a robust risk culture,
- Accountability for risk by risk takers,
- Avoidance of excessive risk concentrations, and
- Ensuring risks are clearly understood, measured, and managed.

## 5.2 Strategic Principles

These principles provide the qualitative basis on which we pursue our financial objectives and to gauge alignment between new initiatives and our risk appetite. These principles include:

- Placing emphasis on quality and stability of earnings,
- Focusing on core businesses, and
- Leveraging competitive advantages.

## 5.3 Financial Objectives

Focusing on long-term shareholder value allows us to work towards sustainable earnings growth, maintenance of adequate capital in relation to the Firm's risk profile, and availability of financial resources to meet financial obligations on a timely basis.

## 5.4 Risk Appetite Measures

The principles stated in 5.2 above provide objective metrics to gauge risk and articulate the Firm's risk appetite. They provide a link between actual risk-taking activities and the risk management principles, strategic principles and governing financial objectives described above. These measures include Operations and Technology related risks as well as those related to liquidity, capital and credit risks.

Furthermore, the Firm uses the four main strategies to manage various risks

| Response | Definition | Example |
|---|---|---|
| **Risk Acceptance** | Deciding not to change the current situation and accept the risk exposure as it is considered to fall within Firm' risk tolerance. Acceptance entails no specific action, but also does not permit modification of the risk exposure through ongoing review & oversight of the robustness of mitigating controls. | • Inherent to Business as usual |
| **Risk Mitigation** | Reducing the probability of occurrence or impact of a risk (or both) to an acceptable threshold. This is typically achieved through the improvement of existing controls or the addition of new controls, systems or personnel. Mitigation may also include contingency, in the event that the risk still arises (e.g. the business continuity plan). | • Enhanced control environment<br>• Enhanced capital buffer<br>• Enhanced systems or increase personnel |
| **Risk Transfer** | Shifting the threat of impact and/or ownership of response to a third party, through a contractual agreement between the two parties, typically through insurance policies or indemnification or risk transfer pricing. | • Contractual arrangements<br>• Insurance policies<br>• Pricing strategy<br>• Service or process moved to vendor/ 3rd Party |
| **Risk Avoidance** | Eliminating the risk, or protecting the business activities from its impact, e.g. via a restriction or stopping of products or activities | • Complete market exit<br>• Avoid certain clients/products /markets |

## 5.5 Review of Risk Assessment Framework

The Risk manager reviews the risk assessment framework on an annual basis to ensure that it remains relevant in the light of the operating model and historical evidence available as a result of operations over the course of the preceding 12 months. Any changes to the risk management framework are required to be formally approved by the Board of Directors.

## 6. Risk Management Methodology

To ensure that the Firm is able to identify, assess, report and manage risks originating from its activities, it employs the following methodology:

- **Risk Identification** – The RM identifies key risks in relation to commercial operations, all applicable regulations and internal policy requirements.
- **Policy framework** – The Firm has put in place several risk management policies that are described in section 7 below.
- **Risk Assessment** – The RM performs ongoing risk reviews and stress tests to continually assess the risk profile of the Firm and submits reports to the Senior Management on a quarterly basis. The RM also conducts a self-assessment on key risks on an annual basis.
- **Risk Reporting and Escalation** – Results from the reviews are reported to the Senior Management and to the Board.
- **Risk Mitigation** – Results of the risk assessment are discussed at the Board. The RM and other relevant functions recommend mitigating actions and the decisions are documented in the Firm risk register.

## 7. Risk Management Tools

- The RM maintains a risk register which lists and ranks in priority, the risks identified as part of the risk reviews, desk reviews, internal audit and any other internal or external risk assessments.
- In addition, the breaches are reported to the Senior Management on a monthly basis.

### 7.1 Risk Exposure Review Framework

The activity relating to trading of oil products and petrochemicals exposes the Firm to the following risks:

- Counterparty/Credit Risk;
- Market Risk;
- Liquidity and Funding Risk;
- Reputational Risk;

- Legal and Regulatory Risk; and ● Outsourcing Risk

In order to ensure that the Firm maintains a comprehensive view of the above risks and a program for managing these risks, the RM conducts periodic risk reviews in line with the annual risk management plan.

Based on the risks identified, the RM assesses the effectiveness of the various policies and controls in place that are aimed at managing these risks. Furthermore, the RM reviews the Firm's performance against its targets and assesses the impact of adverse economic or industry environment on the performance of the Firm. Results of risk reviews are submitted to the Board of Directors for consideration and action.

## 7.2 Counterparty/Credit Risk

As an organization in the supply and distribution of oil products and petrochemicals, the Firm is exposed to credit risk in relation to its banks, and other buyers/ sellers the Firm deals with.

The Firm does not expose itself to any credit risk in relation to its clients as all transactions require prefunding at a margin.

## 7.3 Market Risk

The Firm does not expose itself to material market risk in trading activities, these activities pricing method and period is back to back. Group III base oil business is also natural hedged buying quotation contains average price of last 4 weeks of Argus price & selling quotation is average price of last 4 weeks and plus one week of Argus pricing period.

## 7.4 Liquidity and Funding Risk

It is imperative for the firm to assess the capacity and ability of its clients provided funding in terms of providing open account terms. Clients are evaluated for their financial health before conducting business and quarterly rechecked for their recent financial situation in order to mitigate liquidity and funding risk. RM is responsible for the collection of essential data and present to risk head for review and approval.

## 7.5 Operational Risk

The Firm has developed an Operational Risk Management (ORM) methodology which ensure that operational risks are appropriately identified and managed with effective controls at an enterprise-wide level. The RM is responsible for the ORM activities of the Firm, which include:

- Conducting operational risk reviews

- Monitoring the operation risk profile of the Firm; and
- Providing period reports to the Board

IT risks are part of operational risk methodology. Risk analysis related to information systems should be performed.
This is repeated once a year or when there are important changes in information systems.
Information related to information systems' technical vulnerability is obtained on time and entity's weakness for these vulnerabilities are evaluated and proper precautions are taken to handle the risks.

Information systems are tested once a year with penetration test by real people or entities that do not have any duty related to performing information security requirements and have national and international certificate about attack & penetration test.

## 7.6 Reputational Risk

Reputational risk is the risk that negative publicity regarding the Firm's conduct or business practices whether true or not, will adversely affect its revenues, operations or customer base, or require costly litigation or other defensive measures.

Reputational risk is managed and controlled through the Firm's Code of Conduct, governance practices, risk management policies, checks to ensure cyber security and confidentiality, transparency of offer documents, and staff training. The Firm considers a broad array of non-economic factors when assessing transactions so that it meets high ethical standards. These factors include the extent, and outcome, of legal and regulatory due diligence pertinent to the transaction, the economic intent of the transaction, the effect of the transaction on the transparency of a customer's financial reporting, the need for customer or public disclosure, conflicts of interest, fairness issues and public perception.

## 7.7 Legal and Regulatory Risk

Legal risk for the Firm is managed by ensuring that each functional unit has a clear understanding of the legal risks to which it is exposed and the regulatory framework within which it operates, in order to ensure compliance with legislation.

All relationships with clients, exchanges, vendors and any other third party are governed by written contracts, agreements, terms and conditions or other appropriate documentation. Such agreements are entered into on arm's length basis (to avoid conflict of interest), are subject to appropriate cross functional review and approved in accordance with the operating limits of authority, including appropriate legal sign off. Where appropriate, such documentation is standardized and is regularly reviewed and updated.

### 7.8 Outsourcing Risk

Outsourcing Risk is the risk associated with services provided by a third party with special focus on cyber-security requirements and controls, non-disclosure agreements (responsibilities, liabilities and remedies thereof) and scope of services, documentation, and extent of risk transfer. Firm's outsourcing risk is effectively managed by the RM of the Firm by identifying all "material" outsourcing contracts and ensuring that the risks associated with such contracts are adequately controlled.

## 8. Risk Review and Reporting

### 9.1 Overview

The RM ensures regular reporting and escalation of the Risk profile to inform the  the Board to enable notification and decision making. The RM performs regular review and reporting of all aspects of the risk management framework and methodology as necessary.

Each functional area is expected to report to the RM as part of the reporting scheduled documented below.

### 9.2 Operational Risk Reporting

#### a. Monthly reporting

Reporting is required from all functional areas to consist of the following data, where available:

- **Risk incidents**: Summary of loss events data and status/reasons of open actions to fix the incident and reduce future exposure of recurrence by each BU along with explanations of missed or delayed target dates to be submitted to the RM. Meetings will be held with each BU, where necessary, to review incidents and to ascertain if any impact to Key Risks/RCSAs in advance of reporting deadlines.

#### b. Quarterly reporting

The RM will provide quarterly reporting to the Board of Directors  consisting of:

- Overall Risk profile and any changes in Key Risk categories
- Provide a status update of any Control improvements for top Key Risks based on materiality

#### c. Annual reporting

Each functional area will work with the RM to complete and report on their RCSAs. The RM will perform a 2nd LOD review and challenge of individual risks and controls as well as provide appropriate aggregate reporting to the Board of Directors. Overall reporting content and granularity will vary to remain appropriate to the needs of the recipient.

Besides monthly, quarterly, and annual reporting, related parties always communicate and evaluate possible risks that may arise with BoD and CEO in daily and weekly trading meetings.

### 9.3 Document Retention

Management information will be retained for a period of six years from the date the final document was published or distributed.

### 9.4 Staff Awareness

The RM will conduct annual training and awareness programs to ensure that employees manage risk appropriately in their day to day business activity, as well as conduct the Risk induction training for all new employees. Training that is provided will reflect the seniority, role, accountability and responsibilities of the individuals for whom it is intended.

## 9. Approval

This procedure is approved by the Board of Directors.

## 10. Disclosure

This procedure is authorized for full disclosure internally within the Company but is designated as 'Confidential' and should not be disclosed to third parties without the prior approval of the Company Directors.

## 11. Review

This procedure will be reviewed and updated on an annual basis and/or when there is a significant change in regulations and/or regulatory requirements and approved by the Board of Director.