
COMPLIANCE GOVERNANCE POLICY

1. Purpose

This Policy sets out an appropriate governance structure for the management and implementation of the compliance function within the Bank and its subsidiaries in Cyprus and abroad. Furthermore, this Policy ensures that there are proper procedures in place for the Bank to comply with the requirements of the CBC Directive on "Governance and Management Arrangements in Credit Institutions (the «CBC Directive») and the EBA Guidelines on Internal Governance (issued 27/9/2017).

This policy should be read in parallel with the Compliance Charter.

2. Sectors Affected

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 in Cyprus and abroad.

3. Policy

A. Compliance Scope

The scope of compliance covers all relevant areas of the Bank and the subsidiaries in Cyprus and abroad. The compliance function establishes, implements and maintains appropriate mechanisms and activities based on the below four areas described in detail in the Compliance Charter:

1. Regulatory Framework
 2. Risk identification, assessment, monitoring
 3. Compliance culture-raising awareness and advisory services
 4. Compliance Reporting
- Within the scope of compliance fall the below areas:
 - i. Client related integrity risk
 - ii. Personal conduct related integrity risk
 - iii. Financial services conduct related integrity risk
 - iv. Organizational conduct related integrity risk
 - v. Organization, systems, procedures

Please refer to Appendix 2 for a more detailed analysis of the areas that fall within the scope of compliance function.

B. Compliance Function Principles

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

I. Compliance starts at the Top

The Board of Directors (BOD) is the owner of compliance 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 the tolerance and tone at the top and ensuring oversight of compliance.

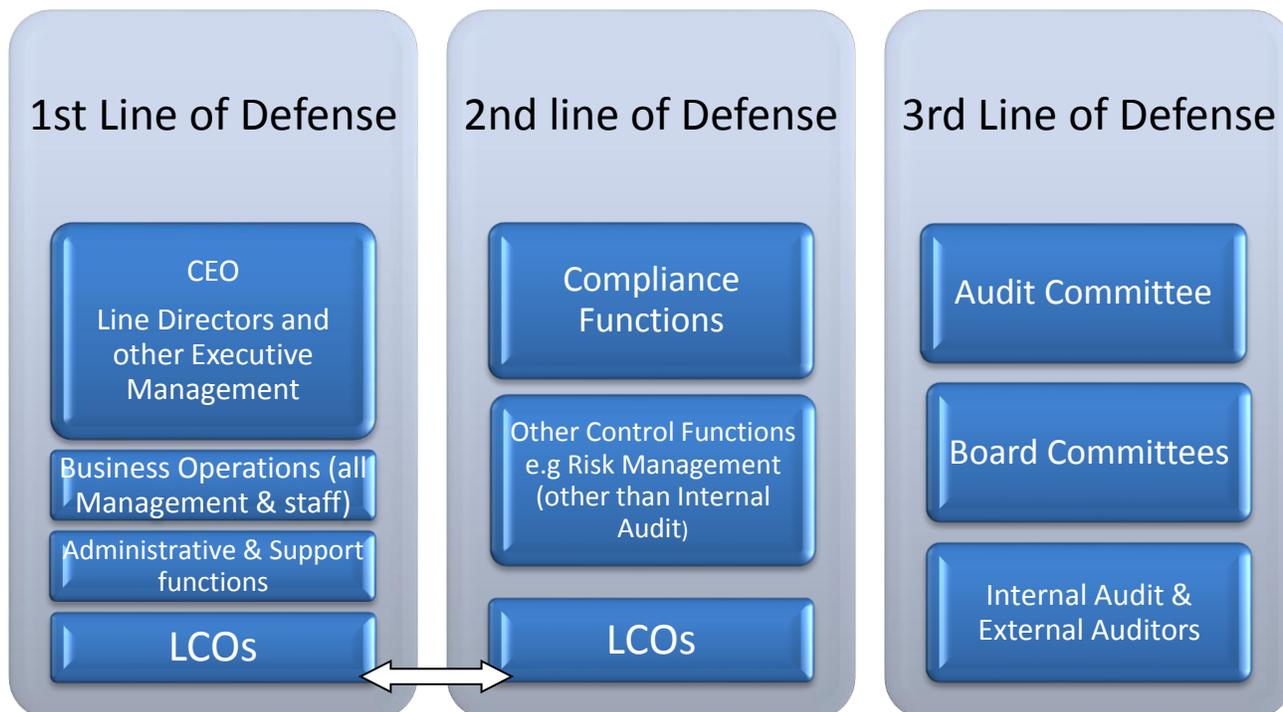
II. Compliance is a responsibility that every employee share.

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 (as below), and exercise of good corporate citizenship and responsible corporate behavior. Each employee via their Management & Compliance Officer is obliged to adhere the compliance guidelines. Therefore, the Bank and its subsidiaries ensure through policies, procedures, effective communication, training and other monitoring measures that Management and staff:

- understand the regulations, standards and best practices associated with the discharge of their operational duties and responsibilities;
- understand associated compliance risks and the need and responsibility for managing these risks;
- understand the importance of internal control functions in managing compliance risks and facilitates their work; and
- Identify with the support of the compliance function (e.g. LCOs & CD) applicable key compliance risks.

III. 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.



IV. The compliance function Independence

The compliance function is independent from operational functions and has adequate authority, stature and access to the management body.

V. The compliance function should have the resources to carry out its responsibilities effectively

The resources to be provided for the compliance function at all levels should 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 should have the necessary qualifications, experience as well as professional and personal qualities to enable them to carry out their specific duties.

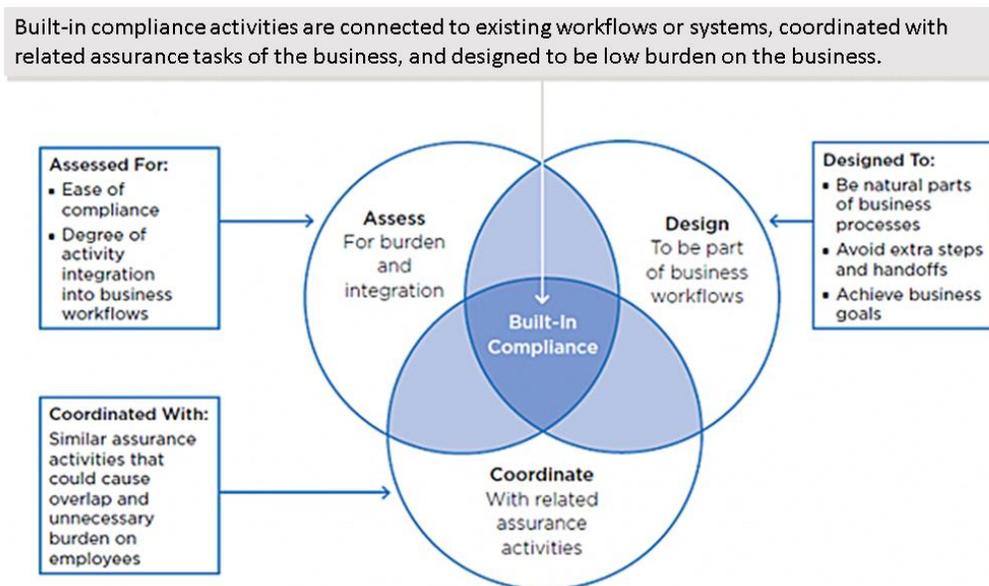
VI. Investigations and external expertise

The compliance function should 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 their responsibilities.

VII. Compliance should be Embedded in the Operations of the Business

Compliance programs must be embedded in the operations of the business meaning 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 functions must include in their program the following:

- i. Design compliance to be part of business workflows
- ii. Coordinate compliance and related assurance activities
- iii. Assess how well compliance is built into the business.



Behavior that creates and supports compliance should be encouraged and behavior that compromises compliance should not be tolerated.

VIII. Access to all information required to perform compliance duties

Compliance staff has 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 should 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.

IX. Outsourcing

Compliance should 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 Director of Compliance.

C. Key Compliance activities & Pillars

Our mission is supported by 5 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 Head of the Compliance Function 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:

- a. Identifying, on an on-going basis, with the cooperation of the Bank's Legal Services, the Regulatory Affairs Department (RAD) and other competent units of the Bank, the legal, regulatory framework which governs and/or affects the operations of the Bank and its subsidiaries.
- b. Ensuring that a complete and updated register of the legal and regulatory framework is maintained and that emanating compliance obligations are documented. This register is widely known as the **Compliance Chart**.
- c. Communicating to business units, branches and subsidiaries, the legal, regulatory and business framework applicable to them. The departments, branches and subsidiaries, in cooperation with Compliance need to:
 - i. identify the compliance obligations emanating from these requirements.
 - ii. measure and assess the impact of these obligations on the bank's processes, procedures and operations.
 - iii. assess the appropriateness of the compliance policies and procedures, following up of any deficiencies identified and, where necessary, formulating proposals for amendments.
- d. Identifying and documenting the compliance risks associated with the Bank's business activities, on a pro-active basis.
- e. Develop 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. Such practices may be reviewed regularly to encompass new technological, or other characteristics.
- f. Maintaining and updating on a quarterly basis a Regulatory Compliance Matrix (RCM) that encompasses the entire regulatory framework that affects the Bank.
 - g. Preparing and subsequently reviewing and revising accordingly on an annual basis all compliance policies on key compliance related issues.
 - h. Formulating proposals for organizational and procedural changes to ensure that identified compliance risks are appropriately managed.
 - i. Ensuring the usage of appropriate tools and mechanisms for monitoring compliance activities which, inter alia, include:
 - the assessment of periodic reports submitted by compliance officers
 - the use of aggregated risk measurements such as risk indicators.
 - 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).
 - targeted trade surveillance, observation of procedures, desk reviews and/or interviewing relevant staff.
 - the verification of how compliance policies and procedures are implemented in practice through on-site reviews
 - the investigation of possible breaches of the compliance policy and regulatory framework with the assistance, if deemed necessary, of experts from within the institution such as experts from the internal audit function or legal services department.
 - j. Ensuring there is an internal alert procedure in place to facilitate employees in reporting confidentially concerns, shortcomings, or potential violations in respect of institutions policies, legal, regulatory, business obligations or ethical issues. The alert procedure should 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.
 - k. Overseeing the complaints process and utilizing the relevant information for improvement of processes and procedures;
 - l. Periodically reassessing and reviewing the scope of compliance audits/ reviews to be performed.
 - m. Cooperate and exchange information with other internal control and risk management functions on compliance matters.
 - n. Ensure compliance with external and internal Regulatory bodies/authorities through reports submitted by LCOs.
 - o. Organizing regular training for management and members of staff for compliance and regulatory matters to increase compliance awareness.
 - p. Providing guidance /advise to staff either orally or in writing on compliance queries.
 - q. 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.

- Ϛ. The CD, in close cooperation with the Risk Management Function should be involved in the establishment of the framework and the approval of new products and new procedures to ensure that all material risks are taken into account and that the institution complies with the current legal framework and, where appropriate, any known forthcoming changes to legislation, regulation and supervisory requirements.
- s. The establishment of a network of Local Compliance Officers throughout the Bank. LCO's have a dual reporting line to departmental managers and CD. LCOs are assessed on an annual basis.
- t. 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.
- u. 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 should be informed.

D. COMPLIANCE REPORTING

Compliance reporting entails:

- 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;
- Reporting in the correct format and ensuring minimum requirements are in accordance with the relevant Directive of CBC and the guidelines of the Head of the Compliance Function. The Head of the Compliance Function must submit, on a quarterly basis a report, to the Audit Committee copied to EXCO. The minimum requirements to be covered in the report are outlined in the CBC Directive.
- Dual reporting of LCOs to their Line Managers and Director of Compliance.
- The Head of Compliance shall submit 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 CEO. This report is subsequently submitted to the Central Bank of Cyprus.
- An Annual Corporate Governance Report.
- An Annual Assessment of the performance of the Board of Directors.
- A compliance reporting diary maintained to facilitate compliance reporting responsibilities.

E. COMPLIANCE REPORTING LINES

The Compliance reporting Lines are described in the Compliance charter and the LCO assessment procedure is described in the compliance manual.

4. 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. Definitions

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.

Annual Compliance Program: sets out the compliance planned activities, such as the implementation and review of specific policies and procedures, compliance risk assessment, 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.

Compliance Chart: The Compliance function maintains an updated register of the existing regulatory framework (laws, regulations and self-regulatory standards) and identifies in cooperation with the departments /subsidiaries concerned the compliance obligations emanating from each regulatory framework.

CRAM: The Compliance Risk Assessment Methodology provides a unified way to capture, assess, mitigate and document Compliance risks. Within this methodology, KCRI refers to Key Compliance Risk Indicators. Detailed description of CRAM is analyzed in a separate document called "CRAM".

Regulatory Compliance Matrix: CD maintains a consolidated Regulatory Compliance Matrix (RCM) that encompasses the entire regulatory framework (only laws and regulations from competent authorities not policies) that affects the Group. The matrix is completed based on the Compliance Chart and indicates the Owner for each legislation included in the Compliance Chart and the Responsible Division/Director and it is agreed with Divisional Directors accordingly. Moreover, the Compliance Matrix reflects the status of compliance of each law which is monitored on an ongoing basis by the Responsible Division's LCO and officially on a quarterly basis by the CD. This matrix



is submitted at least on a quarterly basis to ExCo. For the preparation of RCM, the definitions are important as classified in the policy Regulatory co-ordination and communication with competent authorities:

6. Roles & Responsibilities

Based on the three Lines of Defence Model all responsibilities in relation to the compliance function are clearly assigned, explained and monitored (please refer to Appendix 1).

7. Supporting Procedures

The principles and procedures set out in this policy are implemented via the various compliance related policies and procedures including Compliance Division Procedures Manual, CRAM, Audit Methodology and relevant manuals.

Appendix 1**RESPONSIBILITIES IN RELATION TO COMPLIANCE**

Board of Directors	<ul style="list-style-type: none"> a. Retains the ultimate responsibility for compliance of the Bank with applicable laws, regulations and ethical standards. b. Oversees the implementation of a well-documented compliance policy, which should be communicated to all staff. c. Has oversight responsibility for the management of the Bank's compliance risks and ensures a process is set up to regularly assess changes in the laws and regulations applicable to the Group's activities. d. Establishes a compliance function and ensures its authority to act independently. e. Carries out oversight of Compliance. f. Sets the tone at the top. g. Include compliance responsibilities in job descriptions of top managers.
Audit Committee	<ul style="list-style-type: none"> a. Advises the Board, drawing on the work of the compliance function, on the adequacy and effectiveness of the framework for business conduct. b. Advises the Board, drawing on the work of the compliance function internal and external auditors, on the adequacy and effectiveness of the compliance framework. c. Assesses and monitors the independence, adequacy and effectiveness of the compliance function. d. Submits to the Board recommendations for the appointment or removal of the head of the compliance function. e. Annually appraises the head of the compliance function and subsequently submits the appraisal to the Board. f. Reviews and approves the compliance action plan. g. Reviews and approves the budget of the compliance function, ensuring that it's sufficiently flexible to adapt to variations in response to developments
Ethics, Conduct and Culture Committee	<ul style="list-style-type: none"> a. Oversees management's efforts to foster a culture of ethics within the Group to ensure culture and business



	<p>integrity are applied to all activities of the Group and discourage unethical behaviour.</p> <ul style="list-style-type: none"> b. Review and assess the Bank’s strategy, communications and policies relating to the Code of Conduct. c. Monitors compliance with the Code of Conduct and reviews disciplinary controls. d. Oversees HR initiatives that foster employee engagement and create a culture of ethics and compliance.
<p>CEO & Top management</p>	<p>The Bank’s Senior Management is responsible for the effective management of the compliance risks to:</p> <ul style="list-style-type: none"> a. Allocate adequate and appropriate resources to establish, develop, implement, evaluate, maintain and improve the compliance management methodology. b. Ensure responsibilities and authorities for relevant roles are assigned and communicated to all staff within the Bank and its subsidiaries in Cyprus and abroad. c. Ensure that the compliance function is adequately resourced with persons possessing adequate qualifications. d. Ensure that prompt remedial or disciplinary action is taken if compliance breaches and failures are identified. e. Ensure the implementation of and adherence to the Compliance Policy and its minimum standard. f. Ensure that effective and timely systems of reporting are in place.
<p>Line Directors</p>	<ul style="list-style-type: none"> a. Management of a business unit, regardless of its legal or organizational form, is responsible for implementing the business unit management systems, policies and procedures. b. Providing reasonable assurance that breaches of applicable legal and/or regulatory standards and obligations are prevented, and for safeguarding that business is conducted in accordance with this policy. c. Cooperate with and support the compliance function and encourage employees to do the same. d. Ensure that a suitable person is appointed as Local Compliance Officer with a reporting line to them.



	<ul style="list-style-type: none"> e. Comply and be seen to comply with policies, procedures and processes and attend and support compliance training activities. f. Identify and communicate compliance risks in their activities. g. Integrate compliance performance into employee performance
Head of Compliance Function	<ul style="list-style-type: none"> i. Please refer to the compliance Charter
Regulatory and Privacy Compliance Department	<ul style="list-style-type: none"> a. The implementation of appropriate procedures and controls for the prompt and on-going compliance of the bank and its subsidiary companies in Cyprus with the existing regulatory framework b. Identifying, on an on-going basis, with the assistance of the bank’s Legal Services, RAD 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). c. Arrange trainings of relevant staff. d. Establish and monitor the network of Local Compliance Officers. e. Assisting senior management in the implementation of the compliance policy and the effective management of the compliance risks faced by the bank. f. Acts along with RAD as the primary point of contact with the Competent Authorities and ensures the communication, to the units/ branches/ subsidiaries concerned of the regulatory framework / obligations which affect their areas of operations. g. 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. h. Carrying out, on a periodic basis the review, including on-site reviews of departments/ branches/ subsidiaries assessing the adequacy of their procedures and controls.
Governance and Markets Compliance Department	<ul style="list-style-type: none"> a. Monitors Corporate Governance Compliance in relation to the Board’s functioning, its Committees and its members.



	<ul style="list-style-type: none"> b. Reviews the effectiveness and adequacy of the corporate governance policy of the Bank, incorporates new regulatory provisions and other best practices and prepares amendments. c. Ensures compliance with the Cyprus Stock Exchange Code and the UK Corporate Governance Code as well as with the relevant Governance Directives of the CBC and relevant directives/circulars of the CySEC. d. Monitors compliance of the Bank with Corporate Governance policies in coordination with the NCGC and makes appropriate recommendations to the Board. e. Drafts the Annual Corporate Governance Report in coordination with the NCGC and makes appropriate recommendations to the Board. f. Facilitates the training of the Board members on their duties and responsibilities in relation to Corporate Governance. g. Monitor Compliance with Market Abuse Regulatory Framework and Mifid Regulatory Framework. h. Assesses Conflicts of Interest.
Data Protection Officer (DPO)	<ul style="list-style-type: none"> a. Please refer to the Personal Data Protection Compliance Policy
Other Control Functions (Risk Management, Information Security, Internal Audit)	<ul style="list-style-type: none"> a. Internal control functions should have a close relationship and ensure that there is a clearly identified allocation and division of responsibilities. b. Should promptly inform the heads of other internal control functions of any findings relating to them. c. Meetings of Control Functions.
Risk Management Function	<ul style="list-style-type: none"> a. Communicate accordingly with CD on the institution’s management of compliance risk b. The Compliance function and the Risk Management Function should cooperate and exchange information to perform their respective tasks. c. The findings of the compliance function should be considered by the Risk Management function within the decision –making process
Internal Audit	<ul style="list-style-type: none"> a. The scope and breadth of the activities of the compliance function should be subject to periodic review by the internal audit function. Internal Audit



	<p>should promptly inform the CD of any audit findings relating to compliance.</p> <p>b. Internal Audit acts as a third line of defense providing relevant assurances to the BOD of the effectiveness of the Compliance function.</p>
<p>Legal Services</p>	<p>a. The Legal Department has the primary role in analyzing and considering the impact of new laws and regulations, where the Compliance department generally has the primary role to translate (or ensure translation of) these external rules into clear and workable internal rules.</p>
<p>Local Compliance Officers (LCO)</p>	<p>a. Have a formal status within their department</p> <p>b. Entitled to have access to the information and personnel necessary to carry out their responsibilities.</p> <p>c. Retain their independence and when necessary take appropriate measures to achieve this.</p> <p>d. Local Compliance Officers depending on their role act as first and second line of defense.</p> <p>e. Ensure that they have adequate resources, time and tools to perform their compliance duties.</p> <p>f. Have direct reporting line to their Departmental Manager and functional reporting line to the Director of Compliance.</p> <p>g. The overall role of the (LCO) is to pro-actively support Local Management in managing effectively key compliance risks in their area of business.</p> <p>h. Supports Unit Management and staff in identifying, measuring and managing key compliance risks.</p> <p>i. Provides support and oversight to the Business management in the implementation of regulatory and business changes.</p> <p>j. Maintains and updates the compliance chart of the Unit.</p> <p>k. Maintains and updates on a quarterly basis the Regulatory Compliance Matrix.</p> <p>l. Provides leadership on initiatives which affect several areas of the Business, whether these relate to work which is by nature remedial, developmental or the result of new regulation.</p> <p>m. Reports at least every six months to the Director of Compliance on compliance issues.</p>



	<ul style="list-style-type: none"> n. Monitors customer complaints statistics and relevant procedure followed by Business Lines and reports accordingly, monitoring remedial actions. o. Develops in co-operation with Unit Management a local compliance annual plan, submits it to the Regulatory and Ethics Compliance department for approval and monitors its implementation. p. Ensures that the Business Unit has appropriate arrangements for staff training on compliance issues and/or trains staff accordingly. q. Ensures regulatory reports are duly submitted to Competent Authorities as per the Regulatory Reports Register created and maintained by RAD and reports deviations to GCD. r. Is assessed on his/her performance as an LCO using measurable if available KPIs. s. Maintains and updates the COI/Gift registry.
All staff	<ul style="list-style-type: none"> a. Adhere to the compliance obligations of the organization that are relevant to their positions and duties. b. Participate in training relevant to compliance issues. c. Report compliance concerns, issues and failures.

Appendix 2

Scope of Compliance

Client related Integrity Risk	<ul style="list-style-type: none"> i. Money laundering ii. Terrorist financing iii. Other external crime and fraud iv. Customer due diligence v. Sanctions & embargoes <p>This section covers matters in relation to money laundering and as such is covered under the ML14 1 002 – Policy.</p>
Personal Conduct related Integrity Risk	<ul style="list-style-type: none"> i. Market abuse and personal transactions ii. Business principles and code of conduct iii. Anti-Bribery iv. Inducements (incl. gifts) v. Whistleblowing vi. MIFID vii. Personal Transactions viii. COI
Financial Services Conduct Related Integrity Risk	<ul style="list-style-type: none"> i. Marketing, sales and trading conduct ii. Conduct of advisory business iii. Transparency of product offerings iv. Customer interest and protection v. Complaint handling processes vi. Data protection/privacy vii. Investment services & activities
Organizational Conduct related Integrity Risk	<ul style="list-style-type: none"> i. Corporate Governance ii. Conflicts of interest iii. Internal standards with respect to new product approval and product review process iv. Accounting and auditing requirements* v. Tax laws relevant to the structuring of banking products or customer advice * vi. Treating customers fairly vii. Sector/industry (acceptance) standards viii. Oversight of intermediaries ix. Mergers and acquisitions x. Regulatory registration requirements* xi. Anti-Trust (competition) xii. Social and green responsibility xiii. Information technology and electronic banking



	<ul style="list-style-type: none"> xiv. Market abuse and organizational insider trading (incl. Chinese walls) xv. Reputational Risk
Organization, systems, procedures	<ul style="list-style-type: none"> i. Organization of compliance ii. IT systems and infrastructure to support compliance iii. Compliance internal procedures/manuals/ methodologies
<p>*Compliance with laws, regulations and standards in relation to accounting, tax and related risks are the primary terrain of the Finance Department of the Bank. In this case the CD has a high-level overview of the organization of compliance and an LCO at the Finance Division has been assigned to assist management for effectively addressing these matters.</p>	

The information contained on this website is provided only as general information. The material on this website is owned by Bank of Cyprus Holdings Plc.

While Bank of Cyprus Holdings Plc endeavors to keep information up to date, it makes no representations or warranties of any kind, express or implied, about the completeness accuracy, suitability or availability with respect to the information contained on the website for any purpose. Any reliance you place on such information is therefore strictly at your own risk.

In no event will Bank of Cyprus Holdings Plc be liable for any loss or damage including without limitation, indirect or consequential loss of damage, or any loss or damage whatsoever arising out of, or in connection with the use of this website's information.