TERMS OF REFERENCE OF THE GROUP BOARD RISK COMMITTEE

Title	**Terms of Reference of the Group Board Risk Committee**
Revision Number	8
Classification	Internal Use
Applicability	Group Board Risk Committee
Owner	Compliance Division
Reviewer(s)	Group Board Risk Committee
Approved by	Board of Directors
Issuing Date	29/11/2023
Effective Date	29/11/2023
Related Policies and Circulars	Corporate Governance Policy and Framework

Revision Table

Version	Approval Date	Initiator	Approver	Description / Changes
1.	2016	Compliance Division	Board of Directors	Revision
2.	2017	Compliance Division	Board of Directors	Revision
3.	2018	Compliance Division	Board of Directors	Revision
4.	2019	Compliance Division	Board of Directors	Revision
5.	2020	Compliance Division	Board of Directors	Revision
6.	2021	Compliance Division	Board of Directors	Revision
7.	2022	Compliance Division	Board of Directors	Revision

Version	Approval Date	Initiator	Approver	Description / Changes
8.	2023	Compliance Division	Board of Directors	Revision

TABLE OF CONTENTS

1. ABBREVIATIONS

Within this document, the following abbreviations are used:

Abbreviation	Explanation
AC	Audit Committee.
Bank	Bank of Cyprus Holdings Public Limited Company (BOCH) and its subsidiary Bank of Cyprus PCL.
Board	The Board of the Bank.
CBC	Central Bank of Cyprus.
CET1	Common Equity Tier 1.
CMRC	Crisis Management and Response Committee.
Chair	The Chair of the Committee.
Committee	Group Risk Committee.
ExCo	Executive Committee.
CISO	Chief Information Security Officer.
CRO	Chief Risk Officer.
FX	Foreign Exchange.
Group	Bank and all its subsidiaries.
HRRC	Human Resources & Remuneration Committee.
ICAAP	Internal Capital Adequacy Assessment Process.
ILAAP	Internal Liquidity Adequacy Assessment Process.
IRRBB	Interest Rate Risk in the Banking Book.
RC	Risk Committee.
OSP	Outsourcing Service Providers.
O-SII	Other Systemically Important Institutions.
SRT	Significant Risk Transfer.
Observer by invitation	A person who is not a committee member and does not have voting rights. He/she attends a meeting because he/she has some contribution to make to the meeting. For example, he/she may submit a report or make a presentation. The person may be a regular("standing") invitee or simply an invitee for particular item/s.
Observer in attendance	A person who is not a committee member, does not have voting rights and does not normally have speaking rights. He/she attends a meeting because of the position he/she holds, normally to be kept informed and/or to provide information and he/she may be invited by the Chair to speak in appropriate circumstances.
Observer-Visitor External	A person outside the organisation (external) who attends a committee for a specific topic following invitation by the Chair.

2. AUTHORITY

1. The Committee is a statutory Committee of the Board of the Bank from which it obtains its authority and to which it regularly reports.

2. The Committee has been delegated authority by the Board in respect of the functions and powers in these Terms of Reference.

3. The Committee is concerned with the business of the Bank, its business units, and subsidiaries, and accordingly its authority extends to all relevant matters relating to the Group.
4. The Committee has authority to investigate any matters within the scope of its terms of reference on whatever resources (including external professional or legal services) and to obtain such information as it may require from any director, officer, or employee of the Group. It shall have access to adequate funding to enable it to discharge its duties.

5. The Chair of the Committee (the "**Chair**") is authorised to provide to this respect approval of expenditure up to a maximum of €20.000 and he/she is required to inform the Committee at the next meeting.

6. For other risk-related engagements the Chair of the Committee is authorised to provide preliminary approval up to €150.000 with the requirement that upon such approval all Committee members are notified (through an e-mail) and they provide their positive confirmation.

7. The Committee reviews annually the Terms of Reference and recommends necessary amendments to the Board.

8. Although the Board has delegated authority to the Committee (including such matters that may be considered and reviewed independently from the executive Directors), the Board as a whole retains ultimate responsibility for the proper and adequate risk management of the Group (including the assessment of applicable risks and setting the Group's risk appetite) and it should reach its own conclusions regarding the reports and recommendations it receives.

3. ROLE OF THE COMMITTEE

The main purpose of the Committee is to review, on behalf of the Board, the aggregate Risk Profile of the Group, including performance against Risk Appetite for all risk types and ensure both Risk Profile and Risk Appetite remain appropriate. Specifically, it will:

1. Assist the Board in overseeing the implementation of the Group's risk strategy and the corresponding limits set.

2. Oversee the identification, assessment, control and monitoring of financial / economic risks and non-financial risks (including operational, technological, legal, reputational, compliance and ESG risks including climate-related & environmental risks (C&E)), which the Group faces in cooperation with the responsible Board Committees.

3. Advise and support the Board regarding the monitoring of the Group's overall actual and future risk appetite and strategy to ensure that they are in line with the business strategy, objectives, corporate culture, and values of the Group.

4. Consider, challenge, and recommend to the Board for approval the Group's overall Risk Appetite.

5. Review the aggregated Risk Profile for the Group and performance against Risk Appetite and report its conclusions to the Board.

6. Identify the potential impact of emerging issues and themes that may affect the Risk Profile of the Group.
7. Ensure that the Group's overall Risk Profile and Risk Appetite remain appropriate given the evolving external environment, the Group's character, and the internal control environment.

8. Seek to identify and assess future potential risks which, by virtue of their uncertainty, of low probability and unfamiliarity may not have been factored adequately into review by other Board Committees.

9. Ensure effective and on-going monitoring and review of the Group's management or mitigation of risk, including the Group's control processes, training and culture, information and communication systems and processes for monitoring and reviewing their continuing effectiveness.

10. Oversee the implementation of the strategies for capital and liquidity management as well as for the overall risks of the Group to assess their adequacy against the approved risk appetite and strategy and to evaluate the adequacy of the forecasts and the effectiveness of the strategies and policies regarding maintenance, in continuous basis, sufficient amounts, types and distribution of internal capital and equity to cover the risks of the Bank.

11. Ensure the effective management of all risks associated with outsourcing.

12. Provide recommendations to the Board on necessary adjustments to the risk strategy resulting from, inter alia, changes in the business model of the Bank, market developments or recommendations made by the risk management Division.

13. The Risk Management Division reports to the Board through the Committee.

4. COMMITTEE COMPOSITION

1. The Committee shall comprise of at least three members. The Committee must consist entirely of independent non-executive Directors who possess individually and collectively adequate knowledge, skills, and expertise to fully understand and monitor the risk strategy and the risk appetite of the Group as well as its risk management and control practices.

2. The Committee shall be chaired by a non-executive independent member of the Board.

3. The Committee shall interact with other committees appropriately. Such interaction shall take the form of cross-participation so that the Chair or a member of the Committee could also be a member of another committee (e.g. the Chairs of the Committee and the AC can respectively be members of the AC and the Committee, however, any further cross-participation of other members should be avoided as this could be classed as overlap).

4. The Chair cannot be the Chair of the Board or the chairperson of any other statutory Committee of the Board.

5. The Board appoints the members of the Committee annually and on an ad hoc basis on the recommendation of the NCG Committee in consultation with the Chair of the Committee.

6. The Board appoints a Chair for a maximum period of six years whether consecutive or not.

5. COMMITTEE MEETINGS

1. The Committee holds regular meetings, at least four (4) per year and additionally, ad hoc meetings whenever called by the Chair of the Committee.

2. As a general rule, notice of meetings together with the agenda and support material of the items to be discussed shall be forwarded to each member of the Committee or any other person required or invited to attend no later than five (5) working days before the date of the meeting.

3. The Company Secretary or his/her nominee shall record and maintain detailed minutes of the meetings of the Committee, including noting the names of those present and in attendance. Draft minutes must be finalised no later than fifteen (15) business days following the meeting, formally approved at the next meeting, and at the same time be submitted to the Board for noting.

4. The quorum for a meeting is two (2) members or 50% rounded up, whichever is the highest.

5. Questions arising at any meeting shall be decided by a majority of votes. In case of an equality of votes the Chair shall have a second or casting vote.

6. The Board's directions for minimum annual attendance requirements for Committees of the Board require Committee members to participate in at least $^{3}/_{4}$ of all meetings (regular and extraordinary) and that any continuous absences not to exceed 2 in number.

7. The CRO is a regular observer by invitation. Based on the nature of their duties as Heads of Internal Control Functions, the Chief Compliance Officer, the CISO and the Internal Audit Director are also considered observers by invitation attending only if a topic related to their function is discussed and they have been invited by the Chair.

8. No person other than a committee member is entitled to attend meetings of the Committee, although others may attend as observers by invitation of the Chair e.g. other Directors that are not members of the Committee, members of the management of the Group or external parties, in order to be informed or to advise or inform the Committee on any agenda issues. Any such persons are present only during the discussion of the specific items and leave the meeting room immediately after, without any participation in the decision-making processes.

9. The Committee shall annually establish a schedule of major topics to be discussed during the year.

10. Decisions beyond this Committee's authority and matters which any member of the Committee deems necessary for escalation will be escalated by the Chair to the Board as appropriate.

6. RESPONSIBILITIES

6.1. Risk Appetite and Strategy

6.1.1. Review management proposals on the desired risk strategy of the Group, in each area of risk (e.g. market, liquidity, credit, equity, regulatory, information security, operational reputational, ESG, digital and capital resources, and ESG, including C&E risks), oversee its implementation, in order to assess its adequacy against the approved risk appetite and strategy and make appropriate recommendations to the Board.

6.1.2. Advise and support the Board on the Group's overall actual and future risk appetite and strategy, taking into account all types of risk, to ensure they are in line with the business strategy, objectives, corporate culture and values of the institution.

6.1.3. Determine the nature, the amount, the format, and the frequency of the information on risk that the Committee desires to receive on the risk position of the Group and, if appropriate of each business unit in order to properly carry out its roles to review, monitor and provide assurance or recommendations to the Board in its areas of responsibility and when there are gaps, how they are to be addressed.

6.1.4. Ensure that risk parameters and risk models developed and used to quantify risk exposures are subject to periodic independent validation.

6.1.5. Evaluate the Group's governance, risk and control framework and oversee its integration with the Bank's decision-making process, covering the whole spectrum of the Bank's activities and units as well as subsidiaries.

6.1.6. Assist the Board in setting the Group’s risk culture and liaise with the ECCC re communicating it to management.

6.1.7. Submit to the Board proposals and recommendations for corrective action whenever weaknesses are identified in implementing the risk strategy resulting from, inter alia, changes in the business model of the institution, markets developments or recommendations made by the Risk Management Division.

6.1.8. Regularly monitor and ensure compliance of the Group with the adopted risk strategy by reviewing exception reports prepared by the Risk Management Division and any other information the Committee considers, necessary and make recommendations to and inform the Board on the significant risks to which the Bank is exposed.

6.1.9. Examine whether incentives provided by the remuneration system take adequately into consideration risk, capital, liquidity and the likelihood and timing of earnings without prejudice to the tasks of the HRRC.

6.1.10. Examine management reports concerning changes anticipated in the economic and business environment, or major internal changes and the extent to which they affect the Group's risk profile and appetite and make appropriate recommendations to the Board.

6.1.11. Carry out robust assessment of the Group’s emerging and principal risks. Focus should be given to those risks that given the Group’s current position, could threaten the Group’s business model, future performance, solvency, or liquidity, irrespective of how they are classified or from where they arise.

6.1.12. Examine high-risk transactions and make recommendations to the Board.

6.1.13. Examine the adequacy and effectiveness of the contingency and insurance strategy of the Group and make appropriate recommendations to the Board.

6.1.14. Review the composition, authorities, duties and responsibilities and effectiveness of other Risk Committees, where such Committees are appointed, that function within the Group and make recommendations to the respective subsidiary Board for rectification.

6.1.15. Assist the Board in overseeing the effective implementation of the risk strategy by senior management, including the development of mechanisms to ensure material exposures that are close to, or exceed approved risk limits are managed and where necessary, mitigated in an effective and timely manner and the identification and escalation of breaches in risk limits and of material risk exposures in a timely manner.

6.1.16. Oversee the alignment between all material financial products and services offered to clients and the business model and risk strategy of the Bank.

6.1.17. Assess the risks associated with the offered financial products and services taking into account the alignment between the prices assigned to and the profits gained from those products and services. Where the prices do not properly reflect the risks in accordance with the business model and the risk strategy, the Committee shall present a remedy plan to the Bank.

6.1.18. Assess and monitor the independence, adequacy and effectiveness of the Risk Management Division and the Information Security function and advice the Board accordingly including on the adequacy and effectiveness of overall risk appetite and Information Security frameworks, which, inter alia, ensures the adequate protection of confidential and personal information of the Bank.

6.1.19. Assess the recommendations of internal or external auditors relevant to Risk Management or InfoSec matters and follow up on the appropriate implementation of measures taken.

6.1.20. Provide advice on the appointment of external consultants that the Board may decide to engage for advice or support.

6.1.21. Report to the Board any current and emerging topics relating to ESG risks and matters, including C&E risks and matters that are expected to materially affect the business. Operations, performance, or public image of the Group or are otherwise pertinent to the Group and its stakeholders and if appropriate, detail actions taken in relation to the same.

6.1.22. The Committee is responsible for the oversight of the whole Group but may delegate tasks to subsidiary risk committees to avoid duplication.

6.2. Risk Policies and Systems

6.2.1. Jointly with AC review provisions proposals of management and other topics of common/shared responsibility and make appropriate recommendations to the Board in relation to the adequacy of these provisions and the methodology adopted.

6.2.2. Review and recommend to the Board for approval the Annual Risk Report and the Annual Information Security Risk Report.

6.2.3. Advice the Board, drawing on the work of the Audit Committee, the Risk Management Division, Information Security function and external auditors, on the adequacy and effectiveness of the Risk Management and Information Security Policies and Framework.

6.2.4. Advise the Board, drawing on the work of the Audit Committee, the Risk Management Division, Information Security function and external auditors, on the adequacy and robustness of information and communication systems to enable identification, measurement, assessment, and reporting of risk in a timely and accurate manner and ensure the adequate protection of the institution's confidential and proprietary information.

6.2.5. Determine the principles that should govern the management of risks, (including ESG and C&E risks) through the establishment of appropriate Risk Policies.

6.2.6. Approve all such risk policies.

6.2.7. Advise the Board, drawing on the work of the AC, the CRO and external auditors, on the adequacy of capital resources in relation to the level of undertaken risks with respect to maintaining on an ongoing basis, amounts, types, and distribution of both the internal capital and own funds adequate to cover the risks to the institution.

6.2.8. Monitor and ensure compliance of the Group with risk management policies, and regulatory requirements and make appropriate recommendations to the Board.

6.2.9. Review, evaluate and make any relevant recommendations to the Board on the ICAAP report which aims to assess all important risks undertaken by the Group and determine capital requirements of the Group. Ensure that the risk profile of the Group is in line with the risk appetite and capital planning approved by the Board.

6.2.10. Review, evaluate and make relevant recommendations to the Board on the ILAAP report which aims to assess all risk to the liquidity of the Group and ensures that the risk profile of the Group is in line with the liquidity adequacy of the Group and its strategic plans.

6.2.11. Ensure that the O-SII buffer is maintained within the limits set by the Central Bank on an individual and consolidated basis, and which consists of and is supplementary to CET1 Capital.

6.2.12. Ensure that stress tests and related procedures are carried out as appropriate on all major risks, at least on an annual basis and where necessary, challenge the appropriateness of limits and adequacy of capital and budgets.

6.2.13. Review a number of possible scenarios, including stressed scenarios, to assess how the institution’s risk profile would react to external and internal events.

6.2.14. Review and recommend for approval to the Board the Recovery Plan and any revisions thereof.

6.2.15. Oversee the SRT framework, monitor compliance with the SRT Policy, review SRT transactions and make recommendations to the Board for approval.

6.2.16. Have access to all relevant information and data necessary to perform its role including information and data from relevant corporate and control functions, for instance legal, financial, human resources, risk, Information and Communication Technology (ICT), and information security, audit, and compliance.

6.2.17. Jointly with the AC oversee information on regulatory compliance, to prevent and combat money laundering, including access to aggregate information.

6.2.18. Assess stress situations escalated by the ExCo through the review and assessment of the recovery and early warning indicators and decide whether to escalate further to the Board with a recommendation to declare a 'Recovery Emergency Situation' and perform an assessment of the Recovery Options.

6.2.19. Recommend to the Board to assign responsibility to the CMRC for the implementation of the Recovery Plan.

6.2.20. Review and monitor key enterprise wide ESG including C&E , metrics, targets, KPIs, KRIs and related goals and monitor the progress towards achieving targets and benchmarks.

6.2.21. Receive and review periodic reports from management on ESG and climate trends, issues, and risks, including developments in applicable regulations, as well as the corresponding mitigation initiatives and controls.

6.2.22. Review on an ongoing basis whether existing policies comprehensively cover climate and environmental risks, including the credit policies for each sector and product.

6.2.23. Review and approve the budgets of the Risk Management Division and Information Security function, ensuring that they are sufficiently flexible to adapt to variations in response to developments.

6.2.24. Evaluate the CRO and the CISO and recommend to the Board, as appropriate, their appointment, replacement, reassignment, or dismissal. Carry out their annual appraisals and submit them to the Board.

6.2.25. Oversee the Outsourcing Framework and ensure effective managing of all risks associated with outsourcing.

6.2.26. Review any planned changes regarding OSPs and the potential impact of these changes on the critical or important functions.

6.2.27. Obtain a report summarising the risk analysis, including legal risk, compliance with regulatory requirements and the impact on service levels relevant to the above changes.

6.2.28. Obtain adequate assurance that:

a. the Senior Executive Management fully comprehends and applies the acceptable risk-taking levels, as defined by the Board,
b. all employees comprehend and apply the risk taking and risk management policy and

c. excessive risk-taking is not encouraged.

6.2.29. Ensure that submissions by the Risk Management Division, the Compliance Division, the Information Security Function, and everyone else are appropriately documented.

6.2.30. The Risk Committee should meet periodically with the Audit and other risk-relevant Committees to ensure effective exchange of information and effective coverage of all risks, including emerging risks and any needed adjustments to the risk governance framework of the Group in the light of its business plans and the external environment.

6.2.31. Conduct a self-assessment and report to the Board the Risk Committee's conclusions and recommendations for improvements and changes.

6.3. Approval of Loans and Limits

6.3.1. The Committee will review and/or approve special or urgent cases of loans, write-offs, DFAs and other Credit Risk requests as these may be submitted by CC3 and as per delegated authorization levels by the Board and above authorities delegated to management.

6.3.2. Review and approve or recommend to the Board for approval changes to market and other nonfinancial risk limits not delegated to the Management Committees.

6.4. Communication and Reporting

6.4.1. Ensure adequate coordination/communication exists between the Board and the management on risk management and information security issues.

6.4.2. Liaise with other Committees of the Board as appropriate, including with the HRRC in relation to the remuneration of persons within the Group's risk management and information security functions.

6.4.3. Formulate the Annual Risk Committee Report included in the Annual Corporate Governance Report of the Group, which should include the following:

a) Confirmation that the Risk Committee has carried out a robust assessment of the principal risks and uncertainties facing the Group, including those that would threaten its business model, future performance, solvency, or liquidity.
b) An explanation of these risks and how the Group has managed and mitigated such risks during the period.
c) An assessment of the adequacy and effectiveness of the Group's risk management and internal control systems during the previous year.
d) An assessment of the appropriateness of limits of risks and the adequacy of provisions and capital.
e) An indication of the Committee's membership, the number of its meetings and attendance over the year and its main activities.

6.4.4. Examine and approve the circumstances under which the Chair can communicate directly with the main shareholders.

6.4.5. Respond, through the Chair, to shareholder questions regarding Group risk management issues at the Annual General Meeting.

6.4.6. Report to the Board regularly on how the Committee discharges its responsibilities and, on the nature, and content of discussion at Committee meetings, recommendations, and actions to take.

6.4.7. The CRO and the CISO will meet regularly with the Chair and will have the right and responsibility to elevate issues to the Chair where they consider it necessary in the furtherance of their responsibilities.

6.4.8. The Chair shall arrange to hold an annual conference call with all chairpersons of subsidiary Audit & Risk Committees and shall report to the Board any concerns.

6.4.9. Annually obtain and review the report on risk committee performance of each major subsidiary and take appropriate action.

6.4.10. Ensure that the Committee's terms of reference are available on the Group's official website.

7. DELEGATION OF AUTHORITIES BY THE MAIN BODY OF THE BOARD OF DIRECTORS

The following matters are delegated by the Board to the Committee:

7.1. Approval of all Group risk management, information security, data protection and ESG policies.
7.2. Approval of the policies governing charitable and political donations and environment.
7.3. Approval of the Group Outsourcing Policy.
7.4. Approval of the Reputational Risk and market risk Policy.
7.5. Approval of credit limits above management threshold and below Board threshold.