GROUP POLICY: COMPLIANCE

POLICY IDENTIFICATION

Title	**Group Compliance Policy**
Policy Number	**CD402**
Revision Number	12
Classification	Public Use
Applicability	Group
Owner	Compliance Division
Reviewer(s)	Internal Audit Division, Risk Management Division
Approved by	Audit Committee
Issuing Date	02/05/2011
Effective Date	02/05/2011
Related Policies and Circulars	Group Corporate Governance Policy, Operational Risk Management Policy, Fraud Risk Management Policy, Anti-Bribery and Corruption Group Policy, Conflicts of Interest Group Policy, Information Security Policy, Group Whistleblowing Policy, Risk Appetite Framework, Group Policy Relating to Prevention of ML and TF, Group Customer Acceptance Policy, Group Sanctions Policy, Reputational Risk Management Policy, Group Customer Complaints Management Policy, Business Continuity Management Policy, New Products/Services Management Policy, Third Party and Outsourcing Risk Management Policy, Control Functions Common Operational Framework, Regulatory Compliance Manual, Organisational Circular 099 on Operational and Reputational Risk Management, Compliance Charter, Group Personal Data Protection Policy, Treating Customers Fairly Group Policy, Compliance Charter, Compliance Division Review Methodology.

Revision Table

Version	Approval Date	Initiator	Approver	Description / Changes
1.0	02/05/2011	Compliance Division	Audit Committee	Initial Write up
2.0	20/01/2015	Compliance Division	Audit Committee	
3.0	23/11/2015	Compliance Division	Audit Committee	Paragr.1 - Introduction of the official Group Compliance Mission Statement Paragr. C - The introduction and maintenance of the Regulatory Compliance Matrix. Paragr. C - The relationship with Regulatory Steering Group and the supporting role provided by the RSCO Appendix 1 - Corporate Governance issues are introduced. Paragr. E - The official assessment of Local Compliance Officers Appendix 1 - Obligations in relation to complaints management Paragr. 4 - The concept of Ethics has been incorporated in the Policy
4.0	12/12/2016	Compliance Division	Audit Committee	Minor revisions
5.0	11/12/2017	Compliance Division	Audit Committee	Minor revisions
6.0	13/12/2018	Compliance Division	Audit Committee	Minor revisions
7.0	30/11/2019	Compliance Division	Audit Committee	Minor revisions
8.0	29/06/2020	Compliance Division	Audit Committee	Minor revisions
9.0	30/08/2021	Compliance Division	Audit Committee	Minor revisions
10.0	24/01/2022	Compliance Division	Audit Committee	Changes as per the revised LCO framework, the appointment of the Chief Compliance Officer and the issuance by the Central Bank of Cyprus of the new Directive on Internal Governance of Credit Institutions dated October 2021.

Version	Approval Date	Initiator	Approver	Description / Changes
11.0	26/09/2022	Compliance Division	Audit Committee	Redrafting as per the new Policy template. No major changes since the Policy was updated on Jan22 following the issuance of the new CBC Internal Governance Directive.
12.0	24/10/2023	Compliance Division	Audit Committee	Minor revisions to define the role of the Subsidiary Compliance Officer (SCO) and the Business Risk and Control Officer (BRCO) which is a new established role within the Bank.

TABLE OF CONTENTS

1. PURPOSE AND SCOPE OF POLICY

The purpose of this policy is to set out the compliance framework that applies within the Bank (BOCH/BOC) and its subsidiaries. It sets out the business and legal environment applicable to the Bank of Cyprus Group as well as the objectives, principles, and responsibilities for compliance and how these responsibilities are allocated and carried out at group and entity level. Furthermore, this policy ensures that there are proper procedures in place for the Bank to comply with the requirements of the CBC Directive on "Internal Governance of Credit Institutions 2021" (the «CBC Directive») and the EBA Guidelines on Internal Governance (issued 26/9/2017).

This policy shall be read in parallel with the Compliance Charter and the Control Functions Common Operational Framework. The Policy is available to all staff through portal and on the website.

The content of this policy is mandatory and represents minimum standards which apply throughout the Bank which includes Bank of Cyprus Holdings PLC and its subsidiaries.

The compliance function establishes, implements, and maintains appropriate tools, mechanisms, and processes to:

1. Ensure:
   a. Effective control over the implementation of the policy.
   b. Time efficiency on all related processes.
2. Enable the Group to identify the relevant and applicable laws, rules, regulations, codes of conduct and standards of good practice, analyse the corresponding risks of non-compliance, and prioritize the Compliance Risks for mitigation and monitoring.
3. Identify, assess, manage, and monitor compliance risks.
4. Promote compliance awareness and the right compliance culture across the Group.
5. Enable the CD to conduct periodic onsite/offsite reviews with applicable laws, rules, regulations, and standards and provide recommendations / advice to management on measures to be taken to ensure compliance.
6. Provide regular compliance reporting to Senior Management, the Board, and authorities.
7. Facilitate the regular updating of compliance policies and procedures (at least annually) to incorporate changes in laws, regulations, and standards of good practice.

The below areas fall within the scope of compliance function (please refer to Appendix for a more detailed analysis):

1. Client related integrity risk.
2. Personal conduct related integrity risk.
3. Financial services conduct related integrity risk.
4. Organizational conduct related to integrity risk.
5. Organization, systems, procedures.

2. ABBREVIATIONS

Within this document, the following abbreviations are used:

Abbreviation	Definition
AC	Audit Committee
AML	Anti Money Laundering
BOC	Bank of Cyprus
BOCH	Bank of Cyprus Holdings
BOD	Board of Directors
CBC	Central Bank of Cyprus
CD	Compliance Division
CEO	Chief Executive Officer
CL	Compliance Liaison
CRAM	Compliance Risk Assessment Methodology
CySEC	Cyprus Securities and Exchange Commission
DPO	Data Protection Officer
EBA	European Banking Authority
ExCo	Executive Committee
FCSCD	Financial Crime & Sanctions Compliance Department
GDPR	General Data Protection Regulation
LCO	Local Compliance Officer
ML	Money Laundering
NCGC	Nominations & Corporate Governance Committee
ORM	Operational Risk Management
RAD	Regulatory Affairs Department
SCO	Subsidiary Compliance Officer
TF	Terrorism Financing

3. DEFINITION OF TERMS

For the purposes of this Policy, the terms listed below have the following meaning:

1. **Annual Compliance Program**
   A program sets out the compliance planned activities, such as the implementation and review of specific policies and procedures, compliance risk assessments, compliance assurance reviews, compliance testing and educating staff on compliance matters, corrective actions to address any control weaknesses that have been identified. The compliance program adopts a risk-based methodology.
2. **Bank of Cyprus Group/BoC Group**
   Means the Bank of Cyprus Ltd, its ultimate holding company and its subsidiaries.
3. **Business Risk and Control Officers**
   Dedicated persons assigned to promote and sustain a corporate culture of risk and compliance within the division as per the guidance received by the control functions.

4. **Compliance Chart/Authoritative Source**

   An updated register of the existing Regulatory Framework (laws, regulations, and self-regulatory standards) that affect the Bank and its subsidiaries. It is maintained by Compliance Division through the Compliance Management System based on new or amended regulations, guidelines and standards.

5. **Compliance Liaison Manager**

   The manager of the CL is responsible for overseeing the actions of the CL and providing any support required. CLs' managers and line directors are strongly encouraged to:

   a. Involve and consult CLs in all areas of the department that encompass compliance issues.
   b. Support them by (a) allowing access to all required information and (b) allocating sufficient time and tools to enable them to perform their role as Compliance Liaisons CLs.
   c. Agree targets and recognize their work and effort in the annual appraisal process.
   d. Approve certain CLs actions performed through the compliance system, as part of the four eyes principle.

6. **Compliance Liaisons**

   CLs are members of staff assigned with compliance responsibilities at the local level. As CLs they are part of the first line of defence when performing their duties in supporting their management in the implementation of regulatory changes, compliance issues and controls and adherence to Group compliance principles. As part of the first line of defence and as facilitators to the second line, they are responsible for identifying, measuring, monitoring, and reporting regulatory risks and ensuring compliance with internal and external regulatory requirements within their department.

   The CLs neither assume, nor undertake compliance function's activities / responsibilities and such mandate is clearly/effectively communicated. There is no delegation of the primary responsibilities of CD to the CLs.

7. **Compliance Risk**

   The risk of impairment to the organization's business model, reputation, and financial condition from failure to meet laws and regulations, internal standards and policies, and expectations of key stakeholders such as shareholders, customers, employees, and society.

8. **CRAM**

   The Compliance Risk Assessment Methodology (CRAM) provides a unified way to identify, assess, mitigate, and document compliance risks. The risk assessment is performed both on the inherent and residual risk based on impact/likelihood criteria. The risk assessment methodology is fully analyzed in the Compliance Division Review Methodology document and is fully aligned with the Group ORM Risk Assessment Scoring Methodology.

9. **Impact**

   The extent to which the compliance risk, if realized, would affect the ability of the entity or the Bank to deliver its strategy and objectives within a specified time horizon.

   Typically, impact assessment criteria may include financial, regulatory, health & safety, security, environmental, employee, customer, and other operational impacts. The potential impact of a risk is assessed by considering the potential direct damage (i.e., financial impact such a fines and penalties), as well as any other indirect consequences that may result from regulatory or reputational issues such as relations / service to clients, relations with mass media, impact on the Group's reputation, etc.

10. **Inherent Risk**

    The function of Impact X Likelihood, without taking into consideration particular controls in place, expressed on a scale of 1-25. Essentially, the inherent risk is the worst-case scenario of the risk under question.

11. Likelihood

Likelihood of occurrence refers to the possibility that a given event (compliance risk) materializes into a compliance event/incident within a specific time frame. The likelihood levels can be described as frequency values of risk events occurring, with reference to how easy it is for the underlying vulnerability to be exploited.

12. Local Compliance Officers (LCOs)

Dedicated LCOs with a direct functional reporting line to CD to strengthen compliance oversight and challenge. They are assigned to high- risk areas such as, Consumer Banking Division and CISCO, consolidated areas of the Finance Division and at the IBS for specific AML activities. Dedicated LCOs have the same responsibilities as CD staff and report directly to CD.

13. Regulatory Compliance Matrix / Risk Map

CD through the new compliance management system maintains a consolidated Risk Map i.e., a hierarchy of risks and controls that encompasses the entire regulatory framework (only laws and regulations from competent authorities, not policies) that affect the Group along with mitigating actions for the management of risks. The Risk Map reflects the status of compliance of each law which is monitored and updated on an ongoing basis by the Responsible Division's CL and Regulatory Compliance Department through the gap analysis of new or amended regulations, assessment of new products & services, incidents, operating models, complaints, findings from onsite/offsite compliance reviews, internal and external audit findings and investigations by regulatory authorities.

14. Regulatory Framework

Means laws, primary legislation, directives, rules and standards issued by legislators and supervisors, market conventions, codes of practice promoted by industry associations etc. These go beyond what is legal obligation and embrace broader standards of integrity and ethical conduct.

15. Residual Risk

The overall residual risk, which is a function of Impact X Likelihood, after taking into consideration particular controls in place, expressed on a scale of 1-25.

16. Subsidiary Compliance Officer (SCO)

Each subsidiary appoints its own Compliance Officer who reports directly to the Audit Committee of the subsidiary. As part of the CD oversight SCOs maintain a 2nd line of reporting to the CD. As such, CD bears responsibility for effective oversight on an ongoing basis of the Subsidiaries' Compliance Officers (SCOs) of the Group (CISCO, Eurolife, General Insurance and Jinius) who act as independent second line of defence at the Subsidiary (vs the role of the CLs as first line of defence). SCOs have the same responsibilities as CD staff for their area of responsibility.

4. GENERAL PRINCIPLES

The Bank and its subsidiaries implement an integrated and institution-wide compliance culture based on the following principles:

1. **Compliance starts at the Top.**

   The BOD is the owner of the compliance framework and holds the ultimate responsibility for the management of the compliance function. This means that the BOD and the rest of the executive management, lead by example and show visible commitment to compliance principles, thereby setting tolerance and tone at the top and ensuring oversight of compliance.

2. **Compliance is a responsibility that every employee shares.**
   Compliance is a responsibility that each individual employee shares, regardless of his/her position within the Bank and subsidiaries. This implies a strong compliance commitment, implementation of three lines of defence and exercise of good corporate citizenship and responsible corporate behavior. Management & Compliance Liaisons must ensure that staff members are informed of their obligation to adhere to the compliance guidelines. Therefore, the Bank and its subsidiaries ensure through policies, procedures, effective communication, training, and other monitoring measures that Management and staff:
   a. Understand the regulations, standards and best practices associated with the discharge of their operational duties and responsibilities.
   b. Understand associated compliance risks and the need and responsibility for managing these risks.
   c. Understand the importance of internal control functions in managing compliance risks and facilitate their work; and
   d. Identify, assess, and manage with the support of the compliance staff (CLs, SCOs, LCOs & other CD staff) key compliance risks.
3. **The three lines of defence model.**
   The Bank applies the three lines of defence model for the governance of the compliance function principles and ensures that compliance culture is appropriately disseminated at all hierarchical levels. The three lines of defence model is described in the Control Functions Common Operational Framework.
4. **The compliance function independence.**
   The Compliance function, as second line of defence, is independent from operational functions and has adequate authority, stature, and access to the management body.
5. **The compliance function shall have the resources to carry out its responsibilities effectively.**
   The resources to be provided for the compliance function at all levels shall be both adequate and appropriate to ensure that compliance risk within the Bank and its subsidiaries in Cyprus and abroad is managed effectively. Compliance officers shall have sufficient skills, knowledge, and experience as well as professional and personal qualities to enable them to carry out their specific duties and shall have access to regular training.
6. **Investigations and external expertise.**
   The compliance function shall conduct investigations of possible breaches of the compliance policy and be allowed to appoint outside experts to perform this task, if appropriate, seek assistance from Internal Audit on specific compliance review issues and obtain access to all records and files of the Bank within its responsibilities.
7. **Compliance shall be embedded in the operations of the business.**
   Compliance programs must be embedded in the operations of the business, thereby becoming an integral part of their daily operations rather than functioning as a separate oversight process. To achieve this as shown in the diagram below Compliance function must include in its program the following:
   a. Design compliance to be part of business workflows.
   b. Coordinate compliance and related assurance activities.
   c. Assess how well compliance is built into the business.

   Behavior that creates and supports compliance shall be encouraged and behavior that compromises compliance shall not be tolerated.
8. **Access to all information required to perform compliance duties.**

Compliance staff have the right on their own initiative to communicate with any staff member and obtain access to any records or files or any other information necessary to enable them to carry out their responsibilities.

Adequate information shall be exchanged between the business lines and the Compliance function and between the heads of the internal control functions and the Management Body of the institution.

9. Outsourcing

Compliance shall be regarded as a core risk management activity within the Bank. Specific tasks of the compliance function may be outsourced, but they must remain subject to appropriate oversight by the Chief Compliance Officer.

Key Compliance activities & Pillars

Compliance mission is supported by the following 4 Strategic Pillars:

Compliance activities (both at a Bank and at a subsidiary level) must be set out in a compliance program prepared and monitored by the Compliance Division to ensure that all relevant areas of the institution and its subsidiaries are appropriately covered, considering their susceptibility to compliance risk. The compliance activities must include at least the following:

1. Identifying, on an on-going basis, with the cooperation of the Bank's legal services, and other competent units of the Bank (where applicable), the legal and regulatory framework which governs and/or affects the operations of the Bank and its subsidiaries.
2. Ensuring that a complete and updated register of the legal and regulatory framework is maintained and that emanating compliance obligations are documented and supported by appropriate action plans (where applicable). This register is widely known as the Compliance Chart /Authoritative Source Library (as per the new compliance management system).
3. Communicating to business units, branches, and subsidiaries, the legal, regulatory, and business framework applicable to them. The departments, branches, and subsidiaries, in cooperation with CD need to:
   a. Identify the compliance obligations emanating from these requirements and record any gaps and appropriate actions for mitigating the gaps in the system.
   b. Measure and assess the impact of these obligations on the Bank's processes, procedures, and operations as per the risk scoring methodology based on the impact / likelihood assessment criteria.
   c. Assess the appropriateness of the compliance policies and procedures, follow up any deficiencies identified and, where necessary, formulate proposals for amendments.
4. Identifying, assessing, and managing the compliance risks associated with the Bank's business activities, on a pro-active basis.
5. Developing appropriate practices and methodologies to measure compliance risk. This methodology is the Compliance Risk Assessment Methodology known as CRAM that assesses compliance risks based on impact

and likelihood criteria. Such practices may be reviewed regularly to encompass new developments, technological, or other characteristics.

6. Maintaining and updating on an ongoing basis the Risk Maps, through the system, upon the introduction of new or amended laws and regulations, major developments such as significant changes to the organisational structure, strategic objectives, undertaking of new initiatives, implementation of new processes or systems, launching of new products or services and new markets, acquired businesses, outsourcing arrangements, strategic decisions related to the above, occurrence of significant regulatory breaches, breach of Key Risk Indicators (KRIs) thresholds, or the occurrence of any other event that may affect the regulatory risk profile of any Group entity.
7. Preparing and subsequently reviewing and revising accordingly at least on an annual basis all compliance policies on key compliance related issues.
8. Reviewing and assessing organizational and procedural changes to ensure that identified compliance risks are appropriately managed.
9. Ensuring the usage of appropriate tools and mechanisms for monitoring compliance activities which, inter alia, include:
    a. The assessment of periodic reports submitted by CLs and SCOs.
    b. The use of aggregated risk measurements such as risk indicators.
    c. The use of reports warranting management attention, documenting material deviations between actual occurrences and expectations (an exceptions report) or situations requiring resolution (an issues log).
    d. Targeted trade surveillance, observation of procedures, desk reviews and/or interviewing relevant staff,
    e. Conducting periodic onsite/offsite reviews with applicable laws, rules, regulations, and standards and provide recommendations / advise to management on measures to be taken to ensure compliance.
    f. Investigating possible breaches and/or conducting investigations requested by competent authorities of the compliance policy and regulatory framework with the assistance, if deemed necessary, of experts within the institution such as experts from the internal audit, legal services, information security, fraud risk management etc.
    g. Investigating and reporting to competent authorities' incidents of non-compliance with the CBC Directive within one month of identification and mitigating actions to prevent a recurrence of similar incidents within two months of identification of the incident.
10. Ensuring there is an internal alert procedure in place to facilitate employees in reporting confidentially concerns, shortcomings, or potential violations in respect of institution's policies, legal, regulatory, business obligations or ethical issues. The alert procedure shall ensure the protection of the personal data of both the person who reports the breach and the natural person who is allegedly responsible for the breach in accordance with the Data Protection Law. Additionally ensuring that this procedure complies with the Law on the Protection of Persons who report breaches of Union law, N. 6(I)/2022.
11. Overseeing the complaints process and utilizing the relevant information for improvement of processes and procedures.
12. Periodically reassessing and reviewing the scope of compliance assurance reviews to be performed.
13. Ensuring that compliance risks arising from ESG risks are duly considered and effectively integrated in all relevant processes of the Bank i.e., identification and assessment on possible impact to new laws or amendments to existing laws during compliance assessments**.**

14. Cooperating and exchanging information with other internal control and risk management functions on compliance matters (as per the Control Functions Common Operating Framework).
15. Identifying training needs on compliance matters and organizing regular training for management and members of staff for compliance and regulatory matters to increase compliance awareness.
16. Providing guidance /advise to staff either orally or in writing on compliance queries.
17. Issuing written instructions and circulars to the Bank and its subsidiaries in Cyprus and abroad for the prompt adjustment of internal procedures and regulations to changes in regulatory framework.
18. Being involved, in close cooperation with the risk management function in the establishment of the framework and the approval of new products and new procedures to ensure that all material risks are considered and verifying that the Bank complies with the current legal framework and, where appropriate, any known forthcoming changes to legislation, regulation and supervisory requirements.
19. Establishing of a network of CLs throughout the Bank and their appraisal on an annual basis as part of their performance appraisal process.
20. Establishing the LCO network in specific significant risk areas with a direct functional reporting line to Compliance Division to strengthen compliance oversight and challenge.
21. CD acts along with RAD, as the primary point of contact between the competent authorities and the Bank and its subsidiaries. RAD ensures all regulatory correspondence / requests are effectively identified, assessed, and distributed.
22. CD ensures that the Bank's subsidiaries take steps to ensure that their operations are compliant with local laws and regulations. If the provisions of local laws and regulations hamper the application of stricter procedures and compliance systems applied by the Bank, especially if they prevent the disclosure and the exchange of necessary information between the entities within the Bank, the Head of Compliance shall be informed.

Processes and Tools for Managing Regulatory Compliance Risks

Regulatory compliance risks are identified using a combination of methods and sources. Key tools for effective risk identification, assessment, monitoring and management of regulatory compliance risks and the sources used are indicated in the following table:

Identification source	Description	Compliance Management System
Regulatory Change Management	Assessment of live regulatory updates received daily, through the case management module, of the compliance management system (OneSumX).	Compliance risk management system, which enables centralized & integrated maintenance of Regulatory Library, Risk and Control Libraries,
RCSAs	Risk and Control Self-Assessments (RCSA) performed by all Group Units (including subsidiaries), under the guidance of Operational Risk Management Department, with the participation of CD and the Compliance Liaisons network, as per the RCSA methodology.	
Process based compliance risk assessments.	Regulatory risks identified through the assessment for new or amended policies, processes and procedures, project assessments, new product/services assessments, outsourcing arrangements, changes in operating models	

	and structures and any other ad-hoc assessments with regulatory impact.	Regulatory Compliance Risks and Incidents, Issues and Actions, Test Programs.
Compliance Risk Monitoring	Key compliance risk indicators, key performance indicators, regulatory incidents, regulatory criticism, legal cases categorized as regulatory, customer complaints, results from onsite/offsite inspections, results from internal and external audits of compliance with regulations and results from audits/investigations performed by competent authorities. Follow up of mitigating actions.	
Compliance Risk Reporting	Internal and external reporting framework.	

Ethics

The Group is committed to the highest standards of ethics and integrity in all its business dealings. The Compliance function at all levels facilitates the enforcement of these ethical principles and practices as set out in the code of conduct, code of ethics and other related policies. In the spirit as well as the letter of the law, the employees and other stakeholders are expected to apply and uphold the related principles and practices.

5. GOVERNANCE

5.1 Roles and Responsibilities

For the purpose of this policy, the following major roles and responsibilities have been identified:

Board of Directors	Bears the ultimate responsibility for the effective implementation of this Policy and setting the right tone from the top.
Audit Committee	• Approves the Policy • Makes sure that sufficient, dependable, and secure internal procedures are in place to ensure that the Group complies with the policy. • Monitors the effective implementation of the Policy via the Control Functions.
ExCo	• Reviews the Policy prior to submission to the AC. • Ensures that it is effectively embedded throughout the Group's operations.
Chief Executive Officer	Provides approval for the exemptions to the policy
Deputy Chief Executive Officer	Provides approval for the exemptions to the policy
Compliance Division	• Overall responsibility for the drafting and enforcing the policy. • Prepares and updates relevant procedures/circulars as required. • Organizes and conducts relevant training for all staff. • Carries out monitoring reviews to assess the effective implementation of the Policy and recommends corrective action where required.

Risk Management Division	Reviews and assesses the compliance risks addressed in the policy, ensuring that the risks undertaken are within the Bank's risk appetite.
Internal Audit Division	• Periodically assesses the Policy and the Bank's system of internal controls, corporate governance and risk management processes related to the Policy. • Inform AC of its findings and relevant recommendations.
Legal Services	Responsible for: • Providing general advice to the Group on relevant legislation and providing support, guidance and advice to departmental units in relation to legal issues and legal documentation. • Ensuring clauses in contracts avoid abusive language which goes against the Law.
Regulatory Compliance Department	Responsible for: • The implementation of appropriate procedures and controls for the prompt and on-going compliance of the bank and its subsidiary companies in Cyprus and abroad with the existing regulatory framework • Identifying, assessing, and managing on an on-going basis, with the assistance of legal services and other competent departments, all laws, regulations, and self-regulatory standards which govern and/or affect the operations of the bank and maintaining a fully updated register of the existing regulatory framework (Compliance Chart). • Arranging training of relevant staff in cooperation with Human Resources. • Establishing and monitoring the network of CLs. • Assisting senior management in the implementation of the compliance Policy and the effective management of the compliance risks faced by the bank. • Acting along with RAD as the primary point of contact with the Competent Authorities and ensures communication, to the units/ branches/ subsidiaries concerned of the regulatory framework / obligations which affect their areas of operations. • Monitoring the effectiveness of the internal procedures and controls for the implementation of the compliance policy and the management of compliance risk through regular reports. • Carrying out, on a periodic basis, compliance review, including on-site reviews to ensure adherence to compliance policies. • Overseeing the compliance risk assessment process and monitoring the implementation of mitigating actions for the management of identified risks. • Reviewing and analyzing regulatory compliance incidents and ensuring that mitigating actions are implemented to avoid reoccurrence. • Verifying those new products and procedures comply with the current legal environment and business standards and any known changes to

	legislation, regulations, supervisory requirements and business standards. • Monitoring compliance with market abuse Regulatory Framework and the Regulatory Framework pertaining to the provision of investment services and any other regulation under its remit. • Updating this Policy and monitoring its high-level implementation. • Providing guidance, support and advice across the Group for the implementation of this Policy.
Data Protection Officer	Responsible for supervising general compliance with GDPR and for advice on the implementation and interpretation of the Policy throughout the Bank. The DPO is appointed officially by the Bank and his/her credentials are made known to the Commissioner of Personal Data Protection. Please refer to the Personal Data Protection Compliance Policy.
Corporate Governance Officer	Responsible for monitoring the corporate governance compliance in relation to the Board's functioning, its committees, and its members in coordination with the NCGC and making appropriate recommendations to the Board.
Compliance Liaison Manager	Responsible for overseeing the actions of the CL and providing any support required. CLs' managers and line directors are strongly encouraged to: • Involve and consult CLs in all areas of the department that encompass compliance issues. • Support them by (a) allowing access to all required information and (b) allocating sufficient time and tools to enable them to perform their role as CL. • Agree targets and recognize their work and effort in the annual appraisal process. • Approve certain CL actions performed through the compliance system as part of the four eyes principle.
Compliance Liaisons	CLs act as 1st Line of defence with primary responsibility to proactively identify and manage the regulatory risks at local level. Their main responsibilities include the following: • Manage real time regulatory updates assigned to them centrally by the CD, on new or amended regulations and perform an initial assessment/review and gap analysis. • Perform compliance risk assessments and develop action plans for the management of identified risks. • Follow up of mitigation actions and ensure implementation (e.g., actions arising from compliance onsite audits). • Assist their management on compliance issues i.e., identify conflicts of interest, bribery issues, etc. • Perform training on regulatory requirements to the relevant stakeholders within their department.

	• Liaise with action owners and report their progress in the compliance management system. • Design of campaigns for rectification of audit/review findings.
Subsidiary Compliance Officers	SCOs act as 2nd Line of defence with primary responsibility to proactively identify and manage the regulatory risks at their area of responsibility. Their main responsibilities include the following: • Manage real time regulatory updates assigned to them centrally by the CD, on new or amended regulations and perform an initial assessment/review and gap analysis. • Perform compliance risk assessments and develop action plans for the management of identified risks. • Follow up of mitigation actions and ensure implementation (e.g., actions arising from compliance onsite audits). • Assist their management on compliance issues i.e., identify, assess, manage and record conflicts of interest, gifts, bribery issues, etc. • Perform training on regulatory requirements to the relevant stakeholders within their department. • Liaise with action owners and report their progress in the compliance management system. • Design of campaigns for rectification of audit/review findings.
All staff	Responsible for complying with this Policy and its procedures. If any employee becomes aware or suspects that an activity or conduct which has taken place could be unfair or misleading, then the/she has a duty to report it immediately.

5.2 Supporting Documentation

The principles and procedures set out in this Policy are implemented via the various compliance related policies and procedures including the CD procedure manuals, the CRAM, the Control Functions Common Operational Framework and relevant manuals.

5.3 Reporting

Compliance reporting entails:

1. Reporting promptly to senior management and the management body on material compliance failures and weaknesses in Policy and internal control procedures as well as breaches of the regulatory framework identified from compliance monitoring activities, on-site reviews.
2. Reporting in the correct format and ensuring minimum requirements are in accordance with the relevant Directive of CBC and the guidelines of the Compliance Division. The Compliance Division must submit, on a quarterly basis, a compliance report to the Audit Committee copied to the Executive Committee. The minimum requirements covered in the report are as per the guidelines of the CBC Directive.
3. The Compliance Division shall submit for approval an annual report to the Board of Directors within two months from the end of the previous year, via the Audit Committee, which will also be copied to the ExCo. This report is subsequently submitted to the Central Bank of Cyprus.

4. A compliance reporting diary is maintained through the compliance management system to facilitate compliance reporting monitoring and responsibilities.

6. EXCEPTION APPROVAL PROCESS

In cases where there is a request for deviation from this policy, which:

1. is fully justified
2. does not violate the legal/regulatory framework, or constitutes a significant moral lapse, nor does it constitute a significant reputational risk for the Bank and
3. has the approval of the Chief Compliance Officer

then this exception can be allowed with the agreement of the CEO or Deputy CEO of the Bank. The Audit Committee to be notified accordingly.

7. IMPLEMENTATION PROCEDURES (KEY PROCESSES)

Key processes and procedures for the implementation of the Group Compliance Policy are descripted in the separate CD internal manuals and communicated to BOC staff whenever needed.

Appendix 1

Scope of Compliance

Client related Integrity Risk	1. Money laundering 2. Terrorist financing 3. Other external crime and fraud 4. Customer due diligence 5. Sanctions & embargoes
Personal Conduct related Integrity Risk	1. Market abuse 2. Business principles and code of conduct 3. Anti-Bribery 4. Inducements (incl. gifts) 5. Whistleblowing 6. MIFID 7. Personal transactions 8. Conflicts of interest
Financial Services Conduct Related Integrity Risk	1. Marketing, sales, and trading conduct 2. Conduct of advisory business 3. Transparency of product offerings 4. Customer interest and protection 5. Complaint handling processes 6. Data protection/privacy 7. Investment services & activities 8. Unfair practices 9. Consumer Protection
Organizational Conduct related Integrity Risk	1. Corporate Governance 2. Conflicts of interest 3. Internal standards with respect to new product approval and product review process 4. Accounting and auditing requirements 5. Tax laws relevant to the structuring of banking products or customer advice 6. Treating customers fairly 7. Sector/industry (acceptance) standards 8. Oversight of intermediaries 9. Mergers and acquisitions 10. DAC6/FATCA/CRS 11. Regulatory registration requirements 12. Anti-Trust (competition) 13. Social and green responsibility 14. Employment Law Framework 15. Trade Import/Export Law

	16. Technical, Historical & Innovation Regulatory Framework 17. Health & Safety Regulatory Framework 18. Information technology and Cyber Risk 19. Market abuse and organizational insider trading (incl. Chinese walls) 20. Reputational Risk 21. ESG Risk
Organization, systems, procedures	1. Organization of compliance 2. IT systems and infrastructure to support compliance. 3. Compliance internal procedures/manuals/ methodologies 4. Regulatory Reporting