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, assessment and monitoring of risks that may affect the Company's existence, development and sustainability, and the implementation of necessary measures; and to support the effective implementation of the corporate risk management approach across the Company.

This Policy aims to structure our corporate risk management approach and to establish the framework for addressing risks and opportunities through a systematic, holistic and risk-oriented approach.

DCS considers the corporate risk management approach as one of the fundamental governance elements that support strategic planning, decision-making processes, sustainable growth, corporate resilience and long-term value creation.

Within the scope of the corporate risk management approach, not only elements that constitute threats, but also developments that may create strategic opportunities for the Company are assessed.

In this way, it is aimed to increase the Company's resilience against risks, support corporate sustainability and create long-term value for all stakeholders.

2 Scope

This Policy applies to all areas of activity, business processes, and managerial and operational activities of DCS Dijital Gümrük Hizmetleri A.Ş.

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

The Internal Audit Function independently and objectively assesses the effectiveness and adequacy of risk management, internal control, and governance processes and provides reasonable assurance regarding these processes.

Enterprise risk management processes are regularly assessed, monitored, and reported under the coordination of the Early Detection of Risk Committee established pursuant to Article 378 of the Turkish Commercial Code No. 6102.

The Risk Working Group contributes to the monitoring and assessment of risks and opportunities that may affect the Company's activities and to the development of necessary recommendations for action; it submits the required reports to the Early Detection of Risk Committee and the relevant levels of management.

Within the scope of enterprise risk management practices, all risk areas that may affect the Company's activities are assessed through a holistic approach, including strategic, operational, financial, environmental, social, governance, information security, artificial intelligence and technology, ethics, compliance, human rights, supply chain, business continuity, and reputational risks.

Details regarding risk categories, risk assessment methodologies, and implementation principles are defined within the framework of the relevant regulations, procedures, risk inventory, and other internal rules and arrangements.

In line with the principles of corporate governance, transparency, sustainability, and corporate resilience, this Policy aims to support the Company's risk management approach in alignment with national and international good practice standards.

3 Definitions

Corporate Risk Management (CRM): The process of systematically identifying, assessing, monitoring and managing uncertainties and events that may prevent the Company from achieving its strategic objectives or that may be transformed into opportunities.

Risk: The probability of occurrence of a specific event or condition and the potential impact that such situation may have on the Company's existence, activities, financial structure, reputation and objectives.

Opportunity: Refers to developments and circumstances that may contribute positively to the Company's strategic objectives, sustainable growth or operational effectiveness.

Risk Appetite: The level of risk that the Company is willing to accept in order to achieve its objectives.

Risk Tolerance: The level of deviation and exposure that the Company may accept within the framework of the determined risk appetite.

Risk Capacity: The Company's capacity to withstand and manage the risks to which it may be exposed within the framework of its financial, operational, legal and organizational structure.

Risk Portfolio: The overall set of risks to which the Company is exposed or may be exposed, which are systematically identified, classified, prioritized and monitored.

Residual Risk: The level of risk that remains after existing controls and measures regarding risks have been implemented.

Risk Response: The methods and actions determined for accepting, mitigating, controlling, transferring or avoiding risks.

Early Detection of Risk Committee: The committee affiliated with the Board of Directors, established in accordance with Article 378 of the Turkish Commercial Code and tasked with monitoring and assessing risks that may affect the Company's existence, development and sustainability and reporting them to the Board of Directors.

Internal Audit: An independent and objective assurance and consulting activity carried out to evaluate the effectiveness of the Company's activities and the adequacy and effectiveness of risk management, internal control and governance processes.

Internal Control: The overall set of systematic control mechanisms established to ensure that the Company's activities are carried out in compliance with legislation, internal arrangements and determined objectives; to reduce the risks of error, irregularity and misconduct; and to increase the accuracy and reliability of financial and operational reporting.

Three Lines of Defense: The control model consisting of operational units responsible for the management of risks, risk oversight and compliance functions, and internal audit activities providing independent assurance, in order to support the effectiveness of the corporate risk management and internal control system.

First Line of Defense: Operational units and process owners responsible for managing risks and carrying out daily control activities.

Second Line of Defense: Structures that ensure the monitoring and assessment of risks and the support of relevant processes through risk management, compliance, internal control and similar oversight functions.

Third Line of Defense: The Internal Audit Function, which evaluates the effectiveness of risk management, internal control and governance processes from an independent and objective perspective.

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 establishment, implementation, regular review of effectiveness and continuous improvement of an effective, transparent, sustainable and risk-oriented corporate risk management system.

It is essential that the corporate risk management approach be implemented as an integral part of the Company's strategic planning, decision-making, operations management and governance processes.

The timely identification, assessment and monitoring of risks and opportunities that may affect the Company's activities, and their management through appropriate actions, are supported.

Our risk management practices are regularly reviewed and continuously improved in line with applicable legislation, internal Company arrangements, ethical principles and international good practice standards.

The dissemination of the corporate risk management culture across the Company, the support of this approach by all employees, managers and relevant stakeholders, and acting with risk awareness within the scope of their areas of responsibility are expected.

4.2. Fundamental Principles

The following fundamental principles are taken as basis in the implementation of the DCS Corporate Risk Management approach:

Risk-Oriented Approach
It is essential that risks and opportunities that may affect the Company's activities are identified, assessed and monitored at an early stage and managed through appropriate actions.

Holistic and Systematic Management
Corporate risk management processes are carried out across the Company through a holistic and systematic approach, including strategic, operational, financial, compliance, information security, reputation, ESG and sustainability dimensions.

Management of Artificial Intelligence and Technology Risks
Risks that may arise from the development, use, and management of artificial intelligence technologies are assessed within the framework of the enterprise risk management approach. **The Responsible Artificial Intelligence Policy** and other relevant corporate regulations shall serve as the basis for the management of these risks.

Corporate Governance and Accountability
Duties, authorities and responsibilities in risk management processes are clearly defined; actions are taken in line with the principles of transparency, accountability and effective governance.

Integration into Decision-Making Processes
It is essential that the risk management approach be implemented as an integral part of strategic planning, investment, operations, resource management and decision-making processes.

Risk Culture and Participation
It is encouraged that the risk management approach becomes a part of the Company culture, is supported by all employees and relevant stakeholders, and that persons act with risk awareness within the scope of their areas of responsibility.

Continuous Monitoring and Improvement
Risk management processes are regularly reviewed in line with changing internal and external conditions and are continuously improved in line with the results, feedback and experiences obtained.

Independent Oversight and Assurance
The effectiveness of risk management, internal control and governance processes is evaluated from an independent and objective perspective through the relevant oversight mechanisms and the Internal Audit Function.

4.3. Implementation and Monitoring

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

- Identification of risks,
- Systematic classification of risks, creation and keeping up to date of the risk inventory and risk portfolio,
- Analysis, assessment and prioritization of risks,
- Creation and implementation of appropriate management strategies and action plans for priority risks,
- Monitoring and assessment of the implementation status of action plans,
- Regular monitoring and reporting of risks.

In order to ensure that this process is carried out effectively, the necessary organizational structure is established by the Board of Directors, the operating principles of the processes are determined, and practices are regularly reviewed.

Details regarding the execution and monitoring of risk management practices are defined within the scope of the relevant regulations, procedures and other internal arrangements.

The effectiveness of risk management processes is regularly assessed and continuously improved in line with changing internal and external conditions, legislative amendments, operational developments and findings obtained.

5 Responsibilities

Corporate Risk Management at DCS is carried out on the basis of the Three Lines of Defense model, within the framework of the duties and responsibilities set out below.

5.1 Board of Directors

- It is ultimately responsible for establishing the corporate risk management system, ensuring its effective operation and monitoring it.
- It oversees the determination of the Company's risk appetite and risk management approach.
- It oversees and evaluates risk management processes through the Early Detection of Risk Committee.
- It regularly reviews risk management practices and results and ensures that necessary improvements are made.

5.2 Early Detection of Risk Committee

- On behalf of the Board of Directors, it oversees the monitoring, assessment and reporting of all determined risk areas.
- It carries out assessments regarding risk management strategies and practices and develops recommendations.
- It regularly monitors developments regarding the Company's significant risks and carries out necessary assessments.
- It monitors the effectiveness of risk management processes and provides opinions and recommendations to the Board of Directors on matters deemed necessary.

5.3 Internal Audit

- It evaluates the effectiveness of risk management, internal control and governance processes from an independent and objective perspective.
- It provides findings, assessments and recommendations regarding risk management processes.
- It provides independent assurance regarding risk management practices.

5.4 Sustainability and Compliance Directorate

- On behalf of the Early Detection of Risk Committee, it coordinates and carries out the implementation of corporate risk management processes.
- It carries out activities for the identification, assessment, monitoring and reporting of risks; and presents the necessary data and analyses to the Committee.
- It ensures the coordination of the risk inventory, risk assessment activities and related reporting.
- It is responsible for increasing risk management awareness, disseminating the corporate risk culture and coordinating related training activities.

5.5 Senior Management

- It supports the implementation of corporate risk management processes and ensures coordination among the relevant units.
- It oversees the processes of analyzing and prioritizing risks and creating appropriate action plans.
- It supports the effective implementation of risk management practices across the organization.

5.6 Relevant Department Managers

- They are responsible for identifying, monitoring and reporting risks in the business areas for which they are responsible.
- They ensure the effective implementation of preventive and corrective actions.
- They support the effective implementation of control activities in the areas for which they are responsible.

5.7 All Employees

- They act with risk awareness within their own duties and areas of responsibility.
- They timely report potential risks they identify to their managers or the relevant units.
- They actively participate in risk management processes and act in accordance with the relevant internal arrangements.

With this approach, it is aimed to implement the risk management process effectively, in a coordinated manner and sustainably at all levels of the organization.

6 Training and Awareness

DCS carries out training and awareness activities for employees in order to increase the effectiveness of the corporate risk management system and support the dissemination of risk culture across the organization.

The main objectives of these training and awareness activities are as follows:

- Understanding the risk management approach and fundamental principles,
- Internalizing the processes related to the scope of the Policy,
- Developing employees' competencies to identify, assess and report risks associated with their areas of duty and to contribute to appropriate action processes.

Risk management awareness training is provided to newly hired employees as part of the orientation process. For existing employees, regular update and awareness trainings are planned and implemented in line with needs.

The dissemination of the corporate risk culture across the organization is supported through periodic information activities, internal communication efforts and awareness materials.

Training and awareness activities are carried out under the coordination of the Sustainability and Compliance Directorate, in cooperation with Human Resources and the relevant units.

7 Monitoring and Compliance

DCS carries out regular monitoring, control and assessment activities in order to ensure compliance with this Policy and to evaluate the effectiveness of corporate risk management processes.

The effectiveness of corporate risk management practices is reviewed and monitored through internal control, compliance, internal audit and, where deemed necessary, external assessment mechanisms.

The results of assessment, monitoring and review activities carried out within the scope of this Policy are regularly reported to the relevant management levels.

The findings, feedback and assessment results obtained are taken into consideration for the purpose of determining improvement actions, developing risk management processes and increasing corporate resilience.

The relevant units are responsible for creating and implementing the necessary actions regarding identified nonconformities, deficiencies and areas for improvement. The implementation status of the relevant actions is monitored and evaluated where deemed necessary.

8 Non-Compliance with the Policy

DCS considers compliance with the Corporate Risk Management Policy as part of corporate responsibility for all employees, managers and relevant stakeholders.

The intentional or negligent breach of this Policy; situations such as disregard or non-implementation of policy provisions, failure to report risks in a timely manner or failure to effectively support risk management processes may constitute a breach of internal Company arrangements.

In the event that conduct contrary to the Policy is identified, necessary administrative and/or legal actions may be applied against the relevant person or employees within the framework of internal Company arrangements, disciplinary processes and applicable legislation.

DCS expects all employees to fulfill their responsibilities under this Policy and supports the effective implementation of the corporate risk management culture across the organization.

9 Reporting and Whistleblower Protection

Employees are obliged to report any nonconformity, breach or suspicious situation they encounter, regardless of the title, duty or position of the persons engaging in the relevant conduct.

Reports may be submitted via the e-mail address etik@dcscustoms.com.tr.

DCS allows employees to submit reports without disclosing their identities and evaluates anonymous reports with the same sensitivity and seriousness. All reports made are handled by observing the principle of confidentiality within the scope of the Reporting, Consultation and Prevention of Retaliation Policy, and the necessary measures are implemented to protect reporting persons against retaliation.

DCS undertakes to ensure that all reports regarding the breach of this Policy are assessed impartially, fairly and within a reasonable period of time. If, as a result of the examinations and assessments carried out, a breach is identified, necessary corrective and preventive actions are implemented.

10 Review and Revision

This Policy is reviewed at least once a year, taking into account applicable legislation, international good practice standards, corporate needs and implementation results.

The review process is carried out under the oversight of the Early Detection of Risk Committee and under the coordination of the Sustainability and Compliance Directorate. The Internal Audit Function may provide independent assessment and opinions regarding the processes if needed.

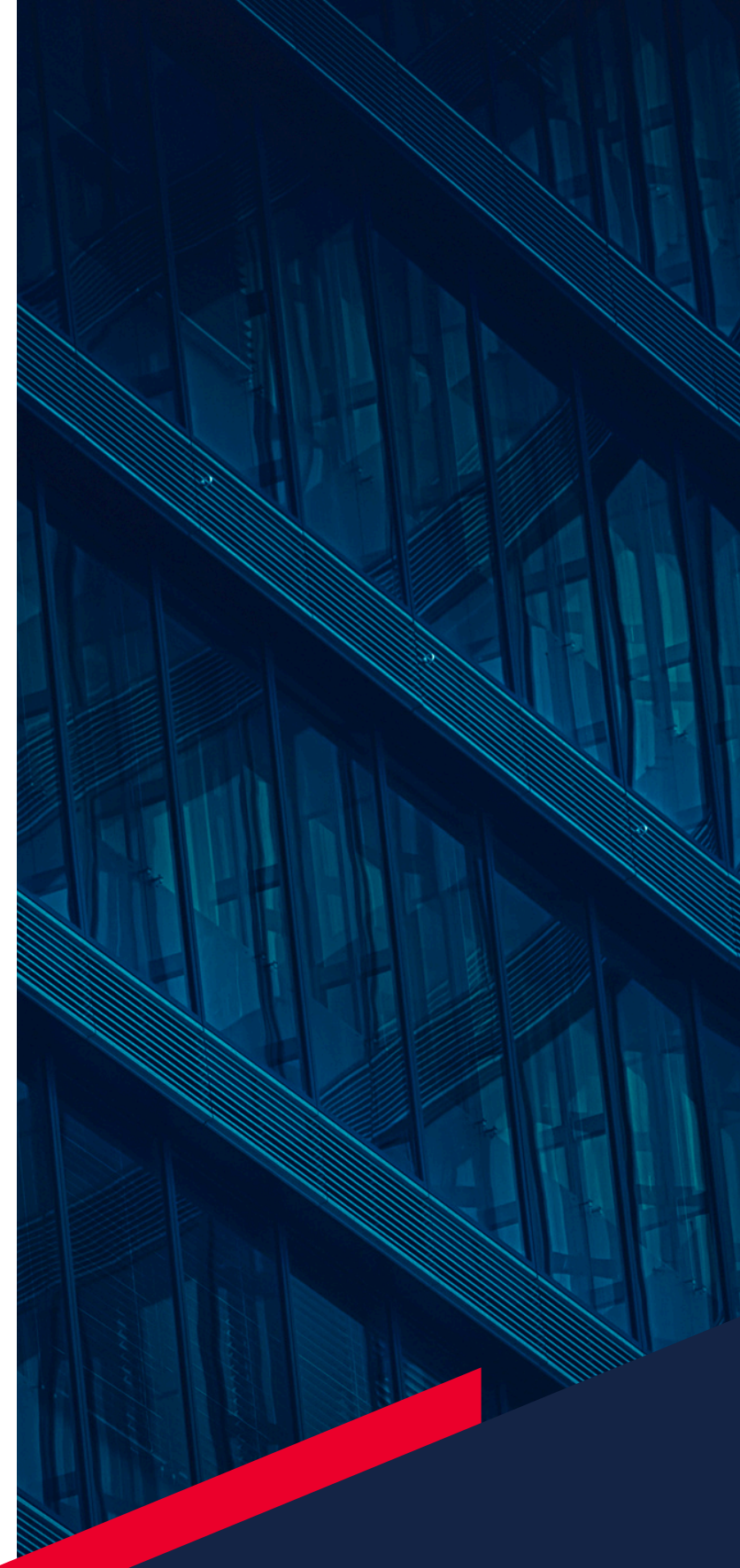
The Policy may be updated where necessary in line with changes in applicable legislation, corporate structure, activity processes, organizational needs and risk assessment results.

Changes and revisions to be made to the Policy are submitted to the approval of the Board of Directors together with reasoned assessments and recommendations, and enter into force if approved.

The current Policy text is published through the Document Management System and recorded in a manner accessible to the relevant parties.

DCS

Compliance Program



www.dcscustoms.com.tr