NAGELMACKERS

Key elements of the Governance Framework of Bank Nagelmackers

I. Internal procedures, codes of conduct and prevention policy

The integrity policy of the Bank manifests itself in a series of procedures and codes of conduct, which can be consulted by every employee of the Bank at any time via the Intranet.

The following may be mentioned in particular in this context:

- the general 'anti money laundering procedure'
- the individual risk scoring and client acceptance procedure
- the code of conduct for the tax-avoidance-prevention
- the repatriation procedure
- the client monitoring procedure
- the financial transactions code of conduct
- the procedure regarding violence, mobbing or sexual harassment at work
- the code of conduct for business gifts
- the anti-bribery and corruption policy
- the anti-discrimination code of conduct
- the privacy procedure
- the remuneration policy
- the MiFID procedure
- the order execution policy
- the procedure on selling and arbitrage advice
- the policy and procedure regarding inducements
- the complaints handling procedure
- the whistleblowing policy

These procedures and codes of conduct are updated whenever this is required. They also receive wider attention on a regular basis through staff training and awareness programmes.

The Bank ensures that there is no discrimination of staff based on gender, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

The Bank's policies are gender neutral. This includes, but is not limited to remuneration, recruitment policies, career development and succession plans, access to training and ability to apply for internal vacancies. The Bank ensures equal opportunities[34] for all staff independent of their genders, including

with regard to career perspectives and aims to improve the representation of the underrepresented gender in positions within the management body as well as in the group of staff that have managerial responsibilities.

II. Continuity policy

In the context of its Business Continuity Management (BCM), the Bank has a Business Continuity Plan (BCP) and detailed Disaster Recovery Plans (DRP) in place in order to be able to operate on an ongoing basis the critical business processes in the event of a crisis and to limit losses in the event of severe business disruption. Disaster Recovery focuses on the information or technology systems that support business functions, as opposed to Business Continuity which involves planning to keep all aspects of a business functioning in the midst of disruptive events. Disaster recovery is a subset of Business Continuity. The ICT business continuity management processes are an integral part of the Bank's overall financial continuity management process.

The BCP/DRP plans are tested at least on an annual basis, and are optimised where possible.

In addition, the Bank also has a Crisis Management Plan (CMP) in place in the context of crisis management. Crisis management exercises are organised on a regular basis. The CMP also includes crisis communication measures allowing to inform all relevant internal and external stakeholders, including the competent authorities and relevant outsourcing providers a timely manner.

The Board of Directors is updated on the status of Business Continuity affairs on an annual basis.

The Bank has a Contingency Funding Plan embedded in the Recovery Plan that is regularly updated and coordinated with ABBH.

III. Risk strategy and risk management framework

1. Risk strategy

Risk management is a bank-wide holistic process and everyone's responsibility. The **final responsibility** for this process remains at the Board of Directors that defines and monitors the risk strategy, the risk appetite and the present risk framework and rests with the Executive Committee that assures its implementation. The implementation is organised along 3 lines of responsibility.

The **first-line responsibility** for risk management rests with the business. This means that everyone ensures that the risks arising from the activities and processes under his/her responsibility are identified, and that appropriate control measures are implemented and maintained to control these risks. First-line business units are primarily responsible for managing risks on a day-to-day basis in line with the institution's policies, procedures and controls, taking into account the institution's risk appetite and risk capacity.

The purpose of risk management department **at the second-line level** is to gain a general understanding of all the risks the Bank is facing in the performance of its on and off-balance activities, to proactively identify them, and to analyse and report on them.

Second-line risk management is furthermore responsible for the methodological direction and challenges of risk management within the bank, and for creating and strengthening risk awareness. Second-line risk management also controls in an independent way compliance with the national and international legislation and if the risks remain in line with the banks' risk appetite. The independent control should be based on policies, procedures, risk limits and risk controls ensuring adequate, timely and continuous identification, measurement or assessment, monitoring, management, mitigation and reporting of the risks and escalation in case of breaches.

The **third-line responsibility** for risk management rests with the Internal Audit department, which carries out an independent assessment of the risk management framework within the Bank, issues recommendations with regard to observed weaknesses, and monitors their implementation.

2. Mission of the Risk Management department

The Risk Management department is part of second-line risk management, with the following **responsibilities**:

- Challenging and assisting in the implementation of risk management measures by the business lines in order to ensure that the processes and controls in place at the first line of defence are properly designed and effective;
- Contribution to risk awareness and a sound risk culture throughout the bank;
- Evaluating how risks identified could affect the banks' ability to manage its risk profile, its liquidity and its sound capital base under normal and adverse circumstances;
- Timely, correct and complete identification, measurement, stress testing and assessment of all types of (material) risks in a quantitative and qualitative way;
- Continuous deepening and broadening of risk measurements, stress tests and assessments, optimizing the methodological practices;
- Documented analysis of the results of measurements, stress tests and assessments, detection of potential problems, and creating awareness and launching an escalation for corrective action, where necessary;
- Reporting of the risks and their management to internal risk committees, the Executive Committee, the Risk Committee and the Board of Directors,
- Collection of knowledge, support, assessment and challenge of the first line risk management;
- Collection of knowledge with regard to methods, models, best practices and market research relating to risk management;
- Analysis of trends and recognise new or emerging risks and risk increases arising from changing circumstances and conditions, including the follow up and implementation of the legislation and regulations with respect to risk management, taking into account the proportionality principles;
- Provide the Board of Directors with all relevant risk-related information to enable it to set the institution's risk appetite level;

- Ensure that the risk appetite is appropriately translated into specific risk limits;
- Assess independently breaches of risk appetite or limits (including ascertaining the cause and undertaking a legal and economic analysis of the actual cost of closing, reducing or hedging the exposure against the potential cost of keeping it);
- Active involvement in all material risk management decisions and any new product or project, strategic decisions or material changes; performing a comprehensive view and understanding of bank's business, and all (material) risks that the bank is facing in the performance of its business as usual activities, and in change processes.

Risk management department has defined the following **main risk factors:**

- Interest rate risk
- Liquidity risk (including ILAAP)
- Counterparty risk (investment portfolio and banking counterparties)
- Counterparty credit risk for non-centrally cleared derivatives
- Credit risk (loan portfolio)
- Model risk
- Pricing of risks in the tariffs
- Operational risks, including fraud risks
- Business continuity
- ICT and security risks
- Third Party Risk (Outsourcing)
- Privacy (GDPR)
- Environmental, social and governance risk factors (ESG)