RISK POLICY

1. PURPOSE AND SCOPE

The purpose of this Policy is to explain the general guidelines and management principles of the risk management strategy and the risk management framework of Aydem Yenilenebilir Enerji A.Ş. This policy covers general guidelines and management principles regarding the risk management strategy and the risk management framework.

The provisions of this Policy apply to all employees of Aydem Yenilenebilir Enerji A.Ş.

2. LEGAL BASIS

The Risk Management Policy has been developed in accordance with regulations of the Capital Markets Board ("**CMB**"), other legal regulations, and relevant provisions of the Company's Articles of Association ("**Articles of Association**"), including Capital Market Law No. 6362, Turkish Commercial Code No. 6102, "Corporate Governance Communiqué" ("**Communiqué**") Numbered II-17.1, and corporate governance principles set out in its annexes.

3. RESPONSIBILITY

The Board of Directors is responsible for the establishment of annual plans and policies through Early Risk Detection Committee. Company's manager / expert responsible for risk management or legal and compliance officer is responsible for the preparation of the supportive documentation, and for implementation of risk management activities in parallel with such plans and policies.

4. DEFINITIONS

In this Policy:

Company means Aydem Yenilenebilir Enerji A.Ş.;

Board of Directors means the Board of Directors of Aydem Yenilenebilir Enerji A.Ş.;

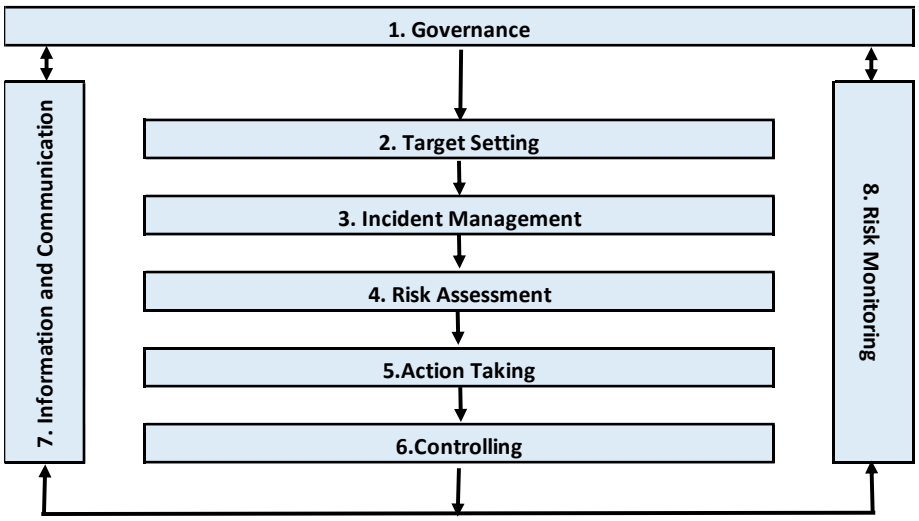
Early Risk Detection Committee means the committee established for the early detection of the risk, which reports to the Board of Directors, and this committee shall hereinafter to be referred to as the "Committee".

5. RISK MANAGEMENT STRATEGY

Company Risk Management is:

- To immediately identify, measure, manage, report and monitor the risks affecting the realization of the strategic, operational and financial goals of the Company;
- To construct the Company's risk profile in line with the Company's risk appetite to respond to new threats and opportunities in order to take maximum advantage out of the returns;
- To ensure that risk management is effective in decision making processes in line with the Company's strategy;

- To protect the Company's capital in line with Company's risk appetite;
- To get an optimal risk return profile by effectively allocating the capital of the company;
- To ensure the sustainable financial performance, income and competitive power to the Company,
- To support decision making processes by providing consistent, reliable and timely risk information;
- To protect the Company's reputation by enhancing the Company's core values, increasing risk awareness level, and developing a strong culture of disciplined and consciously risk taking.



5.1.Governance

The effective structuring and implementation of governance is the basis of all other components of risk management.

5.1.1. Lines of Defence

5.1.1.1. First Line of Defence

Business Units' Managers are primary responsible for effectively controlling of the risks posed by their activities **("first line of defence").** The parties in the first line of defence are responsible for implementation of risk regulations, principles and procedures built by the parties in the second line of defence. Below are the examples of the main activities of the parties in the first line of defence:

- To conduct risk assessments and to plan and take necessary actions to manage risks so that only acceptable risk levels will remain.
- To implement the issues which have stated in Risk Management policies, regulations and procedures, processes.
- To ensure that key controls are effective.

5.1.1.2. Second Line of Defence

The Company's manager / expert responsible for the risk management or legal and compliance officer ("second line of defence") supports the parties in the first line of defence regarding risk management activities.

Below are examples of the main activities of the parties in the second line of defence:

o To act in line with the principles, procedures and regulations regarding Risk Management and to observe related managements' implementation,

o To make suggestions for the improvement of controls,

o To observe the effectiveness of the controls,

o To analyze and report control failures and weaknesses,

o To conduct methodologies related with risk management,

o To ensure that risk management activities are conducted,

o To support definition of the key controls,

o To support business units for risk identification which they are exposed, to monitor the risks,

o To determine the action owners to mitigate risks,

o To report the issues exceed risk appetite, report issues to escalate if it is necessary.

5.1.1.3. Third Line of Defence

Internal Audit acts as a **third line of defence**, therefore Internal Audit ensures independent assurance about the effectiveness of the Risk Management system.

5.1.2. Early Risk Detection Committee

Early Risk Detection Committee has been established to be in charge of and be authorized within the framework of the regulations, including the corporate governance principles in the Turkish Commercial Code No. 6102, the regulations of the Capital Markets Board ("**CMB**"), and the relevant provisions of the Company's Articles of Association. Early Risk Detection Committee operates with the aim of managing risks through early detection of all kinds of strategic, operational, financial and other risks that may jeopardise the existence, development and continuity of the Company, and of implementation of appropriate risk management strategies.

5.1.2.1. Responsibility

Early Risk Detection Committee's duties and authorizations are listed below:

a. To establish a Corporate Risk Management approach throughout the company and efficient risk management framework;

b. To prepare and submit suggestions for the establishment of risk management systems, the establishment of organizational infrastructures related to risk management within the Company and the enhancement of functionality;

c. To submit opinions to the Board of Directors for the establishment of internal control systems, including the processes of risk management and information systems, which can minimize the risks that may affect the stakeholders of the Company, especially the shareholders;

d. To perform studies to determine Risk Management Strategies, Policies, related standards and methodologies used in managing risks throughout the Company and to submit them to the approval of the Board of Directors;

e. To perform studies to define policies that explain the risk appetite of the Company and that correspond with the strategic plans and targets approved by the Board of Directors, and to submit such studies to the Board of Directors for approval;

f. To perform studies within the scope of risk appetite in order to create a proposal related to risk indicators and their thresholds and to submit them to the Board of Directors for approval; to monitor the risk indicators and submit the results, evaluations and recommendations to the Board of Directors when necessary;

g. To ensure that Company's processes and operations are conducted in line with the Company's strategies and risk appetite;

h. To adequately inform the Board of Directors about the risks of Company's activities, including strategy management, capital and resource allocation, risk profile, risk appetite, business activities, financial performance and reputation; to make suggestions if it is necessary;

i. To maintain internal processes, including performing stress tests, where appropriate, to ensure that capital and liquidity levels and asset-liability structure are in accordance with the company's normal and stressful conditions;

j. To integrate risk management and internal control systems into the Company's corporate governance and business processes;

k. To identify, assess and monitor the existing and potential risk factors that may affect the achievement of the Company's goals within the framework of corporate risk management and to determine the principles regarding the management of relevant risks in accordance with the Company's risk appetite and to use them in decision making processes;

l. To evaluate and approve risk studies throughout the Company; to inform the Board of Directors, and to provide suggestions when necessary;

m. To evaluate and recommend risk management strategies for risks that will be accepted, managed, or partially/fully mitigated in the Company;

n. To evaluate the improvement and maintenance of management reports to ensure that information is up-to-date, accurate and relevant;

o. To follow up the latest status of audit issues and findings, to evaluate the efficiency and effectiveness of the actions taken;

p. To follow up and supervise the activities related to Business Continuity Management;

q. To review the risk management systems at least once a year and to ensure that the practices in the relevant departments, which are risk owners, are in accordance with the Committee's decisions;

r. To identify technical bankruptcy at an early stage and to ensure escalating/informing the Board of Directors regarding this item;

s. To submit reports to the Board of Directors every two months that evaluate the current situation, indicate dangers, if any, and include recommendations, and to share the reports with the audit committee and internal audit unit;

t. To prepare and submit an annual evaluation report to the Board of Directors, including the members of the Committee, the frequency of meeting, including the activities carried out, as a basis for the Board of Directors' evaluation regarding principles of operation and effectiveness of the Committee;

u. To perform other duties assigned / to be assigned to the Committee pursuant to CMB regulations and Turkish Commercial Code.

The Committee meets with the Audit Committee at least once a year to ensure accordance with audit results and risk management activities' results.

The Committee immediately informs, in writing, the Board of Directors about its evaluations and major findings and suggestions regarding its mandate and responsibility.

The decisions of the Committee are considered as advices to the Board of Directors, and the responsibility for the responsibility for the final decision on related issues belongs to the Board of Directors. Final decision on related issues belongs to the Board of Directors.

5.2.Target Setting

The targets of the parties in the first and second line of defence related to risk management activities are set in accordance with the company's strategic goals and risk appetite.

5.2.1. Alignment with Activities

The complete integration of risk management into the Company's daily activities and strategic planning is ensured to attain a sustainable competitive advantage.

5.2.2. Risk Management Principles

To ensure alignment of daily activities and risk management activities with the strategic plans, the following principles are observed.

5.2.2.1. Flexibility

The company's risk management framework allows for acceptable flexibilities while complying the company's risk appetite.

5.2.2.2. Risk appetite

The risk appetite is defined as the acceptable and approved maximum risk level.

Board of Directors approved the acceptable risk appetite level by the Early Risk Detection Committee recommendation, and risk appetite level is reviewed once a year or more often if necessary. The risk appetite level determined through the following items:

• Risk Matrix - Risk Levels,

• Limits or obligations,

•Key Risk Indicator thresholds,

After setting the risk appetite, the risk profile of the Company is periodically monitored according to the risk appetite levels. If these levels are exceeded or are likely to be exceeded, necessary actions are taken by the Company's business units with suggestions of the Committee and/or manager/expert in charge of the risk management or legal and compliance officer.

5.2.2.3. Risk Awareness

It is aimed to create strong "risk awareness" culture within the company. This principle is implemented through regular meetings, trainings and reports.

5.3.Incident Management

Incident management is done proactively and prior to risk assessment. There are different techniques for managing incidents.

For example:

• Analysis of occurred incidents,

• Key Risk Indicator results,

• External incidents.

5.4.Risk Assessment

The purpose of Risk Assessment is to identify important risks that may affect the company, processes, projects, products, services, or strategies. The focus of the Risk Assessments is to mitigate the risks to an acceptable (controllable) level and to keep unidentified risks to a minimum level. This goal can be achieved by performing risk identification, risk assessment and risk mitigation stages in the Risk Assessment process.

5.4.1. Risk Assessment Methodology

The aim of the Risk Assessment is to determine inherent risks and other risks in the processes of all business units within the company, together with the business units, to evaluate these risks and to suggest risk management actions.

The stages of the risk assessment process are as follows:

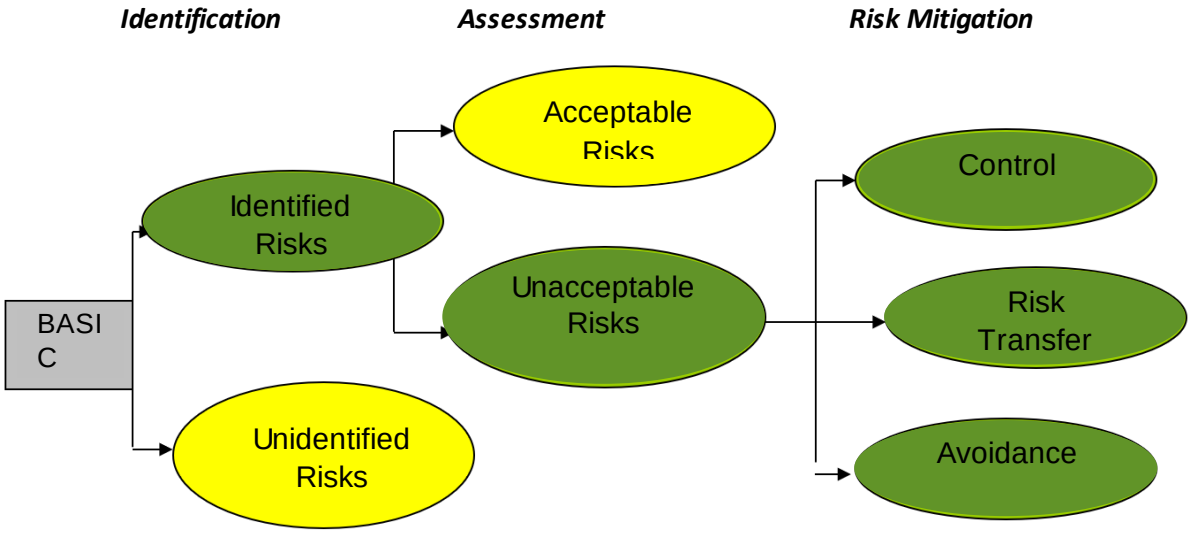
• Identification of the risk (by specifying cause-event-result),

• Determination of existing controls,

• Assessing the impact and probability of the risk,

• Acceptance, rejection, minimization, transfer of risk,

• Determining the action plan and monitoring the action.



Within risk assessment activities business units will have the following opportunities:

- Improving / developing processes,
- Having faster and better risk analysis,
- Being able to identify possible control deficiencies and weaknesses,
- Being able to identify unacceptable risks for business units,
- Measuring the quality of existing controls,
- Being able to increase the efficiency of the operations to a better level,
- Determining and follow up Key Risk / Performance indicators,
- Being able to effective capital usage and allocation.

5.4.1.1. Risk Levels

The following classification of risk levels is used in risk assessment:

- **Critical:** These risks are the risks which exceed the tolerance and their impacts to the Company's goals and / or values are significant. Management should ensure that any incident to which the company has been exposed is identified and should, without any delay, develop a program that has been agreed upon to reduce risks promptly and permanently.
- **High:** These risks are those that exceed the tolerance level. Resources should be determined to reduce risks within a proper timeframe.
- **Medium:** These risks are important in terms of their impact to the Company's goals and / or values. Management develops action plans to reduce risks in a timely manner. Prevention of the deterioration of the situation is achieved by effective monitoring.
- **Low:** These risks are not significant in terms of their impact to the Company's goals and / or values, but management should monitor the risks and take appropriate action to prevent the risks from becoming significant.

The risk level should be evaluated according to the 3 situations described below:

1. **Inherent Risk (Gross Risk):** The risks are evaluated by assuming that there is no control.
2. **Managed Risk:** It is the assessment of risks in current control environment. Assessing managed risks requires identifying all relevant controls and assessment of the effectiveness of the controls. Analysis of differences between inherent risks and managed risks provides a good understanding of the effectiveness of current controls.
3. **Residual (Remaining) Risk:** It is the assessment of risks after risk mitigation actions. Benefit / cost analysis can be conducted for possible risk mitigation actions. Residual risks at critical and high risk levels are considered as unacceptable risk levels. Medium risks are tolerated in exceptional cases and can be considered within the scope of an "acceptable" risk. Low risks are considered in the "acceptable" risk area. Residual risk should be in the "acceptable" (medium or low) risk area.

Risk appetite risk map and scales to be used in risk assessment studies shall be set by the Board of Directors with the recommendation of the Early Risk Detection Committee.

5.4.1.2. Risk Categories

Company risks are classified into 6 main risk categories. Descriptions regarding each risk category are given below.

5.4.1.2.1. Strategic Risk

Strategic risk category shall include, but not limited to:

- Strategic plans are not evaluated effectively,

- Implementing strategic plans inappropriately,

- Unexpected changes in assumptions,

- Risks related to mergers / acquisitions (M&A),

- Risks arising from capital structure preferences,

- Risks arising from governance and organizational design,

- Risks arising from strategic issues, such as risk appetite.

5.4.1.2.2. Operational Risk

They are the risks related to the system, process, human and external incidents. Operational risk category shall include, but not limited to:

- Control risks arising from unwritten procedures / processes and noncompliant with internal regulations;
- Unauthorized activity risks arising from unauthorized employee activities, including but not limited to unauthorized approval or excess of power;
- Process risks which arise during a process, which are not intentional, which result from transaction processes failed due to human error, or from process management;
- Information technology risks arising from loss of confidentiality and / or integrity and / or accessibility of information and insufficient information security;

- Internal and external fraud risks including incidents of misappropriation the Company's procedures, systems, assets, products and / or services by providing financial benefits to the personnel or external third parties by abusing the company with illegal and illegal methods.

5.4.1.2.3. Employment Practices, Security, Business Continuity and Environmental Risks

Employment Practices, Security, Business Continuity and Environmental Risks category shall include, but not limited to:

- Representative relations risks, employee relations risks and employee safety risks arising from employment, health, employee safety, practices contrary to labour laws or agreements, payment of claims related to actions involving personnel injuries or discrimination;
- Personal and physical security risks that threaten the safety and security of people;
- Risks threatening business continuity arising from human, process, system and external events, such as natural disasters, climate changes, terrorism incidents, crisis management risks;
- Risks arising from activities that may threaten the environment directly or indirectly, and may even involve an element of crime.

5.4.1.2.4. Regulation Risks

Regulation risks category shall include, but not limited to:

- Compliance risks that may cause damage to the Company's reputation, legal or regulatory sanctions or financial loss as a result of failure (perceived unsuccessful) to comply with applicable laws, legal legislations and regulations.

5.4.1.2.5. Market Risk

Market risk category shall include, but not limited to:

- Asset-liability risks arising from the mismatch between company assets and liabilities, uncertain asset / liability items, maturity/ duration/ currency mismatch of assets and liabilities;

- Risks arising from changes in interest rates;

- Risks arising from changes in foreign exchange rates;

- Risks arising from liquidity management;

- Risks arising from investment strategies that result in returns less than expected amount;

- Risks related to capital adequacy and management;

- Risks regarding portfolio management;

- Risks from derivative products;

- Risks arising from fluctuations in commodity values;

- Risks arising from cost/price fluctuations;

- Supply / demand mismatch risks;

- Risks regarding funding sources and funding capacity.

5.4.1.2.6. Credit Risk

Credit risk category shall include, but not limited to:

- Risks regarding the management and monitoring of the receivables;

- Concentration risks;

- Risks related to the determination of customer credit ratings;

- Risks regarding the distribution and changes of customer credit ratings;

- Risks related to collateral management and levels;

- Risks related to the adequacy and level of credit risk mitigation techniques.

5.5.Action Taking

Based on the results of the risk assessment, the actions to be taken and plans to be made for the risks other than the risk appetite are determined.

The risk assessment process results in a report that reflects all risks and controls. It is determined which of the selected risk reduction methods will be applied, including the person to take the action and the deadline for the action to be completed. Risk actions are taken by the relevant managements.

It is possible that various combinations of risk mitigation strategies may be used when taking an action. These strategies are given below:

Various combinations of risk reduction strategies can be used in the process of taking action. These strategies are given below.

• Reducing the probability of event occurrence (e.g. implementation of process controls, audit),

• Reducing the impact (example: limits, legal methods),

• Avoiding the risk (by stopping the risk-creating activity if possible),

• The risk acceptance (if the identified risk is within the “acceptable” risk profile),

• Transfer risk (example: through insurance).

5.6.Controlling

Controls are determined for each risk identified within the scope of the risk assessments. Risk owners are responsible for ensuring that adequate controls are in place to mitigate any risk detected. Control activities are valid in the whole organization, at all levels and in all functions. Action plans are created in cases where an existing control cannot adequately manage the risk or needs to be developed to reduce the residual risk to a more reasonable level.

The control activities aim at:

- Monitoring of all identified risks and controls related to them,
- Progressing of action plans made according to the program to minimize the risk or to strengthen the existing control,

- Identifying the action plans that are not completed within the stated timeframe and notifying the related management authorities when necessary,
- Managing all risks appropriately.

5.7.Information and Communication

Risks should be identified, analysed and all authorized parties should be contacted regarding the identified risks. The managers at all levels and the Board of Directors should be informed of the risks in their area of responsibility and take responsibility to manage the risks.

5.7.1. Risk Awareness Culture

The risk awareness culture needs to be improved through communication and training.

5.8.Risk Monitoring

Monitoring is the assessment of whether the company manages its risks effectively. Monitoring is a continuous process to measure and evaluate the effectiveness of controls, to determine whether the risks are within the risk appetite norms and in line with the targeted risk level, and their compliance with policies, regulations, implementation principles and regulations.

Monitoring can be carried out using a variety of techniques, either systematized or supported by other tools.

The basis of the monitoring function is based on the updating of risk assessment studies, as well as monitoring risk appetite, limits and key risk indicators, action monitoring, control tests, review of written regulations, stress tests and other examples on this subject.

5.8.1. First Line of Defence Monitoring Function: Business Units

Business units are responsible for the effective and comprehensive structuring and proper execution of their processes. Risks should be properly mitigated to ensure an effective and comprehensive structuring. In addition, processes should be structured in such a way that the effectiveness of all controls can be continuously monitored, thereby overseeing the relevant application. This **primary monitoring function** should be added to the daily operations of the departments included in the 1st line of defence. The execution of basic controls should always be documented and provable.

5.8.2. Second Line of Defence Monitoring Function: Risk Management

Within the scope of risk management activities, the Company's manager / expert or legal and compliance officer in charge of risk management is responsible for the monitoring of the compliance of the departments in the first line of defence with the risk appetite, policies and regulations, and for monitoring whether or not the management performs its control activities properly. It regularly provides management with risk management reports on the results of monitoring activities. The risk reports should have sufficient details and scope. The Company's manager / expert or the legal and compliance officer responsible for risk management and / or the Committee determine the details and scope.

5.8.3. Third Line of Defence Monitoring Function: Internal Audit

The Internal Audit Unit is responsible for evaluating the effectiveness of the design and functionality of the risk control structure established by the 1st and 2nd line of defence. It submits the audit reports to the Board of Directors.