GROUP POLICY - COMPLIANCE POLICY

POLICY IDENTIFICATION

Title	**Group Compliance Policy**
Policy Number	**CD402**
Revision Number	13
Classification	Public Use
Applicability	Group
Owner	Compliance Division
Reviewer(s)	Internal Audit Division, Risk Management Division
Approved by	Board of Directors
Issuing Date	02/05/2011
Effective Date	02/05/2011
Related Policies	Refer to Appendix 4

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	Minor revisions
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.
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.
13.0	27/06/2024	Compliance Division	Board of Directors (through the Audit Committee)	Major redrafting required for the certification under ISO 37301 – Compliance Management Systems

TABLE OF CONTENTS

1. PURPOSE AND SCOPE

The purpose of this Policy is to set out the compliance framework that applies in the Bank of Cyprus Public Company Limited and its subsidiaries (hereinafter referred to as BoC) and it must be read in parallel with the Compliance Charter and the Control Functions Common Operational Framework; it is available to all staff through corporate portal and for customers on the corporate website.

The Policy sets out the business and legal environment applicable to BoC, the principles and responsibilities for compliance and how these responsibilities are allocated and carried out at group and entity level.

2. ABBREVIATIONS

Within this document, the following abbreviations are used:

Abbreviation	Definition
AC	Audit Committee
BoC	Bank of Cyprus Public Company Limited and its subsidiaries
BOD	Board of Directors
CBC	Central Bank of Cyprus
CD	Compliance Division
CEO	Chief Executive Officer
CL	Compliance Liaison
CGD	Corporate Governance Department
DPD	Data Protection Department
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
RCD	Regulatory Compliance Department
SCO	Subsidiary Compliance Officer

3. DEFINITION OF TERMS

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

1. **Annual Action Plan**
   The Action Plan 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 Action Plan adopts a risk-based methodology.
2. **Bank of Cyprus Public Company Ltd (BoC)**
   Means the Bank of Cyprus Public Company Ltd, its ultimate holding company and its subsidiaries.
3. **Business Risk and Control Officers**

Dedicated officers assigned the task of promoting and sustaining a corporate culture of risk and compliance within their division as per the guidance received by the Control Functions.

4. **Compliance Charter**

   The Compliance Charter is a register of the regulatory framework (laws, regulations, and self-regulatory standards) that affects BoC, and it is maintained by the Compliance Division (part of the Compliance Management System).

5. **Compliance Management System (CMS)**

   The Compliance Management System defines how BoC manages its compliance procedures. It incorporates specific elements and the involvement and cooperation of the Governing Body, Top Management, Control Functions and relevant employees BoC to allow:

   a. Adherence to Laws and Regulations: Ensure strict compliance with legal requirements, regulations, voluntary obligations and ethical standards within the operational context to mitigate risks associated with compliance.
   b. Fostering a Culture of Integrity: Promote ethical business practices, encourage employees and stakeholders to act with integrity, thereby reducing the risk of non-compliance.
   c. Enhancing Operational Governance and Reputation: Support corporate governance and responsibility thus enhancing the BoC's reputation and trust among stakeholders.
   d. Modernization of corporate compliance efforts: aligning with industry practices
   e. Create a more resilient organization and improve business opportunities.
   f. Consider interested parties' expectations.
   g. Demonstrates the BoC's commitment to managing compliance risks effectively and efficiently.

6. **Compliance Function**

   The Compliance Function's role is to ensure that the organization is complying with all applicable laws, rules and regulations, as well as internal codes of conduct, policies and procedures. The Compliance Function establishes, implements, and maintains appropriate tools, mechanisms, and processes to:

   a. Ensure:
      i. Effective control over the implementation of the Policy.
      ii. Efficiency on all related processes.
   b. Enable the organization to identify the relevant applicable laws, rules, regulations, codes of conduct and standards of good practice, assess and analyze the risks of non-compliance, and prioritize the compliance risks for mitigation and monitoring.
   c. Manage, and monitor compliance risks.
   d. Promote compliance awareness and the right compliance culture across the BoC.
   e. Monitor key regulatory risks through monthly / quarterly Key Risk Indicators
   f. Conduct periodic onsite/offsite compliance reviews against applicable laws, rules, regulations, and standards and provide recommendations / advice to management on measures to be taken to ensure compliance.
   g. Provide regular compliance reporting to Senior Management, the Board, authorities, regulatory bodies (the interested parties and their specific needs and expectations can be found in Appendix 2).
   h. 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 the compliance function (refer to Appendix 1 for a more detailed analysis):

   a. Client related integrity risk.
   b. Personal conduct related integrity risk.

c. Financial services conduct related integrity risk.
d. Organizational conduct related to integrity risk.
e. Organization, systems, procedures.

7. Compliance Liaisons

The Compliance Liaisons (CL) are officers assigned with the responsibility of supporting their management in the implementation of regulatory changes, compliance issues and controls and the overall adherence to BoC compliance principles. The CL neither assume nor undertake compliance function's activities / responsibilities and such mandate is clearly communicated. There is no delegation of the primary responsibilities of CD to the CLs. CL are part of the first line of defense and as part of this, they are the facilitators to the second line of defense.

8. Compliance Liaison's Manager

The CL's Line Manager (where applicable) is responsible for overseeing the actions of the CL and providing any support required. They are strongly encouraged to:

a. Involve and consult CLs in all areas of the department that encompass compliance risks.
b. Support them by allowing access to all required information and allocating sufficient time and tools to enable them to perform their role.
c. Agree targets and recognize the CL's work and effort during the annual appraisal process.

9. 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.

10. Impact

The extent to which the compliance risk, if realized, would affect the ability of the entity or the BoC 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.

11. Inherent Risk

The result of the Impact X Likelihood, without taking into consideration particular controls in place. Essentially, the inherent risk is the worst-case scenario of the risk assessed.

12. Residual Risk

The function of Impact X Likelihood, after taking into consideration particular controls in place. Essentially, the residual risk is the best-case scenario of the risk assessed.

13. Likelihood

The likelihood of occurrence refers to the possibility that a given event 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.

14. Local Compliance Officers (LCOs)

Dedicated officers with direct functional reporting to the Compliance Division (to strengthen compliance oversight). They are assigned to high- risk areas and have the same responsibilities as the Compliance Division staff members; they do not handle issues related to data privacy.

15. RCSA

The Risk Control Self-Assessment Methodology (RCSA), provides a unified way to identify, assess, mitigate, and manage risks. The inherent risk level and the residual risk level of each identified risk, i.e. both before and after considering the controls that are in place for mitigating the risk should be assessed. The risk level is determined by assessing the likelihood (possibility that a given risk will occur within a specific timeframe) and Impact. The ORM Risk Assessment Scoring Methodology includes detailed guidelines (OE.099).

16. Regulatory Compliance Matrix

The Compliance Division maintains a consolidated Regulatory Compliance Matrix that comprises of the entire regulatory framework namely the laws and regulations from competent authorities that affect BoC per owner and responsible division along with mitigating actions for the management of risks of non-compliance. The Regulatory Compliance Matrix reflects the status of compliance of each law which is monitored and updated on an ongoing basis by the Responsible Division's CL - SCO and Regulatory Compliance Department through the gap analysis of new or amended rules and regulations.

17. 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 legal obligation and embrace broader standards of integrity and ethical conduct.

18. Subsidiary Compliance Officer (SCO)

Each subsidiary appoints its own Compliance Officer who reports directly to the Subsidiary's Audit Committee. As part of the Compliance Division's oversight, SCOs maintain a 2nd line of reporting to the Division. As such, the Compliance Division bears responsibility for effective oversight on an ongoing basis of the SCOs who act as independent second line of defense at the subsidiary. SCOs have the same responsibilities as the Compliance Division's staff for their area of responsibility.

4. GENERAL PRINCIPLES

BoC implements an integrated and institutional-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 its management. AS part of this role, the BOD and the rest of the executive management, must 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 the responsibility of each individual employee, regardless of his/her position within BoC. This implies a strong compliance commitment, adherence to the three lines of defense and exercising good corporate citizenship and responsible corporate behavior. Management and Compliance Liaisons must ensure that staff members are informed of their obligation to adhere to the compliance guidelines. Therefore, BoC ensures 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 Control Functions Common Operational Framework**
   BoC applies the three lines of defense 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 defense model is described in the Control Functions Common Operational Framework.
4. **The compliance function independence**
   The Compliance Function, as second line of defense, is independent from operational functions and has adequate authority, stature, and access to the management body, as well as reports independently to the Audit Committee.
5. **The Compliance Function shall have the resources to carry out its responsibilities effectively**
   The resources available to the Compliance Function at all levels shall be both adequate and appropriate to ensure that compliance risk within BoC 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 this Policy and be allowed to appoint outside experts to perform this task, if appropriate, seek assistance from Internal Audit on specific compliance reviews' issues and obtain access to all records and files of BoC within these responsibilities.
7. **Compliance shall be embedded in the operations of the business**
   Compliance 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 the Compliance Function must include in its Annual Action Plan 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 must be encouraged and behavior that compromises compliance must not be tolerated.
8. **Access to all information required to perform compliance duties**
   The Compliance Division 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 activity within BoC. Specific tasks of the compliance function may be outsourced following proper procedures, but they must remain subject to appropriate oversight by the Chief Compliance Officer.

5. COMPLIANCE ACTIVITIES AND PILLARS

As a highly regulated entity, BoC must comply with a multitude of regulatory requirements. Compliance obligations under scope include the following:

1. Regulatory compliance relevant to Laws/Directive in CY & EU.
2. Voluntary Codes of Governance such as the UK Corporate Governance Code 2018.

3. Corporate Governance Compliance matters.
4. Relevant legislation and regulation with regards Data Protection.
5. Legislation/regulation on Anti-Money Laundering and Combating Terrorism Financing including relevant legal and regulatory requirements/principles stemming from the provisions set out in the Law for the Implementation of the Provisions of the United Nations Security Council Resolutions (Sanctions) and the Decisions and Regulations of the Council of the European Union Law 58(I) of 2016, and the CBC Directive for Compliance with the Provisions of the United Nations Security Council Resolutions and the Decisions/Regulations of the Council of the European Union.

The Compliance Division's mission is supported by the following 4 Strategic Pillars:

1. Enhanced Compliance Policy & Operating Model
2. Digitization & Automation
3. Enhanced Support to Business and Strengthened Monitoring & Assurance Activities
4. Awareness & Cultural Empowerment

Compliance activities must be set out in an Annual Action Plan prepared and monitored by the Compliance Division to ensure that all relevant areas of the organization are appropriately covered, considering their susceptibility to compliance risk.

The compliance objectives must include at least the following:

1. Identifying, on an on-going basis, with the cooperation of the BoC' Legal Services, and other units of BoC (where applicable), the legal and regulatory framework which governs and/or affects the operations of BoC.
2. Ensuring that a complete and updated register of the legal and regulatory framework is maintained and that stemming compliance obligations are documented and supported by appropriate action plans (where applicable).
3. Communicating to business units, branches, and subsidiaries, the legal, regulatory, and business framework applicable to them. In cooperation with the Compliance Division, they need to:
   a. Identify the compliance obligations stemming 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 BoC'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 BoC's business activities, on a pro-active basis.
5. Developing appropriate practices and methodologies to measure compliance risk. Towards this the Compliance Division fully implements the Operational Risk Management Departments' Risk Assessment Scoring Methodology which has been enhanced to provide detailed scoring criteria and indices with regards to the Regulatory Impact. This methodology assesses compliance risks based on impact and likelihood criteria.
6. The compliance risks are recorded 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. The relevant documentation is 90.2 Risk and Control Self-Assessment (RCSA) Methodology and RCMS Manual and the ORM Risk Assessment Scoring Methodology.

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:
   d. The assessment of periodic reports submitted by CLs and SCOs.
   e. The use of aggregated risk measurements such as risk indicators.
   f. 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).
   g. 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.
   h. 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.
   i. 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 must 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. It is noted that the safeguarding of employees from any form of retaliation is analysed in the Group Whistleblowing policy.
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 BoC 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 of the BoC personnel on compliance matters and organizing regular training for management and members of staff for compliance and regulatory matters to increase compliance awareness. A Training Plan must be prepared on an annual basis by the Compliance Division and must be submitted to the Training Department for approval and implementation.

16. Providing guidance /advise to staff either orally or in writing on compliance queries.
17. Issuing written instructions and circulars to BoC 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 BoC 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 and evaluating them on an annual basis as part of their performance appraisal process (the Data Privacy Department is excluded from the appraisal process).
20. Establishing the LCO network in specific significant risk areas with a direct functional reporting line to the Compliance Division to strengthen compliance oversight and challenge.
21. The Compliance Division acts along with the Regulatory Affairs Department, as the primary point of contact between the competent authorities and BoC. The Regulatory Affairs Department ensures all regulatory correspondence / requests are effectively identified, assessed, and distributed.
22. The Compliance Division ensures that the 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, especially if they prevent the disclosure and the exchange of necessary information between the entities, the Chief Compliance Officer must be informed.

The identification of the compliance risks is made through different sources. Refer below for more information:

Identification source	**Description**	**Registration in:**
Regulatory changes	Monitoring all new and amended regulatory developments and ensuring that a gap analysis is performed upon the introduction of new or amended regulations and that an action plan is created to ensure adherence with the new regulations.	Compliance risk management system, (OneSumX) which enables centralized & integrated maintenance of the Regulatory Library, Issues and Actions and Test Programs.
RCSAs	Risk and Control Self-Assessments (RCSA) performed by all BoC Units, in line with Operational Risk Management Department, with the participation of Control functions including Compliance Division and the Compliance Liaisons network, as per the RCSA methodology.	RCMS which enables the recording of risks, actions, incidents and KRIs with taxonomies for each operational risk category of the non-financial risk taxonomies.
Compliance risk assessments	Regulatory, data privacy and financial crime risks identified through the assessment for new or amended policies, processes and procedures, project assessments, new product/services assessments, outsourcing arrangements, changes in	OneSumX (for identified gaps) / RCMS (for identified risks)

Identification source	Description	Registration in:
	operating models and structures and any other ad-hoc assessments with regulatory, data privacy or financial crime impact.	
Financial Crime and Sanction Monitoring Compliance daily operations	Identified through the daily operations relating to the clients' risk assessments, transactions and alerts monitoring and sanction screening, and through regularly monitoring transactions for unusual or suspicious activity.	RCMS
DPIAs	Identified within the DPIA process carried out at the design stage of any new process, product, system whereby processing of personal data takes place. This tool assists in effectively identifying and minimizing privacy risks.	RCMS
DPD Daily operations	Identified through the day- to- day operations, including breaches under the GDPR, complaints and exercise of data subject requests.	--
Compliance Reviews	As per the Compliance Review Methodology, the Compliance Division performs the following types of reviews to ensure compliance with key Compliance policies and procedures and ensure the effectiveness of controls with regards to key regulatory risks: • Thematic Reviews which address specific subjects/ procedures or circulars. • Sectoral Reviews which focus on a specific Entity and address several themes • Gap Analysis Reviews of new or amended regulations, which depend on the regulatory risk impact for BoC. • Quarterly Bank-Wide Review which addresses important KRIs (applicable for FCSCD only). Sectoral Reviews which focus on a specific Entity and address several themes. • Other types of Reviews following ad-hoc requests by regulators or standard assurance requirements by regulations, which are only applicable for RCD.	Compliance risk management system, (OneSumX) for the recording of findings and recommendations and the monitoring of actions as per agreed deadlines RCMS (reflecting risks identified through the Compliance Reviews)
Internal and external Reviews	Identified through the review and assessment of internal / external audit reports, reports issued by competent authorities and triennial reviews including SREP and onsite inspections.	RCMS

Processes and Tools for Monitoring and Managing Compliance Risks

A combination of methods and sources is utilized to monitor compliance risks. The table below highlights the key tools for effectively monitoring and managing these risks, as well as the sources that are utilized

Monitoring source	Description	Registered in:
KRIs	The Compliance Division monitors all regulatory risks through Key Risk indicators (KRIs) which are monitored monthly. KRIs have been associated with risks in RCMS and through the KRI monitoring, they have been configured to be reported and maintained as per the defined thresholds as established by management. To this end, depending on the frequency of reporting, KRI owners are forced to report the KRIs assigned to them. In cases where KRI thresholds exceed the acceptable thresholds, the KRI owner, in collaboration with the risk owner, must define an implementation plan of action to reduce the KRI to an acceptable risk appetite level. KRIs are reported in the Monthly reports and in the Quarterly to top Management, the Executive Committees and the Audit and Risk Committees.	RCMS
Regulatory Incidents including Legal cases and customer complaints	Operational risks, incidents, legal cases and customer complaints (if leading to potential or actual losses) are recorded in the Operational Loss Database system (RCMS) as per the ORM Incidents Methodology. Following the recording of incidents an assessment takes place to identify the potential control deficiencies that led to the event and the areas of increased operational risk, i.e. perform root-cause analysis, as well as aggregation analysis to recognize patterns of loss events and implement mitigating actions to avoid reoccurrence. Depending on the type and the criticality of the incident the Incident Response and Escalation Process is followed. Incidents are categorized as per the ORM risk taxonomy by cause type, Basel event type and effect type. Corrective actions must be appropriate to the impact of the incident occurring. Incidents of breach / nonconformity / noncompliance with relevant regulations are categorized as "Regulatory (e.g. potential or actual regulatory penalties, incidents of non-compliance with	RCMS

Monitoring source	Description	Registered in:
	regulatory obligations, incident which indicate possible fault with regards to a specific law and regulation, compliance breaches etc.). They are communicated to the Compliance Division through the RCMS system, for review and assessment, as to the root cause analysis and the mitigating actions to avoid reoccurrence based on the categorization of the risk (risk taxonomy). The Compliance Division monitors such remedial actions and considers these in the compliance risk self-assessment process and / or as part of its reporting processes. The owner of the plan or the team/committee responsible for managing the incident (depending on the nature of the incident and the corresponding plan being activated) must continuously assess the potential impact of the incident and the seriousness of the incident. Additionally, the process includes implementing any actions needed, reviewing the effectiveness of any corrective action taken, and proceeding to make changes to the applicable process, should that be necessary. Furthermore, as per the Incident Response and Escalation Process the Corresponding incident management team / committee is invoked. Escalation and reporting of incident occurs when the Owner of the incident or the incident response plan / contingency plan informs the relevant Divisional Director or any other impacted or affected Divisional Director. The Head Business Continuity Risk Management (HBCRM) is informed by the plan Owner. Manager Operational Risk Mgt & Outsourcing Officer is informed by the HBCRM. As per the process, the incident is then reviewed, the causes determined as well as if any similar incidents exist, or can potentially occur. Incidents of non-compliance with the CBC Directive are reported to competent authorities within one month of identification and mitigating actions to prevent a recurrence of similar incidents within two months of identification of the incident. The abovementioned process is duly documented in the ORM Incidents Methodology and the Incident	

Monitoring source	Description	Registered in:
	Response and Escalation Process which are available in the BoC's portal.	
Root cause Analysis	The procedure of the Root Cause Analysis is a process which must be followed by the employees to determine / identify the causes of a specific incident / problem and the corrective actions to avoid its recurrence. The objective is to rectify the issue so that it does not happen again. It is performed once significant issues, repetitive errors, actions that failed to resolve the issue, or similar issues across different units / projects / activities, occur. However, we perform a root cause analysis for all incidents to understand the control failures as defined above. The formal root cause as described in OE 001 is referred to in the Incident Management procedure. For significant incidents, the Root Cause Analysis process should be followed as described in the OE. 001, section 3. Significant incidents for Root Cause Analysis purposes are considered to be: • Incidents arising from problems in IT Systems which are characterized as "major", based on the "IT Incident Management Process" methodology. • Incidents with actual damages ≥ €50K. • Incidents involving new legal actions not connected to existing actions against the bank with actual damages ≥ €50K. • Incidents involving regulatory fines / penalties and/or incidents involving investigation by supervisory authorities. The evaluation of its effectiveness is distributed to the Director of the area in which the incident occurred, in case reoccurrence of the problem / incident.	RCMS

Monitoring source	Description	Registered in:
Follow up actions	Pending Risk Mitigation Actions are monitored through the OneSumX and RCMS systems on a continuous basis. The Compliance Division oversights and approves any changes in the follow up and closure of actions. It is highlighted that when an action is set and a deadline is agreed, the CLs update the system with any progress done within the agreed deadline. When actions are completed for a specific risk, the risk level is reassessed in terms of Impact and Likelihood. Any remaining pending actions are updated, or new actions are recorded.	RCMS OneSumX

Internal and External Reporting

The Internal and external reporting framework ensures that all compliance obligations are implemented. The factors that determine the scope of the reporting framework are determined through KRIs/KPIs measurements which are analyzed on a monthly / quarterly basis and reported monthly to the ExCo and on a quarterly basis to the Audit and Risk Committees. These measurements are generated through the performing data analysis on information generated from various systems. The results from monitoring and measurement are evaluated and determine the actions for the next quarter as well as the new reviews to be planned in next year's action plan. More analytically, 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. The OneSumX ensures the maintenance of internal and external reporting for compliance purposes. Appendix 3 provides a summary of the internal and external reporting.
5. Each year the Corporate Governance Compliance, which is part of the Regulatory Compliance Department, performs an Internal Board Performance Evaluation, which includes the following:
    a. The performance of the Board collectively and individually.
    b. The contribution of the Board collectively and of its committees and individual members:
    c. The development of business objectives, risk appetite, and strategies.
    d. Setting and overseeing the risk and compliance management frameworks.
    e. Establishing and maintaining consistent organisational and operational arrangements and internal control mechanisms.
    f. The composition of the management body and its committees.
    g. Communication with management, shareholders, and competent authority.

h. The roles of the chairperson of the board, the company secretary and senior independent member of the Board.
i. The time commitment of non-executive members and their capacity to critically review information.
j. Evaluation of the collective and individual suitability of the Board and its members.

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.

6. GOVERNANCE

6.1. 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. • Approves the Policy.
Audit Committee	• 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. • Recommends the Policy for approval (to the Board of Directors).
ExCo	• Reviews the Policy prior to submission to the AC (for recommendation) and to the Board (for approval). • Ensures that it is effectively embedded throughout the Group's operations.
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 BoC's risk appetite.
Internal Audit Division	• Periodically assesses the Policy and the system of internal controls, corporate governance and risk management processes related to the Policy. • Informs 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.

Financial Crime & Sanction Compliance Department	Develops and oversees the implementation of the Group's compliance strategy in financial crime matters (Anti-Money Laundering and Terrorist Financing) and Financial Sanctions) to ensure that the Group complies with the legislation, the directives of the Central Bank of Cyprus (CBC), European Union (EU), international practices and international sanctions.
Regulatory Compliance Department	Contributes to the formulation/design of the compliance strategy for governance, markets and regulatory compliance of the Group and oversees its implementation to ensure that the Group complies with local, European, and international regulations and practices that govern the Group.
Data Protection Officer	• Contributes to the formation/design of the compliance strategy in matters of personal data protection and oversees the implementation of the Bank's and the Group's Personal Data Protection strategy to ensure compliance with local, European, and international regulations and practices. • Acts as a Personal Data Protection Officer as defined by the regulatory framework according to which he acts as a point of contact with the Office of the Personal Data Protection Commissioner as well as ensures the effective management of related risks.
Corporate Governance Officer	Contributes to the implementation of the compliance strategy for corporate governance matters to ensure the Group's compliance with local, European and international regulations, international best practices, as well as the main principles of the Irish corporate law regulatory and legislative framework.
Compliance Liaison Manager	Coordinates with various departments within the BoC to align operations with compliance requirements and implement effective compliance measures.
Compliance Liaisons	• The primary point of contact between 1st line Division / Department and the Compliance Division. • Proactively supports the local management in carrying out their responsibilities for compliance with regulatory changes, addressing compliance issues and implementing controls in adherence to compliance principles. • Identifies, measures, monitors and reports risks and ensures compliance with internal and external requirements within his/her department.
Subsidiary Compliance Officers	• Ensures the subsidiary's adherence to all relevant banking laws, regulations, and compliance standards. • Conducts risk assessments, implement compliance measures, and develop strategies to mitigate risks associated with the subsidiary's operations.
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.

6.2 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.

7. 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 of any comments and confirmation of the deviation.

8. IMPLEMENTATION PROCEDURES (KEY PROCESSES)

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

9. Appendix 1 - Scope of Compliance

Level 1	Level 2	Level 3
Regulatory Compliance / Conduct Risk	Improper Business or Market Practices	Failure to comply with new legislation / amendment on existing laws
		Misinterpretation of Regulation
		Breach of regulatory reporting or notification requirements
		Failure to maintaining staff accreditation, permission, and regulatory approvals
		Ineffective relationship with regulators
		Improper licensing/certification/registration
		Unlicensed activity
		Improper trading: Failure to deal, manage and execute trades appropriately
		Activity in un-authorised product or counterparty
		Mis-selling: Offering of inappropriate or complex products to customers
		Failure to handle/remediate complaints
		Failure to market and promote products or services appropriately or to provide adequate pre-sale disclosures
		Unfair treatment of customers during account closure or product withdrawal or maturity
		Post-sales service failure
		Client mistreatment/ failure to fulfil duties to customers

Level 1	Level 2	Level 3
		Client account mismanagement
		Breach of code of conduct and employee misbehavior
		Use of inside information
		Market manipulation/abuse
	Suitability, Disclosure and Fiduciary	Aggressive sales
		Fiduciary breaches
	Product Flaws	Failure to design, approve and maintain appropriate products or services
		Failure to identify operational risks during the design of a new product
		Mispricing of a product
	Bribery and corruption	Offerings to employees by another person or organisation, e.g. payment, gifts, hospitality
		Benefits obtained for an employee's personal gain, rather than for their organisation
		Failure to manage conflicts of interest
		Performance of activities that's beyond the position or remit of an employee
Financial Crime Risk	Money Laundering and Terrorism Financing Risks	Non-compliance with Guidelines including non-performing World Check, obtaining approval for high-risk customers
		Failure to collect and/or update necessary documents e.g. passports, utility bills, company certificates or company minutes for new relationships and existing customers
		Failure to identify UBO or PEP, PEP family members and associates
		Failure to create complete Economic profile including Business Activities, Source of Wealth, Source of Income, Counterparties on onboarding and during the review process
		Conducting a business relationship on a non-face-to-face basis
		Customer or transaction relationships with countries that do not follow the same AML framework as the Bank and are listed as high risk for AML/TF or Tax Crimes

Level 1	Level 2	Level 3
		Using distributors that follow substandard AML/ TF procedures
		Using distribution channels and networks that are vulnerable to ML or TF activities
		Offering complex products or services which involve multiple parties or multiple jurisdictions
		Offering products that have low transparency/ encourage anonymity
		Offering cash intensive products/ services
		Offering products services that facilitate or encourage high value or unlimited value transactions
		Failure to monitor suspicious transactions e.g. identify transactions not in line with business activities, obtain supporting documents, identify and/ or report suspicious transactions
	Sanctions Violations	Lack of details in transactions, trade finance activities or other payments (e.g. intermediary points)
		Difference in sanctions compliance obligations
		Effecting transactions in USD/CAD with a customer dealing with gambling, gambling related services, Money service business, payment service providers and electronic money institutions
Data Privacy Risk	Data Privacy	Breach of GDPR
Corporate Governance Risks	Internal governance Directive	Suitability of members of the management body and key function holders
		Non-compliance with committee composition requirements
		Non-compliance with committees' terms of reference
		Non-compliance with Board functioning requirements
		Non-compliance with allocation of responsibilities
ESG Risks	Environmental Risk	Climate change risk
		Sustainable finance commitment
	Social Risk	Low level of customer satisfaction
		Human advocacy
	Governance Risk	Gender diversity Risk

Level 1	Level 2	Level 3
	Force Majeure Risk	Risk of force majeure, war, strike, riot, crime, epidemic or an event described by the legal term act of God which prevents one or both parties from fulfilling their obligations under the contract

10. Appendix 2 - Interested parties- needs and expectations

External interested parties

Type	Example of bodies	Possible needs and expectations	Control actions
Regulatory bodies and responsible governmental agencies/authorities	• CBC • ECB • EBA • JST • Cyprus Stock Exchange • Central Bank of Cyprus – Resolution Authority • Cyprus House of Parliament • Government Bodies (e.g. Ministry of Finance, Ministry of Energy, Commerce, Industry & Tourism) • Advisory Committee on Economic Sanctions (Committee – SEOK, Ministry of Finance) • Registrar of Companies and Official Receiver • London Stock Exchange • CySEC • Irish Central Bank • Irish Company Registrar • MOKAS • Financial Ombudsman • Commission for the • Protection of Competition • Commissioner for Consumer Protection	Regulatory bodies expect organizations to comply with laws, regulations, and industry standards. They need accurate, prompt reporting and cooperation.	Appointment of the Regulatory Affairs department that acts as the official and primary contact with regulators. Keeps all communication registered. Ensures requirements that arise from regulatory inspections are promptly implemented. Incoming correspondence is distributed to business owners, while monitoring the Bank's promptness and quality of response requirements and adherence to regulatory rules. Maintenance of a registry with all the legislative text the Bank has to comply with. The Bank is rigorously adhering to its reporting obligations
	• Commissioner for Personal Data Protection • European Banking Federation • EIOPA • Association of Cyprus Banks • Environmental Commissioner • Digital Security Authority • Single Resolution Group	Comply with the data protection rules	Appoint a Data Protection Officer to apply the terms of reference including but not limited to monitoring of compliance to GDPR, Co-operating with the Supervisory Authority, consulting on DPIAs, risk-based approach on identifying risks

Type	Example of bodies	Possible needs and expectations	Control actions
	• European Data Protection board • European Commission		

External Interested Parties

Type	Example of bodies	Possible needs and expectations
Customers	• Customers expect product/services that meet quality, safety and regulatory and market standards. • Must establish transparency, reliability, fairness and clarity of terms and services to be provided. • Third-party intermediates need clear communication about the organization's compliance requirements, policies, and expectations. Clearly defined roles and responsibilities and well-defined compliance clauses in contracts or agreements. • Must be well trained / experienced on technical maters and on highly regulated areas (depending on their role of appointment). • Expect to have clear reporting lines for compliance incidents or concerns. They expect fair treatment, adherence to contractual obligations, and ethical practices. • Must apply rules and standards equivalent to those of the Bank.	Customer complains arrangements. Customer feedback (surveys, customer satisfaction, mystery shopping). Relationship management (Pre and post contractual information, communication). Code of Ethics/Conduct. Suitability of products and services offered to clients. Technological advanced services to facilitate compliance and market trends. Compliance Policies is publicly available
Vendors Suppliers Contractors Service-providers		The bank remains ultimate responsible for the outsourced functions / services. Outsourcing policy in place follow guidelines of EBA as the Bank is a regulated entity. Dedicated department/team to access third party agreements and ensure risks are considered and managed.

Type	Example of bodies	Possible needs and expectations
		Continuous monitoring and assessment of the third parties with whom the Bank maintains a relationship.
Owners, shareholders and investors	Investors seek transparency, ethical behaviour, and risk management. They need compliance to protect investments.	Annual reports issued by the Bank addressed to shareholders to give a snapshot of what is going on in the Bank.
Society and community groups	The community expects responsible corporate behaviour, environmental protection, and social responsibility.	Code of ethics and standards of the Bank Sustainability report
Business associates Credit Rating	Associations expect adherence to industry codes and standards	Policies in place that need to be followed Annual KYC Reviews, are carried out by Correspodent Banks. In addition is a Dedicated Unit within the Bank, being responsible for the handling of the Corresponding relationship, whilst the compliance division handling the annual KYC reviews. Dedicated person on Compliance Division, being responsible for handling day to day requests from correspondent Banks
Auditors / Certification Bodies	• These parties assess compliance systems and expect robust processes • Require compliance with the different ISO requirements	Annual surveillance audits to ensure continuous compliance with the certification and ongoing improvement. Certified with: ISO27001

Internal interested parties

Type	Example of bodies	Possible needs and expectations
The governing body/(ies): • Board of Directors • Audit Committee • Risk Committee • Nominations and Corporate Governance Committee	• They expect alignment between compliance efforts and the organization's strategic goals. • Expect monitoring of compliance risks and ensuring risk mitigation measures are in place. • Expect regular reporting on compliance performance and issues, either identified by the • Regulatory Bodies or internally reported / identified incidents. • Expect compliance with laws, regulations, and industry standards.	• Set clear reporting lines and governance arrangements. • Appointment of Committees to monitor specialized matter and dedicated to significant components of the Bank's Compliance Management System. • Documented decision making / action plans to mitigated areas of improvement. • Appointment of the Company Secretary responsible for the coordination of meetings / agendas / drafting minutes / monitoring action plans. Minutes drafted to

Type	Example of bodies	Possible needs and expectations
• HR and Renumeration Committee • Steering Committees	• Need to build and maintain trust with stakeholders. • Need to encourage a culture of compliance and learning.	include sufficient information on the discussions made and decisions taken. • Action plans / decisions taken monitored via separate registry (Pending list) which is monitored / followed-up regularly. • Regular reports / information packages that need to be • submitted to governing bodies.
• Employees	• Employees expect a safe and ethical work environment. They need clear policies, training, and communication regarding compliance.	• Employees are notified regularly for any amendments in existing policies and circular, as well as for announcements • Detailed organizational circulars are updated and published on Employees' Portal which also indicates the referred officer for obtaining clarifications. • Specialized annual training related to compliance matters is mandatory for the Bank's employees (either to all employees or to specific groups) which upon completion is followed by the relevant assessment. • Communication channels are in place for direct communication between Bank's employees and Compliance Division
Internal control functions: • Internal Audit Division • Compliance Division • Risk Management Division • Information Security	• Oversee and give levels of assurance to the Bank's Compliance Management System. • To ensure adequate controls are in place for the effective implementation of a Compliance Management system. • Need to identify, assess and manage compliance risks. • Provide recommendations on corrective actions.	• Monthly, quarterly and annual reports prepared by each function. • Internal investigations conducted by each function. • Departmental KRIs in place related to risks identified. • The Bank implements RCMS which is an Operational Risk/Loss Database system, where risks identified from various sources, as well as, incidents/losses and KRIs are centrally maintained. The

Type	Example of bodies	Possible needs and expectations
	• Need to understand compliance requirements and be aware of compliance risks.	system aims at an efficient/effective identification, measurements, management and monitoring of core risks. • KPIs, OKRs considered during their appraisals. • Independence to their operation.

11. Appendix 3 - Reporting

Frequency of reporting	Report Title	CD responsible department	Submitted to	Competent Authority
Quarterly	Compliance Division Quarterly Report	RCD/FCSCD/DPD/CGD	ExCo / AC	n/a
Monthly	Compliance Key Risk Indicators	RCD/FCSCD/DPD/CGD	ExCo	n/a
Monthly	Key highlights on regulatory developments	RCD	Joint AC/RC	n/a
Quarterly	Customer Complaints Report Statistical Complaints report (based on EBA Guidelines)	RCD	M-RCD	CBC
Quarterly	Nominations & Corporate Governance Committee report	CGD	NCGC	n/a
Quarterly	MiFID statistical report	RCD	EDX Platform	CBC
Quarterly	CSDR report		EDX Platform	CBC
Annually	Annual Compliance Report	RCD	AC / BOD	CBC
Annually	Nominations & Corporate Governance Committee action plan	CGD	NCGC	n/a
Annually	Board evaluation Report (structure, size & composition of the BOD and Board Committees, assessment of the independence of each non-executive director, assessment of the skills, knowledge, and experience of the members	CGD	NCGC	CBC
Annually	Annual Corporate Governance Report	CGD	NCGC / AC	CSE

Frequency of reporting	Report Title	CD responsible department	Submitted to	Competent Authority
Annually	Compliance Division action plan	RCD/FCSCD/DPD/CGD	AC / CEO	CBC
Annually	Compliance with Corporate Governance Code of the CSE and the UK Code	CGD	NCGC	n/a
Annually	FATCA/CRS	RCD	Ariadni Portal	Cy Tax Dept
Ad-hoc	Breaches to Data Protection Commissioner	DPD	N/A	Data Protection Commissioner
Bi annual	Crypto Report	FCSCD	N/A	CBC
Bi annual	AML/CFT SIX – MONTHLY RETURN	IGOD		CBC
Daily	Bank Accounts Registry Central Bank (BAR)	IGOD		CBC
Monthly	Monthly statement of large cash transactions and funds transfers	IGOD		CBC
Monthly	Monthly statement of customer loans and deposits based on the country of permanent residence of the beneficial owner	FCSCD IGOD		CBC
Quarterly	CIP and IIP Report	FCSCD		CBC
Annually	AMLCO Risk Management Report	FCSCD	AC/BOD	CBC
Annually	AMLCO Sanction Risk Management Report	FCSCD	AC/BOD	CBC
Annually	AMLCO Annual Report	FCSCD	AC/BOD	CBC
Annually	Reporting of deposits subject to Russian and Belarusian economic sanctions	FCSCD		CBC
Quarterly	Frozen Funds report	FCSCD		CBC
Quarterly	Reporting Article 8 _Regulation 269/2014	FCSCD		SEOK
Quarterly	Reporting _Article 5a of Regulation 833/2014 Reporting Article 5r of 833/20214	FCSCD FCSCD		European commission CBC or SEOK (new report, has not submitted yet)

Frequency of reporting	Report Title	CD responsible department	Submitted to	Competent Authority
Ad- Hoc	Compliance review reports with key findings and recommendations based on compliance assessments / reviews and investigations	RCD/FCSCD/DPD	CEO, D-CEO, Chairman of the AC, Heads of Control Functions, Exec Director People & Change and Relevant Directors	n/a
Annual	Annual DPO report	DPD	AC	N/A

12. Appendix 4 – Related Policies

Policy Name	Reference Number
Compliance Risk Appetite Statement	CD101
Prevention of Money Laundering and Terrorism Financing Policy	CD102
Sanctions Policy	CD103
Customer Acceptance Policy	CD104
Corporate Governance Guidelines for Group Subsidiaries	CD202
Board Nominations and Diversity Policy	CD203
Corporate Governance Policy & Framework	CD204
Corporate Governance of BOC Executive Committees Policy	CD205
Suitability of Members of the Management Body and Key Function Holders Policy	CD206
Board of Directors Induction and Training Policy	CD207
Compliance Division Charter	CD301
Competition Law Compliance Policy	CD401
Compliance Policy	CD402
Customer Complaints Management Policy	CD403
Market Abuse Policy	CD404
Financial Tax Exchange Information Policy	CD406
Whistleblowing Policy	CD407
Coordination and Communication with Authorities Policy	CD409
MiFID Policy	CD410
MIFID Client Categorisation Policy	CD411
MIFID Conflicts of Interest Policy	CD412
MIFID Costs and Charges Policy	CD413
MIFID Order Execution Policy	CD414
MIFID Research Policy	CD415
MIFID Safeguarding Client Assets Policy	CD416

Policy Name	Reference Number
MIFID Freedom of Establishment and the Provision of Investment Services Policy	CD417
MIFID Appropriateness and Suitability Policy	CD418
MIFID Product Governance Policy	CD419
MIFID Record Keeping and Electronic Communications Policy	CD420
MIFID Transaction Reporting Policy	CD421
MIFID Tied Agents Policy	CD422
Anti-bribery and Corruption Policy	CD423
Treating Customers Fairly Policy	CD424
Conflicts of Interest Policy	CD427
Personal Data Protection Compliance Policy	CD501
Operational Risk Management Policy	
Information Security Framework	
Fraud Risk Management Policy	
Risk Appetite Framework	
Business Continuity Management Policy	
New Products/Services Management Policy	
Third Party Risk Management and Outsourcing Policy	
Control Functions Operational Framework	