Türkiye İş Bankası A.Ş.
Information on Risk Management Policies Applied per Risk Types

Bank risk policies and procedures constitute the internal rules and principles which are approved and enforced by the Board considering Risk Management Division suggestions and executed by the senior management.

Segregated by credit, market, liquidity and operational risk categories, the policies in line with best practice approved by the Board of Directors stipulate general standards including the organization and scope of risk management function, risk measurement methods, roles and responsibilities of the risk management group, risk limit setting methodology, rules governing the breach of limits.

To ensure the conformity of the Bank's risk appetite with business plan and prevailing market environment, risk limits set by the Board of Directors are monitored. In this context, breaches in market, liquidity and credit risk limits are analyzed by Risk Management Division taking market and industry conditions into consideration , and findings are reported to the Audit Committee.

Credit Risk Policy
Credit risk policy sets the framework for credit risk management, control and monitoring, roles and responsibilities and credit risk limits. Credit risk is defined as any situation where the counterparty obligation will not or cannot be fulfilled partially or fully on maturity as affirmed in the agreement.

İşbank maintains identification, measurement and management of credit risk across all products and activities. The Board reviews credit risk policies and strategies annually at minimum. Senior management is responsible for the execution of credit risk policies.

The findings of review of loans and credit risk are reported to the Board and the senior management regularly. Monitoring credit risk is based on the risk levels and composition of the loan portfolio. The monitoring process includes parameters such as maturity, industry, collateral, geography, currency, loan type, and credit risk ratings as a whole, in addition to the assessments on the obligor and the facility. Credit risk monitoring encompasses any additional risks that could stem from possible macroeconomic changes and potential adverse conditions.

Bank's credit risk management policy entails credit portfolio diversification. Segmentation is used to execute dispersion of diversified risk strategy. Segmentation is the separation of portfolio into wide customer groups according to geography, sector, product and similarly affected by the negative changes at the economic and financial sector.

Internal audit and risk management functions regularly assess the internal credit risk rating system as to its compatibility with the structure, size and complexity of the Bank's operations. If diverse circumstances required, necessary adjustments and/or modifications are made to the system.

Credit Risk audition implies independent control of compatibility of credit quality and crediting process with the Bank's policy and application principles by legal arrangements and assessment of credit and other asset provision adequacy.

Asset and Liability Management Risk Policy
Asset and liability management risk is defined as; loss risk caused by Bank's failure to effectively manage all financial risks arising from the bank's assets, liabilities and off-balance sheet transactions. Market risk of trading book, structural interest rate risk of banking book and liquidity risk are all within the scope of asset and liability management risk.

All principles and procedures related to constitution and management of Bank's asset-liability structure and Bank's risk appetite is established by the Board of Directors. Ensuring asset and liability management risk being within the levels imposed by legal legislation and internal risk limits is the primary priority. Internal risk limits are determined by Board of Directors taking into consideration liquidity, target income level, general expectations about the changes in risk factors and risk appetite of the Bank.

Board of Directors and Audit Committee are obliged to track that Bank's capital is used optimally. For this purpose they have to keep risk limits under control and ensure necessary actions being taken.

Asset-Liability Committee is responsible for governance of asset and liability management risk in accordance with the risk appetite and risk limits determined by Board of Directors and within the principles and procedures expressed in this policy.

Measuring asset and liability management risk, reporting the results and monitoring the compliance with the risk limits are the responsibilities of Risk Management Division. Under different scenarios the course of the risk taken is reviewed. Measurement results are tested in terms of reliability and integrity. Asset and liability management risk is reported to Risk Committee and reported to the Board of Directors through Audit Committee.

Compliance with risk limits is closely and continuously monitored by Risk Management Division, Asset-Liability Committee and related business units. In the event of a breach in the risk limits, the breach and its reasons are instantly reported to Board of Directors through Audit Committee. Course of action needed to be taken in order to eliminate the breach is determined by the Board.

Asset and liability management processes and compliance with the policy rules are audited by internal audit system. The principles regarding the audit process, audit reports and fulfillment of action plans to eliminate the errors and gaps determined by internal audit are established by the Board of Directors.

Türkiye İş Bankası A.Ş.
Information on Risk Management Policies Applied per Risk Types

Operational Risk Policy
Operational risk is defined as “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events”. Risk Management Division is responsible for the risk management activity on this particular risk. Operational risk management activities comprise defining, measuring, analyzing, monitoring and reporting of operational risks, following up the new techniques on management of operational risks besides regulatory and internal reporting.

Categorization of inherited operational risks within the activities and processes is made possible by the Enterprise Risk Framework. It serves as the basic document to define and classify the risks and is subject to alteration as conditions change.

The methodology employed to identify operational risks is “self-assessment”. This methodology requires staff with roles and responsibilities in a particular activity to get involved in the risk and control assessment process of that activity. Operational risk management process combines both qualitative and quantitative approaches in measurement and assessment. The measurement process uses data obtained from “impact - likelihood analysis” and “loss database”.

All operational risks inherited in the activities, risk levels of new products and processes, operational losses incurred by the Bank are monitored continuously, risk assessments are updated regularly and reported to the Risk Committee and the Board in a timely manner.

Employees have the understanding of the Bank’s objective to attain a working environment aiming to reduce the probability of loss, considering that the entire internal rules and procedures, led by operational risk policy, and act sensitively to the inherited operational risks and controls.

Consolidated Risk Policies
Compliance with risk management principles related to the Bank’s subsidiaries are monitored through Bank’s “Consolidated Risk Policies” by Subsidiary Risk Unit. Subsidiaries identify their specific risk management policies that cannot divert from or conflict with consolidated risk policies. Subsidiary boards approve company risk policies that form the framework of their risk management systems and processes.

Information Systems Management Policy
The purpose of Information Systems Management Policy is to determine the principles which will constitute a basis for the management of information systems that the Bank uses to fulfill its activities and the procedures in order to define, measure, control, monitor, report and manage the risks derived from using information technologies. With the Policy, the information technologies which is an important element for sustaining Bank activities is intended to be managed effectively as information systems management, being handled as a part of corporate governance practices. On the management of Bank’s information systems and all the elements relating to those systems articles of this Policy are applied.

Risks derived from information technologies are basically assessed within the scope of Bank’s operational risk management. It is essential that those risks which could be seen as multipliers of the other risks derived from activities of the Bank are measured, closely monitored and controlled within the framework of Bank’s integrated risk management.