



BOARD RISK COMMITTEE TERMS OF REFERENCE

April 2022

TABLE OF CONTENTS

A.	AUTHORITY	3
B.	ROLE OF THE COMMITTEE	3
C.	COMMITTEE COMPOSITION	4
D.	COMMITTEE MEETINGS	5
E.	RESPONSIBILITIES	6
	1. <i>RISK APPETITE AND STRATEGY</i>	6
	2. <i>RISK POLICIES AND SYSTEMS</i>	8
	3. <i>APPROVAL OF LOANS AND LIMITS</i>	10
	4. <i>COMMUNICATION AND REPORTING</i>	10
	5. <i>REGULATORY FRAMEWORK</i>	11
F.	DELEGATION OF AUTHORITIES BY THE MAIN BODY OF THE BOARD OF DIRECTORS	11

List of Abbreviations

Abbreviation	Explanation
AC	Audit Committee
CBC	Central Bank of Cyprus
CET1	Common Equity Tier 1
CMRC	Crisis Management and Response Committee
ECCC	Ethics, Conduct and Culture Committee
CISO	Chief Information Security Officer
CRO	Chief Risk Officer
ESG	Environmental, Social and Governance
FX	Foreign Exchange
Group	Company and all of its subsidiaries (including the Bank)
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

A. AUTHORITY

1. The Board Risk Committee ("**the Committee**") is a Committee of the Board of Directors ("**the Board**") of the Bank of Cyprus Holdings Plc ("**the Company**") 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 Company, its business units and subsidiaries (the Company and its subsidiaries being "the Group") and accordingly its authority extends to all relevant matters relating to the Group.
4. The Committee has authority to investigate any matters within 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 Chairperson 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 Chairperson 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 changes to the Board.
8. Although the Board has delegated authority to the Committee as referred to above (including such matters that may be considered and reviewed independently from the executive Directors), the Board as a whole retains ultimate responsibility for the risk management of the Company (including the assessment of applicable risks and setting the Company's risk appetite) and it should reach its own conclusions regarding the reports and recommendations it receives.

B. 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:

- Assist the Board in overseeing the implementation of the Group's risk strategy and the corresponding limits set;
- Identify, assess, control and monitor financial / economic risks and non-financial risks (including operational, technological, tax, legal, reputational, and compliance, and ESG risks) which the Group faces in cooperation with the responsible Board Committees;

-
- Consider, challenge and recommend to the Board for approval the Group's overall Risk Appetite;
 - Review the aggregated Risk Profile for the Group and performance against Risk Appetite and report its conclusions to the Board;
 - Identify the potential impact of key issues and themes that may affect the Risk Profile of the Group;
 - Ensure that the Group's overall Risk Profile and Risk Appetite remain appropriate given the evolving external environment, any key issues and themes impacting the Group and the internal control environment;
 - 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; and
 - 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;
 - Ensure the effective management of all risks associated with outsourcing.

C. COMMITTEE COMPOSITION

1. The Committee has a minimum of 3 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. To ensure coordination with the work of other Board Committees the operations of which may have impact on the risk strategy of the Group, e.g. the AC and the HRRC, the Chairperson of the RC should be a member of the AC and the Chair of the AC should be a member of the RC. Additionally, one member of the RC should be a member of the HRRC.
3. The Chairperson of the committee cannot be the Chair of the Board or the chairperson of any other statutory Committee of the Board.
4. The Board appoints the members of the Committee annually on the recommendation of the NCG Committee in consultation with the Chairperson of the Committee.
5. The Board appoints a Chairperson of the Committee for a maximum period of six years whether consecutive or not.
6. The induction programme shall cover the role of the Committee (including its terms of reference and expected time commitment of its members).

D. COMMITTEE MEETINGS

1. The Committee holds regular meetings, at least 4 per year and additionally, ad hoc meetings whenever called by the Chairperson of the Committee.
2. 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 5 working days before the date of the meeting.
3. The Chairperson of the Committee (using the services of the Company Secretary to the extent necessary and appropriate) ensures that:
 - (a) the Agenda appropriately addresses the issues that require the Committee's attention and is proactive;
 - (b) the Committee members are provided with information in a timely manner in order to effectively consider and decide on the agenda issues and to keep the Committee focused on its primary oversight responsibilities;
4. The Committee shall have access to the services of the Company Secretary, who has the responsibility of ensuring that the Committee receives information and papers in a timely manner. 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.
5. The quorum for a meeting is 2 members or 50% rounded up, whichever is the highest.
6. Questions arising at any meeting shall be decided by a majority of votes. In case of an equality of votes the Chairperson shall have a second or casting vote.
7. The Board's directions for minimum annual attendance requirements for Committees of the Board require Committee members to participate in at least $\frac{3}{4}$ of all meetings (regular and extraordinary) and that any continuous absences not to exceed 2 in number.
8. Regular Attendee of the Committee is the Chief Risk Officer. Based on the nature of their duties as Heads of Internal Control Functions, the Director Compliance, the CISO and the Internal Audit Director are also considered as regular attendees but shall attend only if a topic related to their function is discussed and they have been invited by the Committee's Chairperson.
9. No person other than a member of the Committee is entitled to attend meetings of the Committee, unless invited by the Committee. The Chairperson of the Committee is entitled to invite other Directors that are not members of the Committee, members of the management of the Group or external parties to participate in a meeting, in order to advise or inform the Committee on the issues discussed at the meeting. 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.

-
10. Each member /attendee is personally responsible / liable to declare any conflicts of interest and abstain from the meeting during which the conflicted issue is under discussion. The Secretary of the Committee maintains a relevant section in the Committee minutes.
 11. The Committee shall annually establish a schedule of major topics to be discussed during the year.
 12. 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.

E. RESPONSIBILITIES

1. *Risk Appetite and Strategy*

- Review management proposals on the desired risk strategy both at individual company as well as at Group level, in each area of risk (market, liquidity, credit, equity, regulatory, information security, operational and capital resources), oversee its implementation, in order to assess its adequacy against the approved risk appetite and strategy and make appropriate recommendations to the Board.
 - Advise and support the Board regarding 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.
 - Determine the nature, the amount, the format, and the frequency of the information on risk that the Committee desires to receive on the risk situation of the Group and of each type of risk and 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.
 - Approve metrics or a process to satisfy the Committee that the risk reports and information the Committee receives are accurate, comprehensive, sufficient, objective and depict an appropriate view of the institution's risk profile.
 - Ensure that risk parameters and risk models developed and used to quantify risk exposures are subject to periodic independent validation.
 - 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.
 - Assist the Board in setting the Company's risk culture and liaise with the ECCC re communicating it to management-
-

-
- 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.
 - Regularly monitor and ensure compliance of the Group with the adopted risk strategy by reviewing reports prepared by the Risk Management Division (such as Country Risk violations etc), 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.
 - 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.
 - 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.
 - 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.
 - Examine high-risk transactions and make recommendations to the Board.
 - Examine the adequacy and effectiveness of the contingency and insurance strategy of the Group and make appropriate recommendations to the Board.
 - 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.
 - 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.
 - Review whether prices of liabilities and assets offered to clients take fully into account the Group's business model and risk strategy. Where prices do not properly reflect risks in accordance with the business model and risk strategy, the Risk Committee shall present a remedy plan to the Board.
 - Assess and monitor the independence, adequacy and effectiveness of the Risk Management Division and the Information Security function and advise 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.

-
- Review and recommend to the Board for approval the Annual Risk Report and the Annual Information Security Risk Report.
 - 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 effectiveness of the Risk Management and Information Security Framework.
 - 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.
 - 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.
 - Provide advice on the appointment of external consultants that the Board may decide to engage for advice or support.
 - Report to the Board any current or emerging topics relating to ESG matters that are expected to materially affect the business, operations, performance, or public image of the Company or are otherwise pertinent to the Company and its stakeholders and if appropriate, detail actions taken in relation to the same.
 - The Committee is responsible for the oversight of the whole Group but may delegate tasks to subsidiary risk committees to avoid duplication.

2. *Risk Policies and Systems*

- Determine the principles that should govern the management of risks, through the establishment of appropriate Risk Policies.
- Approve all such risk policies.
- Advise the Board, drawing on the work of the AC, the CRO and external auditors, on the adequacy and effectiveness of risk management policies, processes, systems and controls of the Group, including the appropriateness of limits, the adequacy of provisions and in general, 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.
- Monitor and ensure compliance of the Group with risk management policies, and regulatory requirements and make appropriate recommendations to the Board.
- 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.
- 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.

-
- 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
 - 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.
 - Review a number of possible scenarios, including stressed scenarios, to assess how the institution's risk profile would react to external and internal events.
 - Review and recommend for approval to the Board the Recovery Plan and any revisions thereof.
 - Review and recommend to the Board for approval changes to limits (e.g. Value at Risk, stop loss and position limits for FX, the IRRBB etc).
 - Oversee the SRT framework and monitor compliance with the SRT Policy.
 - Review SRT transactions and make recommendations to the Board for approval.
 - 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.
 - Recommend to the Board to assign responsibility to the CMRC for the implementation of the Recovery Plan.
 - Review and discuss with management the Company's overall ESG strategy, including considering whether the Company should initiate any additional ESG actions or engage with any stakeholders regarding potential key ESG matters.
 - Review and monitor key enterprise-wide ESG metrics, targets, key risk indicators and related goals and monitor the progress towards achieving targets and benchmarks.
 - Receive and review periodic reports from management on ESG trends, issues and risks, including developments in applicable regulations, as well as the corresponding mitigation initiatives and controls.
 - 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.
 - 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.
 - Oversee the Outsourcing Framework and ensure effective managing of all risks associated with outsourcing and:
 - Review any planned changes regarding OSPs and the potential impact of these changes on the critical or important functions.

-
- 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.
 - Obtain adequate assurance that:
 - the Senior Executive Management fully comprehends and applies the acceptable risk-taking levels, as defined by the Board,
 - all employees comprehend and apply the risk taking and risk management policy and
 - excessive risk-taking is not encouraged.
 - Ensure that communication by the Risk Management Division, the Compliance Division and the Information Security Function is adequately documented.
 - 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.
 - Conduct a self-assessment and report to the Board the Risk Committee's conclusions and recommendations for improvements and changes.

3. *Approval of Loans and Limits*

The Committee will review and/or approve special or urgent cases of loans, write-offs, DFAs as these may be submitted by CC3 and as per delegated authorization levels by the Board.

4. *Communication and Reporting*

- Ensure adequate coordination/communication exists between the Board and the management on risk management issues.
- Formulate the Annual Risk Committee Report included in the Annual Corporate Governance Report of the Group, which should include the following:
 - 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.
 - An explanation of these risks and how the Group has managed and mitigated such risks during the period.
 - An assessment of the adequacy and effectiveness of the Group's risk management and internal control systems during the previous year.
 - An assessment of the appropriateness of limits of risks and the adequacy of provisions and capital.
 - An indication of the Committee's membership, the number of its meetings and attendance over the year and its main activities.
- Examine and approve the circumstances under which the Chairperson of the Committee can communicate directly with the main shareholders.
- Respond, through the Chairperson of the Committee, to shareholder questions regarding Group risk management issues at the Annual General Meeting.

-
- 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.
 - The Chief Risk Officer will meet regularly with the Chairperson of the Committee and will have the right and responsibility to elevate issues to the Chairperson where he/she considers it necessary in the furtherance of his/her responsibilities.
 - The Chairperson of the Committee shall arrange to hold an annual conference call with all chairpersons of subsidiary Audit & Risk Committees and shall report to the Board any concerns.
 - Annually obtain and review the report on risk committee performance of each major subsidiary and take appropriate action.
 - Ensure that the Committee's terms of reference are available on the Company's official website.

5. *Regulatory Framework*

As per *Section R of the Board Manual*

F. **DELEGATION OF AUTHORITIES BY THE MAIN BODY OF THE BOARD OF DIRECTORS**

The following matters are delegated by the Main Body of the Board of Directors to the RC:

- Approval of all Group Risk Management Policies and Information Security Policies.
- Approval of the policies governing charitable and political donations, citizenship and environment.
- Approval of the Group Outsourcing Policy
- Approval of the Reputational Risk Policy

The RC Chairperson will be responsible for presenting in summary to the Main Body of the Board the various decisions taken on matters delegated to the Risk Committee by the Board.

Any such delegation is without prejudice to the responsibility of the Board as a whole for all risk assessment, appetite and management issues.