TRANSITION RISK

Transition risk refers to the financial, operational, and strategic risks that a company may face during the shift to a low-carbon economy. This “transition risk” is a significant risk area for banks. Therefore, we aim to align ourselves with this transformation in order to effectively manage it.

According to the World Economic Forum’s annually published Global Risks Report, it was noted that in 2024, half of the top priority risks were environmentally based and related to climate change. Thus, reducing these risks depends on the transition to a low-carbon economy.

The Organisation for Economic Co-operation and Development (OECD) states that in order to address sustainability issues such as reducing global inequalities, preventing climate change, and ensuring prosperity, an average of USD 6.9 trillion in investments is required annually until 2030.

In addition, according to the World Bank’s 2022 report, Turkey alone will need USD 165 billion of investment by 2040 focusing solely on climate change and green transformation. In this context, banks are obliged to monitor all potential impacts both from the “inside-out” (portfolio’s impact on climate change) and “outside-in” (climate change’s impact on portfolios). At Akbank, we therefore prioritize climate transition risk and take action accordingly.

While the average global temperature increase is expected to reach 1.5°C by 2030, strategies and actions to mitigate climate change and its potential destructive impacts are becoming increasingly important for companies. This issue is also closely monitored under the Turkish Sustainability Reporting Standards (TSRS), which emphasize both transition and physical risks of climate change. Within the scope of managing climate change risk as a component of financial risk, we have developed a methodology to identify, measure, and monitor climate risk for use in the Internal Capital Adequacy Assessment Process (ICAAP). Based on this methodology, we allocate capital within ICAAP scenarios for climate risk. We also integrate quantified climate risk scores into risk appetite indicators to monitor the portfolio’s risk profile against set thresholds. Additionally, we have defined risk limits for monitoring climate risks. In the credit allocation process, company ratings are affected depending on the evaluation of climate risk management plans.

Within the Akbank Environmental and Social Risk Framework, we analyze both physical and transition risks of climate change, assess sectors and transactions potentially affected by these risks, and monitor them periodically in line with national and international requirements through environmental and social reviews. We have committed not to finance new coal-fired thermal power plant (TPP) projects, capacity expansions of existing coal-fired power plants, or new coal mining investments. In 2024, we also announced our commitment to exit coal by 2040, taking into account the principles of a just transition.

For our clients’ projects, we require that all large-scale Category A and certain Category B1 projects included in our ESIA process incorporate information on physical and transition risks of climate change, as defined by the Task Force on Climate-related Financial Disclosures (TCFD), within independent consultant reports. For high-risk clients and projects, we request climate change risk assessment studies and closely monitor their processes.

As part of Akbank’s Environmental and Social Risk Framework, we continue to assess climate-related risks and maintain our commitments not to finance new coal-based TPP projects, capacity increases, or new coal mines.

With a focus on our Net Zero carbon target for 2050, announced in 2022, we aim to create value by supporting our clients' transformation. In 2024, we launched the Akbank Net Zero Strategy, which is shaped around credit portfolio climate risk, decarbonization, and operational emissions reduction. Our strategy encompasses fostering a culture of sustainable finance, identifying climate risks and opportunities, turning risks into opportunities, and ensuring effective data management. Through our Sustainable Finance Ecosystem, we provide products, services, and partnerships that support our clients' transition to low-carbon activities. The foundation of our credit portfolio decarbonization strategy is to accompany our clients on their green transformation journey.

In line with international initiatives, we have identified four carbon-intensive sectors in our loan portfolio that are prioritized for absolute and intensity-based decarbonization. We announced medium-term emission reduction targets aligned with the Paris Agreement's 1.5°C scenario and became a member of the Net-Zero Banking Alliance. Akbank Net Zero Strategy Presentation.

We closely monitor our carbon-intensive clients' Net Zero targets and strategies, while continuing preliminary assessments in these sectors. Within our Sustainable Finance Ecosystem, we provide financing products tailored to clients' different stages of Net Zero transition, offering customized solutions that support their needs. This way, we aim to assist our clients in their transition to a low-carbon economy. In 2024, in line with the Net-Zero Banking Alliance Principles (excluding energy and commercial real estate), we carried out client-based climate change assessments for seven priority sectors.

Further details on our work regarding transition risks can be found on pages 22–26 of our TSRS Report: 2024-akbank-sustainability-report-in-compliance-with-turkish-sustainability-reporting-standards.pdf

With products such as the "Low-Carbon Economy Transition Loan," we encourage companies operating in industry, exports, and other carbon-intensive sectors to invest in projects aligned with green criteria and designed to mitigate carbon tax risks. More information is available at: Akbank Sustainable Finance.

ARTIFICIAL INTELLIGENCE (AI) RISK

Artificial intelligence (AI) has become central to decision-making processes in modern banking, driving efficiency in areas such as data processing, fraud detection, credit scoring, pricing, and personalized services. However, as of 2024, global risk literature shows that the rapid expansion of AI is significantly reshaping institutional risk profiles. The World Economic Forum's Global Risks Report 2024 highlights misinformation/disinformation waves as the top short-term risk, with generative AI as one of its main accelerators. According to the IMF's 2024 analysis, around 40% of global employment will be impacted by AI; where the impact is high, risks such as skill mismatches, income inequality, and social tensions rise. Data from the OECD's AI Incidents & Hazards Monitor also shows a steep upward trend in reported AI-related incidents since November 2022, underscoring the rapidly growing need for policy and risk management. Similarly, the World Bank's 2024 report points out that while generative AI carries growth and productivity potential, it may also create systemic risks in inequality, skills gaps, and inclusiveness.

In line with our vision of being the pioneering bank carrying Turkey into the future, at Akbank we leverage AI technologies across multiple areas: improving customer and employee experience, enhancing operational efficiency, and diversifying the financial services we provide. This expansion brings AI under the category of emerging risks.

At Akbank:

- We design our AI systems and decision-making processes with inclusivity in mind, ensuring data is used appropriately and strictly for its intended purpose. Our model development frameworks are aligned with the Bank's goals and risk management strategies and are structured to prevent bias or discrimination.
- To ensure that data does not contain bias toward any individual or community, we develop methods covering inputs, potential correlations, impact analyses of model outputs, and control mechanisms. These are applied not only during development but also updated regularly through periodic reviews.
- From end-to-end model preparation to all customer and employee interaction platforms, we act in accordance with these principles.
- In addition to preventive and corrective mechanisms, we also run training and awareness programs to promote internal adoption of AI.

For trust in AI systems, we commit to transparency in all functions and applications. We ensure that the functioning of systems and the decisions made are sufficiently clear and understandable for stakeholders such as users, product owners, and system designers. Documentation explains how systems operate, what type of data they are based on, and which algorithms are used. This includes design decisions, inputs, version logs, model algorithms, usage guidelines, and model results. Through regular controls, we monitor the effects of model performance. We also track and apply up-to-date techniques and algorithms explaining how AI models work.

We share relevant information with stakeholders in line with our internal policies, information-sharing standards, and procedures. In collaborations with suppliers, we extend our responsible AI controls—especially transparency—by asking them to identify impacts and assess potential areas for improvement, while ensuring that our requests do not restrict innovative ideas. Our approach is constructive and innovation-oriented.

We establish centralized, distributed, or hybrid monitoring mechanisms, depending on the field of application, to manage and record decisions, operations, and ongoing processes linked to AI models and systems. Under this principle, model owners are accountable for outcomes and related decisions. Processes, systems, and procedures are developed to enable accurate monitoring.

With the accountability principle, we ensure clear and transparent documentation throughout the lifecycle of AI systems—from development to operation and decommissioning. We adopt both reactive and proactive accountability mechanisms:

- Reactive accountability means responding proportionally and in a timely manner to incidents or requests regarding AI systems and their outputs.
- Proactive accountability means anticipating and preparing for potential future harms within reasonable limits.

We ensure AI systems are developed in line with defined resilience and security principles. Protecting user data, ensuring system continuity, and maintaining the highest security standards are central. This enables us to prevent interruptions and security threats while consistently achieving optimal results.

By keeping humans in the loop, we build structures that enable automated, end-to-end flows while allowing for intervention when needed. With advanced distributed systems for our critical technology infrastructure, we ensure scalability and accelerate adaptation to new developments. For live environments, we provide high-level services through contingency centers.

For our employees, we establish principles and standards in coding, risk and security auditing, process monitoring and updating, and data protection, ensuring they remain current. In AI initiatives, we place utmost importance on the privacy and protection of personal data. We comply with both Bank-wide standards and national laws and regulations. We safeguard customer data, bank secrets, and all sensitive information by managing access authorizations and controlling who can access which data types. For data analysis and modeling, only authorized customer data is used, ensuring the modeling process is conducted under the best conditions.

We ensure data security policies apply to all data used or generated throughout the AI lifecycle. This includes training, testing, validation, monitoring, model input data, inferences derived from processing, synthetic data produced, and model outputs. Both data privacy and data security are monitored with equal priority.

In line with this, we comply with the Banking Law, the Regulation on Banks' Information Systems and Electronic Banking Services, the Regulation on Sharing Confidential Information, and the Law on the Protection of Personal Data. Additionally, we adhere to Akbank's Social Media Use Policy for Employees, Digital Trust Principles, Information Risk Management Policies, and all related Bank-issued documents on privacy and security.