

### **APPENDIX 3**

The **duties and responsibilities of the Risk Committee** are summarised as follows:

#### **Risk Management Sector**

- i. To advise the Board of Directors for the implementation, by the Senior Managers, of the Bank's risk strategy and the application of the respective limits that have been set, taking into account:
  - The requirements set by the Directive of the Central Bank of Cyprus on Regulations for Governance and Management Arrangements currently in force.
  - The Bank's financial and risk profile.
  - The Bank's ability to manage and control risks.
- ii. To assist the Board of Directors in overseeing the implementation of the strategy by the Senior Management Executives, including:
  - The development of mechanisms for ensuring the management of significant exposures that approach or exceed the approved risk limits, and where necessary, their mitigation in an effective and timely manner.
  - The timely identification and any escalation of breaches of risk limits and significant risk exposures.
  - Controlling whether the values of assets and liabilities offered to customers take into account the business model and risk strategy of the Bank. Where the values do not accurately reflect the risks, according to the business model and risk strategy, the Committee shall submit a corrective plan to the Board of Directors.
  - Submitting proposals to the Board of Directors and suggestions for corrective measures when shortcomings are identified in the implementation of the risk strategy, as well as suggestions for the appointment or removal of the Head of the Risk Sector.
  - Advising the Board of Directors, on the basis of the work of the Audit Committee, the Risk Sector, the Financial Services Division and the external auditors, in connection with the adequacy of provisions and the effectiveness of the risk management framework and the strategies and policies in connection with the maintenance, on an ongoing basis, of adequate amounts, types and distribution of internal funds and equity to cover the Bank's risks.
- iii. The Committee shall determine the nature, quantity, form and frequency of the information it needs to receive in connection with the Bank's risk status and for each kind of risk and every business unit, having an obligation to: :
  - Approve measurements or procedures in order to confirm that the reports and information it receives regarding risk-related issues are accurate, complete and reflect the true picture of the Bank's risk profile.
  - See to it that the risk parameters and risk models that have been developed and are used for quantifying them are subjected to periodic independent ratifications.
- iv. It monitors the adjustments to the methodology of calculating expected credit losses, evaluates and proposes to the Board of Directors for approval, on a quarterly basis, the quarterly provisions.
- v. It monitors the development and updating of credit risk models, the development and implementation of the relevant governance framework for credit risk models. It evaluates and proposes to the Board of Directors for approval the results of the validation of credit risk models.



- vi. The Committee shall evaluate the Bank's strategic objectives, risk strategy, including the risk appetite for IRRBB, and internal governance. It also oversees the implementation of the governance arrangements within the Bank that ensure effective and prudent management of the Bank. It oversees the IRRBB framework, the institution's risk appetite framework and proposes to the Board of Directors for approval of the corresponding policies and methodologies.
- vii. It shall ensure adequate access to information regarding the Bank's risk status and if required and deemed appropriate, it shall seek the contribution of expert external consultants.
- viii. The Committee shall evaluate on an annual basis the adequacy and effectiveness of the Bank's risk management policy and procedures, as well as compliance regarding:
  - Undertaking, monitoring and managing risks (market, credit, interest rate, liquidity, and operational) according to the category of transactions, and customers according to the risk level (such as occupation, activity), establishing upper limits each time for undertaking risks as a whole for each type of risk and further allocating each of these limits, per currency, sector, etc.
  - Establishing limits for ceasing loss-making activities or other corrective measures.
  - The suitability of limits, the adequacy of provisions and the adequacy in general of own capital in relation to the level and form of the risks undertaken, on the basis of the annual report of the Head of the Risk Sector.
- ix. An appraisal of the Head of the Risk Management Division shall be conducted on an annual basis, and this shall then be submitted to the Board of Directors and, where judged necessary suggestions shall be made to the Board of Directors regarding the appointment or removal of the Head.
- x. Reviews and endorses the Head of the Risk Management Sector's replacements list and intermediary successor and submits it to the Nominations, Corporate Governance and Sustainability Committee for approval, in accordance with the provisions of the Bank's "Policy regarding the succession plans of the Members of the Board of Directors, Senior Managers and Key Function Holders".
- xi. The Committee shall formulate the risk undertaking and capital management strategy which responds to the Bank and the Group's business goals and to the adequacy of available technical and human resources.
- xii. It shall evaluate and propose for approval by the Board of Directors the Bank's Credit Risk Management Policy which must be in line with the Bank's business plan and meet the conditions of the relevant Guidelines of the Central Bank of Cyprus and review it at regular intervals (at least once a year) and revise it accordingly.
- xiii. It shall then review at regular intervals the approved Credit Risk Management Policy as well as the Bank's important policies and procedures in connection with credit risk, and set appropriate approval levels. In this framework, it shall evaluate and propose to the Board of Directors for approval the general credit lending criteria, including the general terms and conditions, through the Credit Regulation.
- xiv. It shall see to the development of an internal risk management system and its incorporation in the decision making process for business decisions throughout all the activities/Sectors of the Bank (e.g. decisions concerning the introduction of new products and services, the pricing of products and services adjusted to risks).
- xv. It shall receive and evaluate the reports submitted every quarter by the Risk Management Sector, as well as its individual suggestions regarding the implementation of suitable techniques for adjusting risks to acceptable levels.
- xvi. Receives regular reports, ad hoc information, announcements and opinions from the Head of the Internal Audit Functions, regarding the existing risk profile of the Bank, the risk culture and risk limits, as well as any significant violations that may have arisen, with



detailed information and recommendations on remedial measures to be taken, or proposals on how to address them.

- xvii. It shall review reports in connection with the Stress Test Governance Framework as well as the results of stress tests, which might be submitted by the Risk Management Sector. The stress tests are conducted in the framework of monitoring risks as well as in order to comply with the Directive of the Central Bank of Cyprus on Regulations for Governance, Regulation 575/2013 in which it is mentioned in paragraph (i) of the Preamble, as well as the rest of the relevant Regulatory Framework. The Committee, after having reviewed the results in question from the stress tests, shall inform the Board of Directors accordingly, explains the respective aspects, and addresses the questions / issues raised and where deemed necessary, it shall make suggestions for corrective measures to be taken.
- xviii. Review on a periodic basis and makes decisions on the content, form and frequency of information to be submitted to the Committee, in respect of the various risks.
- xix. It oversees the alignment, on the one hand, between, all important financial products and services offered to the customers and, on the other hand, the Bank's business model and risk strategy.
- xx. Cooperates with other Committees of the Board of Directors whose activities may have an impact on the risk strategy (e.g. Audit and Remuneration Committees), and maintains a regular communication with the Bank's Internal Audit Functions, and in particular with the operations of the risk management and ICT and security risk.
- xxi. It shall secure communication of the Internal Audit Division, the internal auditors and the Competent Authorities, and the Board of Directors in connection with risk management issues.
- xxii. Without prejudice to the duties of the Remuneration Committee, and in order to contribute to the formation of sound remuneration policies and practices, the Risk Committee is required to examine whether the incentives provided by the system, policies and practices take into account the Bank's risk, capital and liquidity, as well as the likelihood and timing of making profits.
- xxiii. On the basis of the reports of the Internal Audit Division and the external auditors, the Risk Committee shall ensure:
  - The effectiveness and compliance with the risk management procedures and the related credit granting procedures, including the provisioning policy (identifying any risks not covered).
  - The adequacy of procedures in connection with the internal evaluation of the Bank's capital adequacy.
  - Assessments as to whether the procedure or methodology for calculating the impairment of the value of loans and other assets and any changes during use.
- xxiv. When deemed necessary, ensures the sufficient participation of the Internal Audit Functions and other relevant divisions (Human Resources, Legal Services, Financial Services), within their respective areas of expertise and/or secures advice from external experts.
- xxv. It shall approve the Rules of Procedure of the Risk Management Sector and any updates to it, if required, and shall submit it for ratification to the Board of Directors.
- xxvi. It shall evaluate the independence, adequacy and effectiveness of the Risk Management Sector and submit its evaluation to the Board of Directors.
- xxvii. It shall ensure that the Risk Management Sector has in place adequate resources and the required position within the Bank.



Information Technology and Communications (ICT) and Security Risk

- i. It shall secure the ICT and security risk management function, which covers the entire Bank. It also ensures the independence and objectivity of the audit function in question (Directorate of Information Security and Personal Data Protection).
- ii. It shall secure the monitoring and review of the application of the ICT and security risk management framework, including the information security policy, as well as the monitoring, assessment, management and reporting of the ICT and security risks.
- iii. It shall approve the Rules of Procedure of the Information Security and Personal Data Protection Division and update them, if required and submit them for ratification by the Board of Directors.
- iv. In the beginning of each year, it shall evaluate the Report of the Bank's Head of Information Security, which must cover at least the following:
  - A summary of the most important information security risks face by the Bank at the time of submission of the reports.
  - A list of all significant information security incidents that occurred in the course of the year and the corrective measures taken to prevent the recurrence of similar incidents.
  - Any important actions taken in the previous year in order to improve shortcomings in the information security environment.
  - Any outstanding issues that endanger the Bank's information security.
- v. It shall advise the Board of Directors, on the basis of the work of the Audit Committee, the Information Security and Personal Data Protection Division and the external auditors, about the adequacy and effectiveness of the information security framework.
- vi. It shall advise the Board of Directors, on the basis of the work of the Audit Committee, the Risk Management Sector, the Information Security and Personal Data Protection Division and the external auditors, about the adequacy and soundness of the ICT systems, so that they:
  - Enable the identification, measuring, evaluation and reporting of the risks in a timely and precise way.
  - Ensure adequate protection of the Bank's confidential and proprietary information.
- vii. It shall conduct an annual evaluation of the Head of the Information Security and Personal Data Protection Division and then submit this to the Board of Directors, and where deemed necessary, it shall make suggestions to the Board of Directors for the appointment or removal of the Head.
- viii. Reviews and endorses the Head of the Information Security's replacements list and intermediary successor and submits it to the Nominations, Corporate Governance and Sustainability Committee for approval, in accordance with the provisions of the Bank's "Policy regarding the succession plans of the Members of the Board of Directors, Senior Managers and Key Function Holders".
- ix. It shall evaluate and monitor the independence, adequacy and effectiveness of the Information Security and Personal Data Protection Division.
- x. It shall ensure that it is fully informed about the advice and recommendations made by the Head of the Information Security and Personal Data Protection Division in the framework of his/her duties in connection with issues of personal data, as these stem from the European Data Protection Regulation.
- xi. It shall evaluate the Report of the Head of the Information Security and Personal Data Protection Division, in connection with issues of personal data.

Digital Operational Resilience and Compliance with Regulation (EU) 2022/2554 – DORA, and any other applicable regulatory framework

The Risk Committee is responsible for overseeing the Bank's compliance with Regulation (EU) 2022/2554 on digital operational resilience. In this context:

- i. Monitors and evaluates the implementation of the ICT risk and security management framework, ensuring its integration into the Bank's overall risk management framework.
- ii. Oversees the management of cybersecurity incidents and the effectiveness of reporting and response mechanisms.
- iii. Reviews the adequacy of procedures for overseeing risks arising from third-party technology providers.
- iv. Monitors the conduct of business continuity and recovery testing, as well as the evaluation of their outcomes.
- v. Recommends to the Board of Directors the approval of relevant policies and procedures, ensuring they meet the requirements of the Regulation and are integrated into the broader corporate governance framework.

Monitoring of non-performing exposures

In cooperation with the competent Divisions/ Bodies of the Bank, it shall:

- i. Evaluate at regular intervals and at least on a six-monthly basis and refer to the Board of Directors for final approval, the Arrears Management Strategy for the Wholesale and Retail Banking Sectors and its basic assumptions and admissions and shall submit the revised strategy to the Central Bank of Cyprus.
- ii. Monitor the submission of the required proposals on arrears for amending the Business Plans and Budget.
- iii. Monitor the submission of reports in connection with the management of exposures in arrears.
- iv. Monitor the Business Plan and refer it for approval to the Board of Directors.

The Committee shall comply with the Guidelines of the European Central Bank which refer to the measures, procedures and best practices that banks must follow in the framework of managing non-performing loans.

In particular, the Committee shall implement the following:

- i. Revise at regular intervals and approval on an annual basis the framework for managing and treating non-performing loans.
- ii. Monitor the implementation of the above framework.
- iii. Define management priorities (including quantitative targets) and the goals for the activities and actions for managing non-performing loans.
- iv. Monitor periodically (at least quarterly) the progress of works as against the goals and the fundamental principles laid down in the framework for managing non-performing loans.
- v. Set appropriate procedures for making decisions in connection with the management of non-performing loans, which are submitted.
- vi. Evaluate and propose for approval by the Board of Directors, policies in the framework for managing non-performing loans and ensure that these policies are fully understood by the Bank's staff.
- vii. Ensure adequate internal audits of administrative procedures in connection with the aforementioned framework (particularly in connection with the classification of non-performing loans, provisions, valuations, and the viability of restructurings).

Ensure that the Bank's management executives who are responsible for the framework for managing non-performing loans possess the necessary experience and skills.

*Other duties and responsibilities*

The Committee shall:

- i. Conduct self-evaluations and submit to the Board of Directors reports with the conclusions and suggestions for improvements and changes.
- ii. Provide advice in connection with the placement of external consultants for risk management issues, whom the Board of Directors might decide to appoint to provide consultancy or support services.
- iii. Ensure the availability of funds in and out of the Bank which are required for supporting its work.
- iv. The Committee shall cooperate and communicate with the Audit Committee, in connection with the effective supervision of the limitation of certain basic risk and management areas, including climate risks and other risks related to the Environmental, Social and Governance areas and capital management and their effects of on the Internal Audit System.
- v. Submit its annual, and semi-annual Activity Reports to the Risk Management Committee of the Alpha Bank S.A.