9. The Company applies the principle of transparency hence employees can communicate to the relevant management about any issues that occur in the Bank's operational activities.
10. The entire process of recruitment, development and career path is carried out taking into account the competence of employees.
11. Management assigns and places employees based on job exposure, level of knowledge, ability, mastery of technical competence and application of behaviour and results of employee performance assessment.
12. The Board of Directors establishes a corporate culture that reflects the values underlying the conduct of the entire Bank's levels.
13. All levels of the Bank are required to have integrity and uphold ethical values.
14. Management becomes a role model, always increases the engagement level of all employees and has a high personal commitment to the development of a sound Bank.
15. Management is obliged to improve an effective risk culture and ensure that it is inherent at every level of the organization.

For the oversight of the Board of Directors and control culture, the Company sets strategies & objectives as requirements for an effective event identification, risk assessment and risk response

process, consisting of:
1. Strategic Objectives, the high-level targets and in line with the Bank's vision and mission.
2. Operational Objectives, the derivative goals and strategic objectives at the operational level (activities, work units and others).

The Company has standard procedures for targets setting in accordance with the vision, mission and risk appetite.

Risk Recognition and Assessment

The Board of Directors identifies events that could potentially affect the Bank's ability to implement strategies and achieve targets effectively. The identification is carried out on events that are expected to have a negative impact (risk) that require the Bank's assessment and response. Identification is also carried out on events that are expected to have a positive impact which is an opportunity for the Board of Directors in developing strategies to achieve the Bank's goals.

In identifying potential events, the Board of Directors considers all aspects of the organization.

Risk assessment is a series of actions starting from the identification, analysis and measurement of the Bank's risk to achieve the set targets. Risk assessment is carried

out on all types of risks inherent in each process/activity that has the potential to harm the Bank.

The Bank has a written risk management policy, which is determined by the Board of Directors and approved by the Board of Commissioners.

Risk assessment is carried out by identifying the risks appetite, setting limits and its risk control techniques, assessing risks that can be measured (quantitative) and those that cannot be measured (qualitative), as well as against risks that can be controlled and cannot be controlled, taking into account their costs and benefits. The risk assessment methodology is a benchmark for creating risk profiles in the form of data documentation that can be initiated periodically. Furthermore, the Bank must decide whether to take these risks or not, by reducing certain business activities.

Internal control needs to be reviewed appropriately in the event that there are risks that have not been controlled, both previously existing risks and newly emerging risks. The implementation of the review includes conducting continuous evaluations of the influence of any changes in the environment and conditions, as well as the impact of achieving targets or the effectiveness of internal control in the Bank's operational and organizational activities.

The Board of Directors establishes measures to respond to risks based

INTERNAL CONTROL SYSTEM

on an assessment of the risks and relevant controls.

Control and Separation of Functions Activities

Control activities include control activities and segregation of duties, with the following description:

1. Control Activities
   Control activities engage all levels of the Company, which includes planning, setting policies and procedures, implementing controls and early verification processes to ensure that policies and procedures have been consistently adhered to, and are activities that cannot be separated from every function or activity of the Company on a daily basis. Control activities are implemented at all levels of functions according to the Company's organizational structure, which includes:
   a. Review by the Board of Directors (Top Level Review)
      The Board of Directors periodically requests explanations (information) and operational performance reports from the Head of the Work Unit in order to review the realization results compared to the targets that have been set. Based on the review, the Board of Directors immediately detects problems, such as control weaknesses, financial statement errors or other irregularities (fraud).

b. Functional Review
   This review is carried out by Internal Audit Unit at the time of audit or in the process of reporting to the regulator, which includes:
   - Review the risk assessment (risk profile report) produced by the Risk Management Unit.
   - Analysing operational data, both data related to risk and financial data, namely verifying details and transaction activities compared to outputs (reports) produced by the Risk Management Unit.
   - Review the realization of the implementation of work plans and budgets made by each work unit (Group/Branch), in order to:
     - Identifying the causes of significant deviations.
     - Sets the requirements for corrective actions.

c. Control of information systems
   - The Company carries out verification of the accuracy and completeness of transactions, as well as the implementation of authorization procedures in accordance with applicable regulations.
   - The Company carries out IT control measures to produce systems and data to maintain confidentiality and integrity and support the achievement of the Company's objectives.
   - Control of information systems includes:
     - Control over data centre operations (databases), procurement systems, development and maintenance of systems/applications. Such control is applied to servers, and user work stations, as well as networks.
     - Application control is applied to the program used by the Company in processing transactions and to ensure the availability of an effective audit process and to check the correctness of the audit process.

d. Physical controls
   - Physical asset control is carried out to ensure the implementation of physical security of the Company's assets.
   - Physical asset control includes securing assets, records and documentation, as well as limited access to application programs.
   - The Company must check the value of assets (appraisal) periodically.