# CORPORATE RISK MANAGEMENT POLICY

DCS

Compliance Program

# Corporate Risk Management Policy

## 1 Purpose

The purpose of the DCS Corporate Risk Management Policy is to ensure the early identification of risks that may affect the company's existence, development, and sustainability; to take appropriate measures against such risks; and to increase risk awareness across the organization.

Through this policy, our corporate risk management approach is structured, and a framework is established for systematically and holistically identifying, analyzing, monitoring, and managing all risks.

Within the framework of its corporate risk management methodology, DCS addresses risks in all dimensions, primarily environmental, social, governance, operational, strategic, financial, and compliance areas; regularly evaluates, monitors, and reports high-priority risks.

In this way, resilience against risks is strengthened, contributing to sustainable growth and the company's long-term value-creation capacity.

## 2 Scope

This policy covers all areas of activity and business processes of DCS Dijital Gümrük Hizmetleri A.Ş.

Corporate Risk Management practices are carried out with the participation of the Board of Directors, the Early Risk Detection Committee, the Sustainability and Compliance Directorate, relevant functional managers, and all employees.

The main risk areas covered by the policy are as follows:

- **Strategic and External Risks**

Risks arising from external environmental factors (macroeconomic developments, geopolitical events, legal changes, natural disasters, and other external factors) that may affect the company's ability to achieve its long-term strategic goals, competitive power, and corporate reputation

- **Financial Risks**

Risks that may affect the company's financial structure, income–expense balance, and financial sustainability.

- **Operational Risks**

Risks arising from legislation, internal, and external operations.

- **Software, Systems, and Information Security Risks**

Risks to IT infrastructure, data security, and the continuity of information systems.

- **Legal Risks**

Risks of liabilities and sanctions arising from non-compliance with legislation and legal proceedings.

- **Third-Party Relationships and Supplier Risks / Human Resources and Human Rights Risks**

(Risks related to HR management, employee and human rights, decent work conditions, and procurement processes)

- **ESG and Compliance Risks**

Risks arising from environmental, social, and governance issues, and compliance with regulatory requirements.

- **Anti-Corruption and Ethics Risks**

Risks related to unethical conduct, corruption, and conflicts of interest.

These risks are regularly assessed and managed by the Early Detection of Risk Committee established in accordance with Article 378 of the Turkish Commercial Code.

The Committee monitors the risks identified under the above headings and determines actions to be taken, reporting them to the Board of Directors.

This structure ensures that the Corporate Risk Management Policy aligns with the UN Global Compact Principles and the governance, transparency, and sustainability requirements under GRI Standards (2021), supporting best practice standards.

# 3 Definitions

**Corporate Risk Management (CRM):** The systematic process of identifying, assessing, monitoring, and managing uncertainties or events that may hinder or turn into opportunities for achieving the company's strategic objectives.

**Risk:** The probability of an event or condition occurring and its potential impact on the company's existence, activities, financial structure, reputation, and objectives.

**Risk Appetite:** The level of risk a company is willing to accept in pursuit of its objectives.

**Early Detection of Risk Committee:** A board-level committee established in accordance with Article 378 of the Turkish Commercial Code, responsible for monitoring, evaluating, and managing risks that may affect the company's existence, development, and sustainability.

**Internal Control:** A set of control mechanisms designed to ensure compliance with legislation, internal regulations, and objectives; reduce error, fraud, and abuse risks; and increase the accuracy and reliability of financial and operational reporting.

**Three Lines of Defense:** A structure comprising three defense layers with distinct roles and levels of independence to enhance the effectiveness of risk management and internal control:

- **First Line of Defense – Operational Processes:** Business units responsible for day-to-day activities.
- **Second Line of Defense – Oversight and Compliance:** Risk, compliance, and control functions such as the Early Risk Detection Committee.
- **Third Line of Defense – Internal Audit:** Independent and objective audit activities carried out by internal audit.

# 4 Policy Statements

## 4.1 Policy Commitment

As the Board of Directors of DCS Dijital Gümrük Hizmetleri A.Ş., we declare our commitment to the implementation of an effective, transparent, and sustainable corporate risk management system and to its continuous enhancement and improvement.

The ultimate priority of the Corporate Risk Management Policy is the protection of human rights, the welfare and rights of employees, the protection of the environment and natural resources, the sustainable safeguarding of the company's assets and reputation, and the creation of long-term value for all stakeholders.

Our risk management practices will be continuously reviewed and developed in line with relevant legislation, international best practice standards (GRI, UNGC, SDGs, etc.), and our company's ethical values.

All our employees, business partners, and managers are expected to act in accordance with this policy and to support the corporate risk management culture.

## 4.2 Core Principles

The following core principles are fundamental to the implementation of the DCS Corporate Risk Management Policy:

**Proactive Approach:** Early identification of risks and the adoption of preventive approaches are essential. Potential threats and opportunities are assessed proactively.

**Holistic and Systematic Management:** All risks are addressed and managed with a holistic and systematic approach across the company.

**Sustainability and Long-Term Perspective:** Risk management processes are conducted in line with sustainable growth objectives and the understanding of long-term value creation.
Transparency and Accountability: Transparency, open communication, and accountability principles are adhered to in the management of risks.

**Compliance and Ethical Conduct:** Full compliance with all applicable laws, regulations, and internal company policies and procedures is ensured; ethical values are observed.

**Inclusive and Pervasive Culture:** Risk management is not limited to specific units but is broadened with the contribution of all employees and business partners, becoming an integral part of corporate culture.

**Continuous Improvement:** The effectiveness of risk management processes is regularly reviewed and continuously improved based on experience and changing circumstances.

## 4.3. Implementation and Monitoring

The Corporate Risk Management process at DCS consists of the following main stages:

- Identification of risks,
- Analysis, measurement, and prioritization of identified risks,
- Development and implementation of appropriate management strategies and action plans for priority risks,
- Regular monitoring, assessment, and reporting of risks.

To ensure the effectiveness of this process, the Board of Directors establishes the necessary organizational structure, defines the operating principles of the processes, and reviews them regularly.

The details of the execution and monitoring of risk management practices are defined in the Risk Management Regulation and relevant internal regulations.

The effectiveness of the risk management process is continuously reviewed and further developed in line with changing internal and external conditions.

# 5 Responsibilities

Corporate Risk Management at DCS is carried out based on the three lines of defense model within the following responsibility framework:

**Board of Directors:**

- Has ultimate responsibility for establishing, ensuring the effective operation of, and monitoring the corporate risk management system.
- Oversees risk assessment activities through the Early Detection of Risk Committee.
- Reviews risk management practices and results at least once a year and ensures necessary improvements are made.

**Early Detection of Risk Committee:**

- On behalf of the Board of Directors, ensures monitoring, assessment, and reporting of all identified risk areas (including Human Rights, Employee Rights and Decent Work, Environment, and Anti-Corruption).

- Guides the development and implementation of risk management strategies.
- Monitors the effectiveness of the risk management process and provides recommendations for improvement.

**Sustainability and Compliance Directorate:**

- Coordinates and implements corporate risk management processes on behalf of the Early Detection of Risk Committee.
- Carries out the identification, monitoring, assessment, and reporting of risks; presents necessary data and analyses to the Committee.
- Is responsible for raising awareness of risk management, disseminating the corporate risk culture, and coordinating related training activities.

**Senior Management:**

- Coordinates the implementation of corporate risk management processes.
- Responsible for identifying, analyzing, prioritizing risks, and preparing and implementing appropriate action plans.
- Ensures that risk management practices are disseminated across all units.

**Relevant Department Managers:**

- Responsible for identifying, monitoring, and reporting risks in their respective areas of responsibility.
- Ensure the effective implementation of preventive and corrective actions.

**All Employees:**

- Act with risk awareness within their areas of duty and responsibility.
- Report identified potential risks to their managers or relevant units in a timely manner.
- Actively participate in risk management processes and comply with established internal regulations.

This approach aims to ensure that the risk management process is implemented effectively and widely at every level of the organization.

## 6 Training and Awareness

DCS conducts regular training and awareness activities for all employees to enhance the effectiveness of the corporate risk management system.

The main objectives of these training programs are as follows:

- Understanding risk management principles,
- Internalizing the scope of the policy and related processes,
- Developing employees' ability to identify, report, and manage risks within their areas of responsibility

.

New employees are provided with risk management training during the orientation process, while annual refresher training is planned and delivered for current employees.

In addition, periodic information activities and internal communication materials are used to continuously support risk management awareness throughout the organization.

These training and awareness activities are coordinated by the Sustainability and Compliance Directorate in cooperation with Human Resources.

## 7 Monitoring and Compliance

DCS regularly conducts audit and evaluation activities to ensure compliance with this policy and identify potential risk areas

The effectiveness of corporate risk management practices is continuously monitored through internal audit, external audit, and internal control mechanisms.

Assessment results regarding this policy are reported to relevant management levels as part of regular compliance reporting.

Findings and feedback form the basis for determining improvement actions and further developing corporate risk management processes.

## 8 Breach of Policy

DCS considers compliance with the Corporate Risk Management Policy a binding obligation for all employees across the organization.

Deliberate or negligent violation of this policy; disregard of its provisions, failure to apply them, or failure to report risks in a timely manner constitutes a breach of internal regulations.

Employees who act contrary to the policy will be subject to necessary administrative and/or legal actions in accordance with internal disciplinary procedures. Such actions may include warning, reprimand, reassignment, termination of employment, and, where necessary, reporting to the competent legal authorities.

DCS expects all employees to fully comply with the obligations under this policy and will implement the relevant measures without any discrimination where necessary.

## 9 Reporting and Whistleblower Protection

DCS provides the necessary mechanisms for employees, suppliers, and other stakeholders to report concerns related to violations of this Policy confidentially and without fear of retaliation. Employees must report any person engaged in such behavior, even if it involves their managers or superiors.

Reports can be made via the email address: etik@dcscustoms.com.tr.

DCS grants its employees the right to submit reports without revealing their identity and treats anonymous reports with the same seriousness. All reports are handled in accordance with the **Whistleblowing, Consultation**, and **Anti-Retaliation Policy**, ensuring confidentiality and taking measures to protect the whistleblower from retaliation.

DCS is committed to investigating all reports of violations of this policy promptly and fairly. If a violation is confirmed, the company will take appropriate corrective measures and work to remedy any resulting damage.

## 10 Review and Revision

This policy is reviewed at least once a year from the date of entry into force for compliance with local and international laws.

The review process is carried out under the coordination of the Early Risk Detection Committee and the Sustainability and Compliance Directorate.

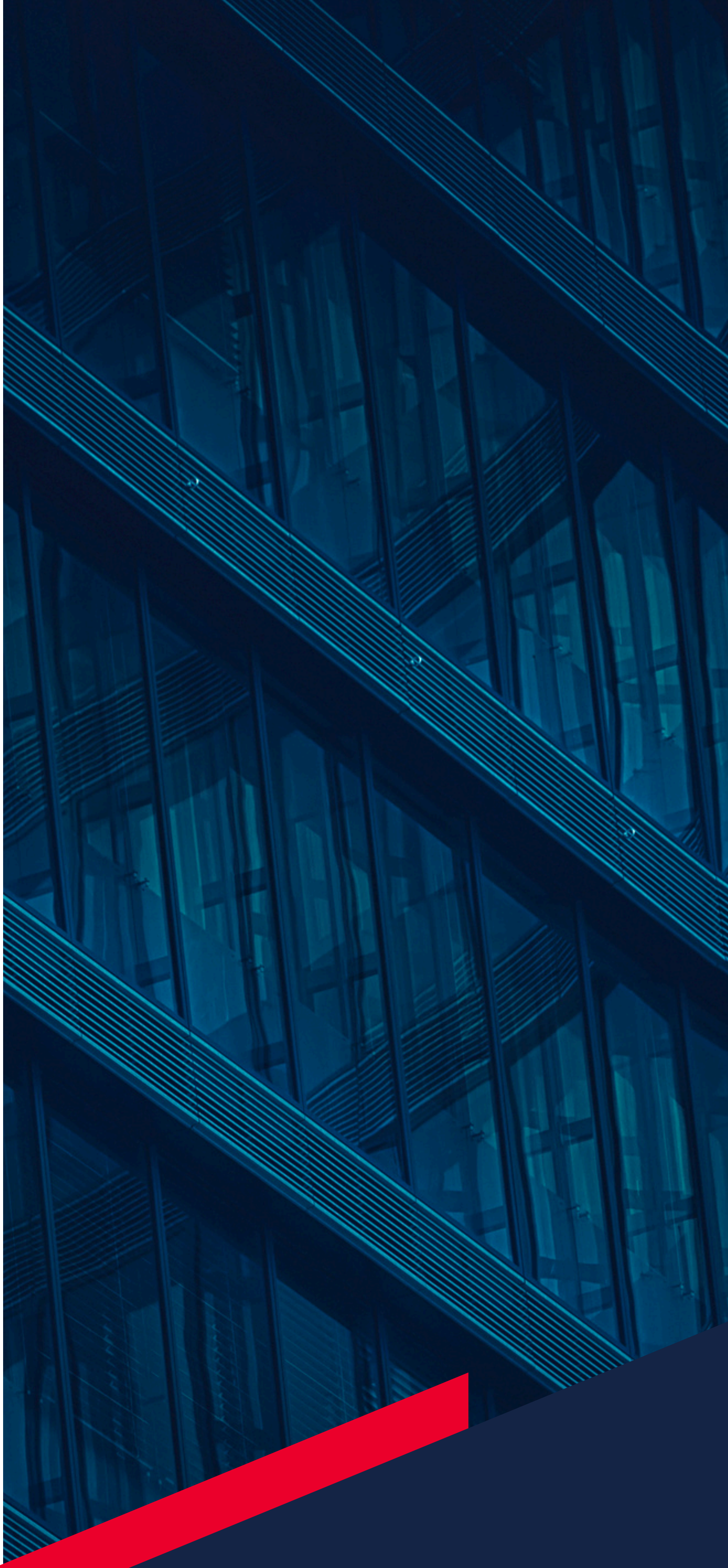
The policy is updated, as necessary, to reflect changes in applicable laws and regulations as well as in DCS business practices.

Other changes and revisions are prepared as justified amendment proposals based on relevant risk assessments, submitted for the approval of the Board of Directors, and, if approved, put into effect.

The current version of the policy is published through the Document Management System, made accessible to all relevant parties, and formally recorded.

DCS

# Compliance Program



www.dcscustoms.com.tr