GROUP POLICY - COMPLIANCE POLICY

COMPLIANCE POLICY

Title	**Group Compliance Policy**
Policy Number	**CD402**
Revision Number	14
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	Appendix 2

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	Minor revisions
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.
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

Version	Approval Date	Initiator	Approver	Description / Changes
14.0		Compliance Division	Board of Directors (through the Audit Committee)	Additions relating to covering the ISO audit review gaps (Appendix 3 & 4)

TABLE OF CONTENTS

1. PURPOSE AND SCOPE

The purpose of this Policy is to outline the compliance framework that is applicable to the **Bank of Cyprus Public Company Ltd and its subsidiaries (referred to as BoC)** and must be read alongside the Compliance Charter and the Control Functions Common Operational Framework. This policy is accessible to all staff through the corporate portal and to customers via the corporate website.

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

As a highly regulated entity, BoC must adhere to numerous regulatory requirements. The scope of compliance obligations includes:

1. Regulatory compliance related to CY & EU Laws/Directives.
2. Voluntary Governance Codes such as the UK Corporate Governance Code 2018.
3. Corporate Governance Compliance matters.
4. Relevant legislation and regulations concerning Data Protection.
5. Legislation and regulations on Anti-Money Laundering and Combating Terrorism Financing, including adherence to relevant legal and regulatory requirements/principles derived from the provisions 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.

2. ABBREVIATIONS

Within this document, the following abbreviations are used:

Abbreviation	Definition
AC	Audit Committee
AML	Anti-Money Laundering
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
CGF	Corporate Governance Function
DPD	Data Privacy 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

Abbreviation	Definition
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, and corrective actions to address any control weaknesses that have been identified. The Action Plan adopts a risk-based methodology.
2. **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.
3. **Compliance Charter**
   The Compliance Charter is a document that outlines the BoC regulatory environment (laws, regulations, and standards). It is maintained by the Compliance Division.
4. **Compliance Management System (CMS)**
   ISO 37301 is an international standard that sets out the requirements for establishing, implementing, maintaining, and improving an effective compliance management system (CMS) within an organization. The standard was published in 2021 and is the successor to ISO 19600, which was first published in 2014. More information on the ISO, Policy Statement and the ISO Manual, can be found in Appendix 3 and Appendix 4 (respectively).
   The Compliance Management System defines how BoC manages its compliance procedures. It incorporates specific elements and the extent of the involvement of the Governing Body, Top Management, Control Functions and staff to achieve:
   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.
5. **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 1).
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:

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

6. **Compliance Liaisons (CLs)**

   Compliance Liaisons (CL) are officers assigned with the responsibility of supporting their management in the implementation of regulatory changes, compliance issues and controls and 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.

7. **Compliance Liaison's Line 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 with targets and recognize the CL's work and effort during the annual appraisal process.

8. **Compliance Risk**

   The potential harm to the organization's business model, reputation, and financial health from not complying with laws, internal standards, and stakeholder expectations. The impact of uncertainty on objectives can be either beneficial or detrimental.

9. **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 fines and penalties), as well as any other indirect consequences that may result from regulatory or reputational issues such as relations / service to clients, relations with mass media, impact on the Group's reputation, etc.

10. **Inherent Risk**

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

11. **Residual Risk**

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

12. **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.

13. **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.

14. **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 (OE099).

15. **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.

16. **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.

17. **Subsidiary Compliance Officer (SCO)**

Each subsidiary designates its own Compliance Officer (Subsidiary Compliance Officer - SCO) who reports to the Subsidiary's Audit Committee. Additionally, SCOs have a secondary reporting line to the Compliance Division, which is responsible for ongoing and effective oversight of these officers. SCOs share the same duties as the Compliance Division staff within their scope.

4. GENERAL PRINCIPLES

BoC implements an integrated and institutional-wide compliance culture based on the following principles:

1. **Compliance starts at the Top**
   The Board of Directors (BOD) is the owner of the compliance framework and is ultimately responsible for its management. To meet this responsibility, the BOD and executive management must lead by example, show dedication to compliance standards, and establish the tone and tolerance from the top.
2. **Compliance is a responsibility that every employee shares**
   Every BoC employee is responsible for compliance, regardless of their role. This means committing to strong compliance, following the three lines of defense, and demonstrating good corporate citizenship. Management and Compliance Liaisons must ensure staff are aware of these obligations. To support this, BoC uses policies, procedures, communication, training, and monitoring to ensure:
   a. Employees are knowledgeable about regulations, standards, and best practices relevant to their roles.
   b. Employees acknowledge and handle compliance risks.
   c. Employees value the significance of internal controls in mitigating these risks.
   d. Employees detect, evaluate, and manage major compliance risks with assistance from compliance staff.
3. **The Control Functions Common Operational Framework**
   BoC uses the three lines of defense model to govern compliance principles and ensure that a culture of compliance is spread throughout all levels. This model is detailed in the Control Functions Common Operational Framework.
4. **The compliance function independence**
   The Compliance Function operates as the second line of defense, maintaining independence from operational roles. It possesses sufficient authority, status, and direct access to the management body, and reports independently to the Audit Committee.
5. **The Compliance Function shall have the resources to carry out its responsibilities effectively**
   The Compliance Function is equipped with sufficient and suitable resources at all levels to effectively manage compliance risk within BoC. Compliance officers possess the necessary skills, knowledge, and experience, as well as the professional and personal attributes required for their roles and have access to ongoing training.
6. **Investigations and external expertise**
   The Compliance Function investigates potential Policy breaches, can hire external experts, if necessary, request support from Internal Audit, and access BoC's records and files within its duties.
7. **Compliance shall be embedded in the operations of the business**
   Compliance is woven into the business's daily operations, not treated as a separate oversight. The Annual Action Plan for the Compliance Function includes:
   a. Integrating compliance into business workflows.
   b. Coordinating compliance and assurance activities.
   c. Evaluating how effective compliance is embedded in business.
   d. Promoting behavior that supports compliance and rejecting any that undermines it.

8. **Access to all information required to perform compliance duties**
   The Compliance Function staff can independently contact any employee and access necessary records or information to fulfill their duties.
9. **Outsourcing**
   BoC considers compliance a fundamental responsibility. While compliance tasks can be delegated externally through correct protocols, they must always be under the suitable supervision of the Chief Compliance Officer.

5. COMPLIANCE ACTIVITIES AND PILLARS

5.1. Strategic Pillars

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

1. Business Support & Monitoring Assurance
2. Compliance Policy & Operating Model
3. Digitization
4. Awareness & Cultural Empowerment

The Compliance Division crafts and manages an Annual Action Plan, highlighting all relevant compliance activities considering risk levels. Activities include:

1. Collaborating with Legal Services and other BoC units to identify governing legal frameworks.
2. Maintaining an updated register of legal obligations and supporting action plans.
3. Informing business units about applicable legal, regulatory, and business frameworks, identifying compliance obligations and gaps.
4. Measuring the impact of obligations on BoC's processes via risk scoring.
5. Assessing compliance policies, addressing deficiencies, and proposing amendments.
6. Proactively managing compliance risks in business activities.
7. Implementing methodologies to measure compliance risk using enhanced Operational Risk Management scoring.
8. Documenting compliance risks tied to new/amended laws or significant organizational changes.

Additional responsibilities involve reviewing and revising compliance policies annually, ensuring effective management of compliance risks, using various tools for monitoring compliance, conducting reviews, investigating breaches, including internal reporting systems, and overseeing complaint processes.

Training requirements: The Division also provides guidance and issues instructions to align internal procedures with regulatory changes. In collaboration with the risk management function, it helps establish frameworks for new products and procedures, ensuring alignment with current legal frameworks.

The Division evaluates CLs annually (excluding Data Privacy Department). It works with Regulatory Affairs as the main liaison with authorities and ensures subsidiaries comply with local regulations, notifying the Chief Compliance Officer of any legal conflicts.

5.2. Identification of Compliance risks

Compliance risks are identified using various sources, listed below:

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.
Compliance risk assessments	Regulatory, data privacy and financial crime risks identified through the assessment of new or amended policies, processes and procedures, project assessments, new product/services assessments, outsourcing arrangements, changes in operating models and structures and any other ad-hoc assessments with regulatory, data privacy or financial crime impact.	OneSumX (for identified gaps) / RCMS (for identified risks)
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 with the effective identification and minimization of 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	Compliance risk management system, (OneSumX) for the recording of findings and recommendations and the

Identification source	Description	Registration in:
	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 Group-Wide Review which addresses important KRIs (applicable for FCSCD only). • Other types of Reviews following ad-hoc requests by regulators or standard assurance requirements by regulations, which are only applicable for RCD.	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

5.3. Processes and Tools for Monitoring and Managing Compliance Risks

Various methods and sources are used to track compliance risks. The following table outlines the main tools for effectively monitoring and managing these risks and the sources utilized:

Monitoring source	Description	Registered in:
KRIs	The Compliance Division tracks regulatory risks using Key Risk Indicators (KRIs), monitored monthly. These KRIs, linked to RCMS risks, are reported and maintained within management-defined thresholds. If thresholds are exceeded, the KRI owner and risk owner must create a plan to reduce the risk to an acceptable level. KRIs are included in Monthly and Quarterly reports to top Management, Executive Committees, and 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 documented in the Operational Loss Database system (RCMS) according to the ORM Incidents Methodology. After recording incidents, an assessment is conducted to identify potential control deficiencies that caused the event and areas with increased operational risk. This includes root-cause analysis	RCMS

Monitoring source	Description	Registered in:
	and aggregation analysis to detect loss event patterns and implement actions to prevent recurrence. The Incident Response and Escalation Process is followed depending on the incident's type and severity. Incidents are categorized by cause type, Basel event type, and effect type using the RCMS taxonomy (refer to Appendix 1). Corrective actions must be appropriate to the incident's impact. Incidents of breach/nonconformity/noncompliance with relevant regulations are labeled as "Regulatory" and include potential or actual regulatory penalties, non-compliance with regulatory obligations, and events indicating possible legal faults. These incidents are communicated to the Compliance Division via RCMS for review, root cause analysis, and mitigating actions based on risk categorization (risk taxonomy). The Compliance Division monitors these remedial actions and integrates them into the compliance risk self-assessment process and reporting processes. The plan owner or responsible team/committee continuously assesses the incident's potential impact and severity, implements necessary actions, reviews corrective action effectiveness, and alters applicable processes if required. Moreover, as per the Incident Response and Escalation Process, the corresponding incident management team/committee is activated. Incident escalation and reporting occur when the incident Owner or contingency plan informs the relevant Divisional Director or any other affected Divisional Director. The Head of Business Continuity Risk Management (HBCRM) is informed by the plan Owner, while the Manager Operational Risk Management & Outsourcing Officer is notified by the HBCRM. The incident is then reviewed to determine the causes and assess the possibility of similar incidents occurring. Non-compliance incidents with the CBC Directive are reported to competent authorities within one month of identification, and actions to prevent similar incidents are implemented within two months. The processes described are comprehensively documented in the ORM Incidents Methodology and the Incident Response and Escalation Process, which are available on the BoC's portal.	

Monitoring source	Description	Registered in:
Root cause Analysis	Root Cause Analysis helps employees identify reasons behind specific incidents or problems and suggests corrective actions to prevent recurrence. It addresses significant issues, repetitive errors, unresolved actions, and similar problems across various units. Conducted for all incidents, the analysis seeks to understand control failures as detailed in OE 001 and Incident Management procedures. For major incidents, follow OE 001, section 3 guidelines. Significant incidents include: • Major IT system problems per IT Incident Management Process. • Incidents causing damages ≥ €50K. • New legal actions with damages ≥ €50K. • Regulatory fines or investigations by authorities. • Effectiveness evaluations are sent to the Director of the area where the incident occurred to prevent recurrence.	RCMS
Follow up actions	Pending risk mitigation actions are continuously monitored using the OneSumX and RCMS systems. The Compliance Division oversees and approves of any changes in the follow-up and closure of these actions. It is important to note that once an action is set and a deadline is agreed upon, the CLs update the system with any progress made within the specified timeframe. Upon the completion of actions for a particular risk, the risk level is reassessed in terms of Impact and Likelihood. Any remaining pending actions are updated, or new actions are documented.	RCMS OneSumX

5.4. Internal and External Reporting

The internal and external reporting framework ensures adherence to all compliance obligations. The scope of the reporting framework is determined through KRIs/KPIs measurements, which are evaluated monthly or quarterly and reported to the ExCo monthly and to the Audit and Risk Committees quarterly. These metrics are generated by performing data analysis on information from various systems. The results from monitoring and measurement guide next quarter's actions and the planning of new reviews for the following year's action plan. In more detail, compliance reporting involves:

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. OneSumX ensures the maintenance of internal and external reporting for compliance purposes. Appendix 1 provides a summary of the internal and external reporting.
5. Each year 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 organizational 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.

5.5. Ethics

BoC upholds the utmost standards of ethics and integrity in all its business activities. The Compliance function across all levels ensures these ethical values and practices, as outlined in the code of conduct, code of ethics, and related policies, are enforced. Employees and other stakeholders are expected to embody and sustain these principles and practices in both spirit and letter.

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	• Make 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. • Inform AC of its findings and relevant recommendations.
Legal Services	Responsible for: • Providing general advice to the Group on relevant legislation and providing support, guidance and advice to departmental units in relation to legal issues and legal documentation. • Ensuring clauses in contracts avoid abusive language which goes against the Law.
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 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, 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 he/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 BoC 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 – Reporting & RCMS Taxonomy

Frequency	Report Title	CD responsible department	Internal Recipient	External Recipient
Daily	Bank Accounts Registry Central Bank (BAR)	FCSCD/IGOD	--	CBC
Monthly	Compliance Key Risk Indicators	Divisional	ExCo	n/a
Monthly	Key highlights on regulatory developments	RCD	Joint AC/RC	n/a
Monthly	Monthly statement on large cash transactions and funds transfers	FCSCD/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	Compliance Division Quarterly Report	Divisional	ExCo / AC	n/a
Quarterly	Customer Complaints Report Statistical Complaints report (based on EBA Guidelines)	RCD	M-RCD	CBC
Quarterly	Nominations & Corporate Governance Committee report	CGF	NCGC	n/a
Quarterly	MiFID statistical report	RCD	--	CBC
Quarterly	CSDR report	RCD	--	CBC
Quarterly	CIP and IIP Report	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
Biannually	Crypto Report	FCSCD	--	CBC
Biannually	AML/CFT SIX – MONTHLY RETURN	FCSCD/IGOD	--	CBC
Annually	Annual Compliance Report	RCD	AC / BOD	CBC
Annually	Nominations & Corporate Governance Committee action plan	CGF	NCGC	--
Annually	Board evaluation Report (structure, size & composition of the BOD and Board Committees, assessment of the independence of each non-	CGF	NCGC	CBC

Frequency	Report Title	CD responsible department	Internal Recipient	External Recipient
	executive director, assessment of the skills, knowledge, and experience of the members			
Annually	Annual Corporate Governance Report	CGF	NCGC / AC	CSE
Annually	Compliance Division action plan	Divisional	AC / CEO	CBC
Annually	Compliance with Corporate Governance Code of the CSE and the UK Code	CGF	NCGC	--
Annually	FATCA/CRS	RCD	--	Cy Tax Dept
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
Annually	Annual DPO report	DPD	AC	--
Ad-hoc	Breaches to Data Protection Commissioner	DPD	--	Data Protection Commissioner
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	--

The RCMS taxonomy relating to Compliance is the below:

Level 1	Level 2	Level 3
Regulatory Compliance / Conduct Risk		Failure to comply with new legislation / amendment on existing laws
		Misinterpretation of Regulation

Level 1	Level 2	Level 3
	Improper Business or Market Practices	Breach of regulatory reporting or notification requirements
		Failure to maintain 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 unauthorized products 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
		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 organization, e.g. payment, gifts, hospitality
		Benefits obtained for an employee's personal gain, rather than for their organization
		Failure to manage conflicts of interest
		Performance of activities that's beyond the position or remit of an employee
Financial Crime Risk	Money Laundering	Non-compliance with Guidelines including non-performing World Check, obtaining approval for high-risk customers

Level 1	Level 2	Level 3
	and Terrorism Financing Risks	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
		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

Level 1	Level 2	Level 3
		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
	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 – 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 Categorization 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
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	OE099
Information Security Framework	--
Fraud Risk Management Policy	--
Risk Appetite Framework	--
Business Continuity Management Policy	--

Policy Name	Reference Number
New Products/Services Management Policy	OE117
Third Party Risk Management and Outsourcing Policy	OE199
Control Functions Operational Framework	--

11. Appendix 3 - Policy Statement for ISO 37301 [Clause 5.2]

Bank of Cyprus Public Company Ltd

Bank of Cyprus Public Company Ltd (BoC), established in 1899, is the largest banking and financial services provider in Cyprus. It offers comprehensive services including retail, corporate, private banking, wealth management, and international banking, operating through divisions and leadership roles for both the Bank and its subsidiaries.

At Bank of Cyprus Public Company Ltd, we are unwavering in our commitment to uphold the highest standards of compliance and ethical conduct in all aspects of our operations. As a leading financial institution, we recognize the critical importance of maintaining a robust compliance management system to ensure integrity, transparency, and accountability.

The Bank of Cyprus's Compliance Division plays a critical role in maintaining the integrity and operational soundness of the organization. The Compliance Division is responsible for ensuring that the Bank adheres to all applicable laws, regulations, and internal policies. The Compliance Division serves as a guardian of the Bank's ethical and regulatory standards, working diligently to mitigate risks and prevent legal breaches.

Our Commitment

The Compliance Division of the Bank of Cyprus Public Company Ltd is dedicated to implementing and maintaining a comprehensive Compliance Management System (CMS) in accordance with the ISO 37301 standard. This international standard provides a framework for the development, implementation, maintenance, and improvement of a compliant culture and practices within our organization.

Framework / Key Principles

- **Integrity**: We adhere to the highest ethical standards, ensuring that our actions are consistent with our values and principles.
- **Transparency**: We maintain open and honest communication with all stakeholders, providing clear and accurate information written in plain language about our compliance policies and practices, which must be implemented and enforced.
- **Accountability**: We take responsibility for our actions and decisions, ensuring that we meet our legal and regulatory obligations.
- **Non-compliance consequences:** We maintain a zero-tolerance policy that can result in sanctions, financial penalties, or disciplinary actions. Employees are encouraged to report compliance concerns without fear of retaliation.
- **Continuous Improvement**: We are committed to continuously enhancing our CMS by regularly reviewing and updating our policies, procedures, and practices.

Objectives

As part of our commitment to ISO 37301, the Compliance Division of the Bank of Cyprus Public Company Ltd aims to:

- Ensure compliance with all relevant laws, regulations, and internal policies including consistency in the Compliance Policy.

- Promote a culture of compliance and ethical behavior throughout the organization.
- Identify and mitigate compliance risks effectively.
- Provide training and support to employees to enhance their understanding and adherence to compliance requirements.
- Foster a proactive approach to identifying, monitoring and addressing compliance issues.

Record and regularly revise the compliance objectives, ensuring they are accessible to stakeholders.

Commitment of Management

Our senior management team is fully committed to the successful implementation of ISO 37301. They provide the necessary resources and support to ensure that the CMS is effective and aligned with the Bank's strategic objectives.

The Bank has established well-defined governance frameworks and allocated responsibilities, ensuring the Compliance Division has direct access to the Governing Body. This setup guarantees its independence and accountability throughout the organization.

Stakeholder Engagement

Bank of Cyprus Public Company Ltd values the input and feedback of our stakeholders. We are dedicated to engaging with our customers, employees, regulators, and other stakeholders to understand their concerns and expectations, and to incorporate their insights into our compliance practices.

Conclusion

Adopting the ISO 37301 standard is a testament to our commitment to excellence in compliance management. Bank of Cyprus Public Company Ltd is dedicated to fostering a culture of integrity, transparency, and accountability, ensuring that we meet the highest standards of ethical conduct and regulatory compliance.

Signed,

Marios Skandalis

Chief Compliance Officer

Bank of Cyprus Public Company Ltd

Date: 22/10/2024

12. Appendix 4: ISO Compliance Management System

The appendix summarizes the requirements of the ISO 37301 standard.

1. Introduction

This document outlines the Compliance Management System (CMS) framework for Bank of Cyprus, aligning with the ISO 37301 standards. The CMS seeks to promote a robust compliance culture, manage compliance risks, and ensure compliance with laws, regulations, and internal policies.

2. Context of the organization

2.1. Understanding the organization and its context [Clause 4.1]

Bank of Cyprus Public Company Ltd (BoC) is the biggest banking and financial services group in Cyprus. Founded in 1899, it provides a full range of services such as retail, corporate, private banking, wealth management, international banking etc. It operates within a structured framework that includes various divisions and leadership roles, covering both the Bank and its subsidiaries. The CMS applies across the entire Bank at the legal entity level, excluding other group subsidiaries.

In alignment with ISO 37301 Clause 4.1, BoC recognizes the necessity of a comprehensive understanding of the organization and its context to establish a robust compliance management system. This entails an in-depth analysis of both internal and external factors that could influence the organization's ability to achieve its compliance objectives. Internal factors include the organization's structure, governance, culture, and resources, while external factors encompass the economic, social, regulatory, and competitive environment within which it operates. By systematically evaluating these elements, the BoC ensures that the compliance strategy is not only aligned with the organization's goals but also adaptable to the dynamic landscape in which it functions. This proactive approach aids in identifying potential risks and opportunities, thereby fostering a resilient and responsive compliance framework.

BoC has determined the external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended result(s) of its CMS are:

Category	Issues
Political	**External Issues** • EU driven Law and new regulations (e.g. ESG) • Legislative Changes affecting banking operations • Corruption and Political Interference • Impact of Geopolitical conflicts (e.g. Sanctions) **Internal Issues** • Compliance with legislative changes • Conflicts of interest • Bank's influence in political sphere as a systemic bank in Cyprus
Economic	**External issues** • External pressure for managing financial risks • Unemployment rates • Inflation

Category	Issues
	• Exchange Rates • Economic conditions such as recessions or changes in interest rates can affect stability and profitability • Market Competition **Internal Issues** • Capital adequacy to support initiatives and absorb losses • Performance rates • Liquidity management • Credit risk management
Social	**External Issues** • Change in client needs impacting types of financial products and services in demand • Changes in education levels of clients leading to higher expectations for transparency and adherence to compliance standards • Changes in employments patterns can affect the use of banking services and consider the need for adjusting products • Increase in environmental awareness and preference towards green products • Social Networks transforming customer service and marketing strategies • Public perception and trust **Internal Issues** • Employee awareness on compliance and strategic goals and tolerance • Employee trainings
Technological	**External Issues** • Rapid technological advancements • Cybersecurity threats • Cloud technology • Technological Advancements can impact on how BoC operates and interacts with customers **Internal Issues** • Secure IT systems • Data protection measures
Environmental	**External Issues** • Consumer preference for green products • Environmental regulations and climate change impacts on banking operations • Renewable Energy Adoption • Energy Efficiency Regulations • Corporate Sustainability practices **Internal Issues** • Internal sustainability initiatives and resource management
Legal	**External Issues** • Compliance requirements

Category	Issues
	• Reputational risk **Internal issues** • Operational risk and fraud management • Litigation and Legal Disputes
Cultural	**External Issues** • Public Trust **Internal Issues** • Compliance Culture • Risk Culture to ensure adherence of all employees to risk management practices • Communication • Employee Engagement • Leadership and Governance • Transparency

2.2. Understanding the needs and expectations of interested parties [Clause 4.2]

In alignment with ISO 37301 Clause 4.2 which mandates organizations to identify and consider the interests of all stakeholders, including customers, regulatory bodies, and employees, to ensure that their requirements are met, and any potential risks are mitigated, BoC not only aligns its operations with international quality management principles but also reinforces its commitment to transparency, accountability, and continuous improvement.

The interested parties in the BoC CMS as were as their possible needs and expectations were identified to be:

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.	Regulatory bodies expect organizations to comply with laws, regulations, and industry standards. They need accurate, prompt reporting and cooperation. Comply with the data protection rules	• 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

Type	Example of bodies	Possible needs and expectations	Control actions
	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 • Commissioner for Personal Data Protection • European Banking Federation • EIOPA • Association of Cyprus Banks		regulatory inspections are promptly implemented. • Incoming correspondence is distributed to business owners, while monitoring BoC's promptness and quality of response requirements and adherence to regulatory rules. • Maintenance of a registry with all the legislative text BoC must comply with. • BoC is rigorously adhering to its reporting obligations. • 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
	• Environmental Commissioner • Digital Security Authority • Single Resolution Group • 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. • It 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 matters 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.	• Customer complaints 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 are publicly available

Type	Example of bodies	Possible needs and expectations
	• Must apply rules and standards equivalent to those of the Bank.	
Vendors Suppliers Contractors Service-providers		• BoC remains ultimately responsible for the outsourced functions / services. • The outsourcing policy in place follows guidelines of EBA as BoC is a regulated entity. • Dedicated department/team to access third party agreements and ensure risks are considered and managed. • Continuous monitoring and assessment of the third parties with whom BoC maintains a relationship.
Owners, shareholders and investors	Investors seek transparency, ethical behavior, and risk management. They need compliance to protect investments.	Annual reports issued by BoC are addressed to shareholders to give a snapshot of what is going on in BoC.
Society and community groups	The community expects responsible corporate behavior, environmental protection, and social responsibility.	Code of ethics and standards of the BoC 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 Correspondent Banks. In addition is a Dedicated Unit within BoC, being responsible for the handling of the Corresponding relationship, whilst the compliance division handling the annual KYC reviews. Dedicated person in 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. • Following guidelines of international standards.

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 • HR and Renumeration Committee • Steering Committees	• 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. • Need to build and maintain trust with stakeholders. • Need to encourage a culture of compliance and learning.	• Set clear reporting lines and governance arrangements. • Appointment of Committees to monitor specialized matters and dedicated to significant components of the Bank's Compliance Management System. • Documented decision making / action plans to mitigate areas of improvement. • Appointment of the Company Secretary responsible for the coordination of meetings / agendas / drafting minutes / monitoring action plans. Minutes drafted to 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.
• HR Department	• 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 BoC's employees (either to all employees or to specific groups) which upon

Type	Example of bodies	Possible needs and expectations
		completion is followed by the relevant assessment. • Communication channels are in place for direct communication between BoC's employees and the 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. • Need to understand compliance requirements and be aware of compliance risks.	• Monthly, quarterly and annual reports prepared by each function. • Internal investigations conducted by each function. • Departmental KRIs in place related to risks identified. • BoC 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 system aims at efficient/effective identification, measurements, management and monitoring of core risks. • KPIs, OKRs considered during their appraisals. • Independence to their operation.

2.3. Determining the scope of the compliance management system [Clause 4.3]

This document outlines the scope and applicability of the CMS. BoC considers the requirements detailed in Section 2.2 for the interested parties, section 2.5 for the Compliance Division's obligations and Section 2.6 for the Compliance Risk Assessments of the ISO 37301 standard as well as the external and internal issues when defining this scope. Detailed information regarding the scope is documented in pertinent sections of the Compliance Policy.

2.4. Compliance Management System [Clause 4.4]

BoC has established, implements, and maintains a documented CMS that complies with the requirements specified in Section 2.2 regarding external and internal issues. The CMS undergoes continual improvement via regular reviews and annual updates, which are approved by the BoD AC.

This Policy encapsulates the BoC's core values, objectives, and its overall compliance risk profile. It is tailored to the BoC's specific context as defined in Section 2.3, addressing both Internal and External Issues through an extensive analysis of factors affecting its compliance efforts. This analysis covers BoC's business model, including strategy, size, operations, and sustainability; the nature and extent of relationships with third-party vendors and partners—also detailed in BoC's relevant outsourcing policies; the prevailing legal and regulatory landscape relevant to the BoC's activities, supported by system usage; current economic conditions, identified through regulatory landscape classification as well as social, cultural, and environmental considerations; and the BoC's internal structure, policies, processes, procedures, resources, and overall compliance culture, all of which are comprehensively reflected in the Compliance Policy.

2.5. Compliance Obligations [Clause 4.5]

This document outlines the systematic approach followed by BoC for identifying compliance obligations by performing:

1. New product / New Services compliance risk assessments.
2. Continuous monitoring of regulatory changes through industry associations, government publications, and legal counsel establishes a regulatory framework to assess the compliance impact of BoC's activities, products, services, obligations.
3. Comprehensive compliance assurance reviews to identify potential compliance risks across BoC's operations.
4. Engage the Compliance Liaisons and Subsidiary Compliance Officers to monitor the activities in their respective departments in response to regulatory requirements.
5. Engage in regulatory projects

The Compliance Division also maintains many Policies relating to compliance matters and annually, a Compliance Division action plan is developed and endorsed by top management, detailing updates to policies, procedures, and training. This ensures ongoing compliance with updated, accurate, and easily accessible documentation for staff.

Therefore, BoC can demonstrate a structured process for identifying, assessing, and managing its compliance obligations.

2.6. Compliance risk assessment [Clause 4.6]

BoC employs a comprehensive, group-wide risk assessment methodology.

1. Identifying Compliance Risks

Compliance risks stem from various sources and have the potential to impact different aspects of BoC's operations. To effectively identify these risks, BoC considers the Compliance Obligations - These obligations include laws, regulations, standards, and internal policies. Understanding these requirements is essential for relating them to BoC's activities, products, services, and relevant operational aspects.

2. Identifying risks relating to Activities, Products, and Services

An examination of all business activities, products, and services is necessary to uncover any compliance risks. This involves scrutinizing every department and function to ensure that no potential risk is overlooked.

3. Analysing Compliance Risks

Once compliance risks have been identified, the next step is to analyze them. This process involves assessing the likelihood and potential impact of each risk using the BoC RCSA Methodology.

4. Evaluating Compliance Risks

Evaluation involves prioritizing compliance risks based on their analysis and determining the appropriate actions to manage them.

5. Mitigation Strategies

BoC develops and implements effective mitigation strategies which are essential for managing compliance risks. These strategies may include policy updates, training programs, process improvements, and enhanced monitoring mechanisms. Detailed action plans outlining the steps taken to address compliance risks are documented and regularly updated. This ensures transparency and accountability within BoC.

6. Monitoring and Review

Compliance risk management is an ongoing process. Organizations must regularly monitor and review their risk mitigation strategies to ensure their effectiveness and make necessary adjustments. Specifically, the Compliance Division oversees all regulatory risks using Key Risk Indicators (KRIs), which are monitored monthly. KRIs have been linked to risks in the RCMS, and their monitoring is configured to adhere to the thresholds set by management. Consequently, depending on the reporting frequency, KRI owners must report the KRIs assigned to them. If KRI thresholds surpass acceptable levels, the KRI owner, along with the risk owner, must develop an action plan to bring the KRI within an acceptable risk appetite level. KRIs are included in monthly reports and quarterly reports to top management, the Executive Committees, and the Audit and Risk Committees. Moreover, detailed information regarding the compliance risk assessment is provided in Section X of this policy.

7. Outsourced and Third-Party Processes

Compliance risks are not limited to internal operations; they can also arise from outsourced and third-party processes. BoC assesses the compliance risks associated with its third-party relationships. This includes suppliers, contractors, service providers, and partners. Due diligence and regular audits as part of this process, identify and mitigate these risks. In general, outsourcing certain functions can bring efficiency but also introduces compliance risks. BoC evaluates these arrangements to ensure that outsourced processes adhere to compliance obligations.

8. Periodic and Situational Assessments

Compliance risk assessments are not a one-time activity. They are conducted periodically and whenever there are significant changes in circumstances or organizational context.

- Periodic Reviews - Regular assessments, such as annual reviews, help organizations stay updated on emerging risks and ensure continuous compliance.
- Material Changes - Situations such as regulatory updates, or significant operational changes necessitate immediate risk reassessment. BoC stays agile and responsive to adapt to these changes effectively.

9. Documentation and Record Keeping

Maintaining comprehensive records of compliance risk assessments and the actions taken to address identified risks is crucial. BoC retains documented information on its compliance risk assessments. This includes risk identification processes, analysis methodologies, evaluation criteria, and mitigation strategies.

3. Leadership [Clause 5]

3.1. Leadership and commitment [Clause 5.1]

3.1.1. Governing Body and top management [Clause 5.1.1]

To show leadership and commitment to the CMS, the BoC governing body and top management ensure that this Policy and objectives align with BoC's strategic direction and are integrated into business processes via regular reports like the Quarterly Report. They also support resource requests for the CMS.

The BoC governing body and top management encourage continuous improvement by providing feedback on CMS processes to achieve outcomes; they support responsibilities within their influence to maintain the independent role of the Compliance Division; they establish BoC's values through policies and procedures for compliance, remain informed about compliance issues, and take necessary actions.

Generally, commitment to compliance is upheld, addressing noncompliance and inappropriate behavior.

3.1.2. Compliance culture [Clause 5.1.2]

At BoC, a strong compliance culture is established and upheld at all levels. The BoC governing body and top management are dedicated to maintaining high standards of behavior, ensuring employees understand their compliance duties and feel empowered to report concerns. This commitment is reinforced through clear communication, regular training, effective internal channels, and recognition of compliance achievements. Noncompliance is strictly not tolerated, as reflected in the annual Risk Culture (ETHOS) scores and Organization Health Index monitoring.

3.1.3. Compliance governance [Clause 5.1.3]

The top management and the governing body of BoC have direct access to the Compliance Division and vice versa. The division maintains its independence by reporting directly to the Board, which ensures its authority and independence.

3.2. Compliance Policy [Clause 5.2]

Refer to Appendix 3.

3.3. Roles, Responsibilities and authorities [Clause 5.3]

3.3.1. Governing body and top management [Clause 5.3.1]

The roles of the Governing Body and Top Management are detailed in the Roles and Responsibilities section within this Policy, as well as in corresponding sections across all Compliance Division policies. These policies are sanctioned by the Board. Any modifications are disseminated through the Organization Department during weekly updates and can be accessed on the corporate portal; some of the policies are also posted on the corporate website.

Both top management and the governing body participate in Compliance Training related to the Regulatory framework during onboarding and every six months thereafter. Additionally, all members of the Governing Body and Top Management are required to undergo training on the Compliance Policy, which outlines their specific roles and responsibilities.

The performance of the Compliance Policy is reported to the governing body and top management through clear reporting structures and defined metrics for compliance assessment. These reports are issued monthly and quarterly, featuring metrics such as KPIs and KRIs to identify compliance risks, incidents, control effectiveness, and findings from compliance reviews.

Top management allocates sufficient resources (personnel, budget, technology) to establish, develop, implement, evaluate, maintain, and enhance the Compliance Policy. They also ensure that strategic and operational goals align with compliance obligations by including their feedback in the reports.

The Governing Body ensures that Top management's performance is measured against predetermined compliance objectives by incorporating specific KPIs into their appraisals.

Integration of compliance performance into employee appraisals is achieved by providing clear policies, training, and regular communication about compliance.

Employees are informed promptly of updates to circulars and any amendments to existing policies via weekly emails from the Organization Department and publications on the corporate portal, indicating points of contact for clarification. Moreover, mandatory annual specialized training on compliance matters is provided to all employees or specific groups, followed by assessments upon completion.

Accountability mechanisms, including disciplinary actions, are established and maintained through the introduction of adequate controls for the effective implementation of a CMS which involves identifying, assessing, and managing compliance risks and offering recommendations for corrective actions.

To thoroughly understand compliance requirements and awareness of compliance risks, the following steps are followed:

1. Establishing communication channels for direct interaction between BoC employees and the Compliance Division.
2. Monthly, quarterly, and annual reports prepared by each function.
3. Conducting internal investigations by each function.
4. Maintaining departmental KRIs related to identified risks.
5. Implementing RCMS, an Operational Risk/Loss Database system, to centralize risks from various sources, incidents/losses, and KRIs, aiming for efficient risk identification, measurement, management, and monitoring.
6. Considering KPIs and OKRs during employee appraisals.

These processes are detailed further in the Internal Interested Parties of this Policy.

3.3.2. Compliance function [Clause 5.3.2]

A dedicated Compliance Division is established with clear responsibilities, authority, and resources to oversee the CMS. The Compliance Division 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. Employees and other stakeholders are expected to apply and uphold these principles and practices both in spirit and letter of the law.

The Compliance Division manages the CMS, including identifying compliance obligations, maintaining compliance risk assessment records (as per clause 4.6 of ISO 37301), aligning the system with compliance goals, and measuring compliance performance on a monthly and quarterly basis through metrics such as KPIs and KRIs to identify risks, incidents, controls effectiveness, and review findings.

Additionally, the Compliance Division evaluates the CMS's performance to determine if corrective action is required through a consistent detailing and reporting framework in the annual action plan, conducting periodic reviews of the compliance management system (as per clauses 9.2 and 9.3 of ISO 37301). To ensure a system for raising and addressing concerns, the Compliance Division has established a robust, confidential reporting process under the Whistleblowing policy, referenced in this Policy, encouraging and protecting employees who report potential violations while ensuring confidentiality.

The Compliance Division practices oversight by appropriately allocating responsibilities to meet compliance obligations throughout BoC; integrating compliance into policies, processes, and procedures; training relevant employees as needed; and establishing compliance performance indicators. As per section 6 of this Policy, the Compliance Division is responsible for drafting and enforcing the policy, preparing and updating relevant procedures/circulars as needed, organizing and conducting staff training, and performing monitoring reviews to assess effective policy implementation and recommend corrective actions when necessary.

The Compliance Division’s policies and procedures are accessible by all company employees and subsidiaries through the corporate portal and provide advice on compliance-related matters. It also receives unlimited access to senior decision-makers, early involvement in regulatory projects and new product processes at all BoC levels, and access to required personnel, documentation, and data, along with expert guidance on relevant standards, codes, and laws.

Additionally, according to Section 5 of this Policy, the Compliance Division identifies training needs and organizes regular sessions for staff and management to enhance compliance awareness. An Annual Training Plan is prepared by the Compliance Division and submitted to the Training Department for approval and implementation.

3.3.3. Management [Clause 5.3.3]

Within their scope, management is responsible for ensuring compliance by collaborating with and supporting the compliance department and encouraging employees to do likewise. All employees directly supervised by the Compliance Division adhere to BoC’s policies, procedures, and compliance requirements.

The Compliance Division identifies and communicates operational compliance risks via the RMD function and integrates compliance duties into existing business practices and procedures within their areas of responsibility through implementation in new product processes and other review processes.

Additionally, compliance training sessions raise employees' awareness about their compliance responsibilities. These training courses include a test portion at the end to ensure that employees meet training and competence standards. Furthermore, retaliation is prevented through training and by encouraging employees to voice their compliance concerns, which can be reported through various accessible channels, including a dedicated and confidential compliance line (via phone, online, or letter) under Internal Audit, anonymously or otherwise, thus protecting them from retaliation. Management also actively engages in managing and resolving compliance-related incidents and issues, receiving quarterly reports to ensure appropriate actions are recommended and executed once corrective action requirements are established.

A CMS Representative has been appointed, responsible for:
1. Developing and implementing the CMS
2. Monitoring and assessing compliance risks
3. Providing compliance training and awareness
4. Reporting compliance issues to management and relevant authorities

These duties are specifically outlined within their job description and role of the “CMS Manager” is a secondary role undertaken by the Manager Internal Governance and Operations Compliance.

3.3.4. Personnel [Clause 5.3.4]

Employees must follow BoC's policies, procedures, and respective responsibilities as described in their job description. They can also raise concerns and attend necessary training sessions.

4. Planning [Clause 6]

4.1. Actions to address risks and opportunities [Clause 6.1]

1. Strengthened Compliance Culture

One of the foremost opportunities presented by ISO 37301 is the cultivation of a robust compliance culture within BoC. ISO 37301 encourages commitment to compliance at all organizational levels, from top management to front-line employees. This standard fosters an environment where compliance is seen not merely as a regulatory requirement but as an integral part of the bank's values and operations.

By embedding compliance with the organizational culture, BoC can:

a. Reduce the incidence of non-compliance: A strong compliance culture ensures that employees are more likely to adhere to policies and procedures, reducing the risk of regulatory breaches.
b. Enhance employee morale: When employees understand and appreciate the importance of compliance, they are more engaged and motivated to uphold the bank's standards.
c. Improve reputation management: A bank known for its commitment to compliance is more likely to gain the trust and confidence of customers, investors, and regulators.

2. Operational Efficiency and Cost Savings

Implementing ISO 37301 can lead to significant improvements in operational efficiency and cost savings.

The standard provides a framework for identifying, assessing, and mitigating risks systematically, which can streamline compliance processes and reduce redundancies.

Key benefits include:

a. Optimized resource allocation: By identifying and prioritizing high-risk areas, banks can allocate resources more effectively, ensuring that compliance efforts are focused where they are needed most.
b. Reduction in compliance-related costs: A proactive approach to risk management can prevent costly regulatory fines and penalties, as well as the expenses associated with remediation efforts.
c. Enhanced process automation: ISO 37301 encourages the use of technology to automate compliance processes, reducing manual workloads and minimizing the potential for human error.

3. Enhanced Risk Management

ISO 37301 provides a structured methodology for managing compliance risks, which can significantly enhance the bank's overall risk management framework. By integrating compliance risk management with the bank's broader risk management strategies, institutions can achieve a more cohesive and comprehensive approach to risk mitigation.

Opportunities in this area include:

a. Improved risk identification and assessment: The standard emphasizes continuous monitoring and assessment of compliance risks, enabling banks to stay ahead of emerging threats and vulnerabilities.
b. Proactive risk mitigation: With a clear framework for implementing controls and measures, banks can address compliance risks before they escalate into significant issues.
c. Integration with enterprise risk management (ERM): ISO 37301 facilitates the alignment of compliance risk management with the bank's overall ERM strategies, ensuring a holistic view of risk across the organization.

4. Better Decision-Making and Strategic Planning

The data-driven approach encouraged by ISO 37301 enables better decision-making and strategic planning within the compliance division. By leveraging insights from compliance risk assessments and audits, banks can make informed decisions that align with their strategic objectives and regulatory obligations.

Benefits include:

a. Informed strategic planning: Access to comprehensive compliance data allows banks to identify trends and patterns, informing long-term strategic planning and decision-making.
b. Improved governance: ISO 37301 promotes transparency and accountability in compliance processes, strengthening the bank's governance framework.
c. Enhanced stakeholder communication: Clear and consistent compliance reporting facilitates better communication with stakeholders, including regulators, shareholders, and customers.

5. Continuous Improvement and Innovation

ISO 37301 emphasizes the importance of continuous improvement in compliance management. By fostering a culture of ongoing evaluation and enhancement, banks can innovate and adapt to changing regulatory landscapes and market conditions.

Opportunities for continuous improvement include:

a. Regular audits and reviews: Periodic audits and reviews of compliance processes ensure that the bank remains aligned with the best practices and regulatory requirements.
b. Feedback mechanisms: Encouraging feedback from employees and stakeholders can identify areas for improvement and drive innovation in compliance management.
c. Adaptability to regulatory changes: A proactive approach to compliance allows banks to quickly adapt to new regulations and guidelines, maintaining compliance and competitive advantage.

Opportunities arising from risk identification: BoC has put in place a process to identify and address risks within its Compliance Policy. For actions to mitigate these risks, the Compliance Division starts by recognizing key considerations:

a. Compliance Objectives (Clause 6.2 of ISO 37301): BoC's established compliance goals at various levels and functions are considered during risk and opportunity identification.
b. Compliance Obligations (Clause 4.5 of ISO 37301): The compliance obligations that inform the basis of the risk assessment are identified by BoC.
c. Compliance Risk Assessment (Clause 4.6 of ISO 37301): Results from ongoing compliance risk assessments are integrated into the risk and opportunity identification process.

Actions undertaken include a formal risk assessment process (RCMS) to identify risks potentially impacting compliance effectiveness, which encompasses training stakeholders or Subsidiary Compliance Liaisons on proper identification methods. Each identified risk and opportunity are assessed based on likelihood and potential impact. Action plans are then developed for each critical risk to mitigate it. To evaluate the effectiveness of these actions, KRIs/KPIs are monitored and reported monthly and quarterly. Specific mitigation actions are agreed upon between the Compliance Division and other stakeholders.

Opportunities arising from compliance reviews: Annual and ad hoc compliance assurance reviews are conducted, with findings reported quarterly to the Board. Ongoing monitoring involves root cause analysis, lessons learned, all parts of the risk management process managed by the Compliance Division. The risk identification process, compliance review methodology, and subsequent actions are documented and communicated within BoC via RCSA processes.

Opportunities arising from all the Compliance Division's activities: Every initiative undertaken by the Compliance Division presents an opportunity, which is thoroughly documented in the division's Annual Action Plan.

4.2. Compliance objectives and planning to achieve them [Clause 6.2]

At the appropriate levels and functions, BoC is responsible for establishing compliance objectives. These objectives must adhere to this Policy, be quantifiable where possible, consider relevant requirements, be monitored, be communicable, be updated as necessary, and be accessible in a

documented format. Other considerations include resource allocation, accountability, timelines for completion, and methods for assessing outcomes.

According to section 5 of this Policy, BoC's compliance objectives include at least the following:

1. Continuously identifying the legal and regulatory frameworks governing or affecting BoC operations, with cooperation from BoC's Legal Services and other units.
2. Maintaining an up-to-date register of legal and regulatory frameworks, documenting compliance obligations, and supporting them with appropriate action plans.
3. Communicating the relevant legal, regulatory, and business frameworks to business units, branches, and subsidiaries in coordination with the Compliance Division.
4. Identifying compliance obligations and recording any gaps with actions to mitigate them.
5. Measuring and assessing the impact of these obligations on BoC's processes as per risk scoring methodologies.
6. Evaluating compliance policies and procedures, addressing deficiencies, and proposing amendments if necessary.
7. Proactively identifying, assessing, and managing compliance risks associated with BoC's activities.
8. Developing practices and methodologies to measure compliance risks, fully implementing the Operational Risk Management Departments' Risk Assessment Scoring Methodology which evaluates compliance risks based on impact and likelihood.
9. Recording compliance risks upon new or amended laws and regulations, major organizational changes, strategic objectives, new initiatives, systems, products, services, market entries, acquisitions, outsourcing, significant regulatory breaches, and other events that affect the regulatory risk profile.
10. Preparing, reviewing, and revising all compliance policies regarding key issues at least annually.
11. Reviewing and assessing organizational and procedural changes to ensure proper management of identified compliance risks.
12. Using appropriate tools and mechanisms to monitor compliance activities (through KPIs and KRIs), including periodic reports by CLs and SCOs, aggregated risk measurements, exception reports, issues logs, and onsite/offsite reviews.
13. Investigating potential breaches or incidents of non-compliance, conducting requested investigations by competent authorities, and reporting to them within specified timeframes.
14. Ensuring an internal alert procedure is in place for confidentially reporting concerns, with protections accorded under Data Protection Law and whistleblower protection legislation.
15. Overseeing complaint processes to leverage information for process improvements.
16. Periodically reassessing the scope of compliance assurance reviews.
17. Integrating compliance risks arising from ESG risks into relevant processes.
18. Cooperating and sharing information with other internal control and risk management functions on compliance matters.
19. Identifying training needs, organizing regular trainings, and preparing annual Training Plans for approval and implementation.
20. Providing guidance to staff on compliance queries and issuing written instructions and circulars to update internal procedures in response to regulatory changes.
21. Collaborating with the risk management function in framework establishment and approval of new products, ensuring consideration of all material risks and compliance with current and forthcoming legal frameworks.

22. Establishing a network of CLs and evaluating them annually (excluding the Data Privacy Department) as part of their appraisal process.
23. Forming the LCO network in specific high-risk areas with direct functional reporting to the Compliance Division to enhance oversight.
24. Acting jointly with the Regulatory Affairs Department as the primary contact between competent authorities and BoC, ensuring regulatory correspondence and requests are properly managed.
25. Ensuring subsidiaries comply with local laws and regulations, with the Chief Compliance Officer informed if stricter procedures are hindered by local provisions.

4.3. Planning of changes [Clause 6.3]

CMS updates may happen as needed and annually during the policy review process. The reasons and implications for changes are explained and the CMS's effectiveness, resource availability, and any necessary reallocation of responsibilities are evaluated as appropriately.

5. Support [Clause 7]

5.1. Resources [Clause 7.1]

BoC has resources that allow the Compliance Division to obtain the financial, human, and technical support needed for the CMS. This includes external expert advice, infrastructure, training for CPDs, software applications for efficiency, and updates on compliance management and legal obligations through systems like OneSumX and World-Check.

5.2. Competence [Clause 7.2]

5.2.1. General [Clause 7.2.1]

BoC identifies key competencies affecting compliance through role-specific parameters and ensures all employees receive regular compliance training throughout the year according to the Annual Action Plan. Additionally, employee competence is assessed via KPIs in performance appraisals for Compliance Liaisons and evaluated for compliance skills. Documentation of these processes is kept in the HR system and is accessible.

Per Appendix 2, employees are regularly notified about any amendments to policies and circulars, with updates published on the corporate portal, which also lists the referred officer for clarifications. Mandatory annual compliance training is provided to all or specific groups of employees, followed by an assessment.

5.2.2. Employment process [Clause 7.2.2]

BoC ensures staff adherence to compliance requirements by setting employment conditions, providing access to policies and training, and addressing violations. During hiring, transfer, or promotion, BoC evaluates compliance risks and applies due diligence. BoC periodically reviews performance targets, bonuses, and incentives to prevent noncompliance.

According to Section 4 of this Policy, the Compliance Division investigates possible breaches and can appoint outside experts if needed, seek Internal Audit assistance, and access all records relevant to the matter.

Also, Section 5 of this Policy, outlines an internal alert procedure for employees to report concerns or potential violations confidentially, ensuring data protection and compliance with relevant laws. Employee safeguarding from retaliation is addressed in the Group Whistleblowing Policy.
Before any hiring, transfer, or promotion, BoC follows due diligence procedures and considers compliance risks. Performance targets, bonuses, and incentives are periodically reviewed to prevent noncompliance. Documentation required before hiring is specified in the HR Policy and Procedures.

5.2.3. Training [Clause 7.2.3]

From hiring onward, employees receive regular and scheduled training. This training is: a) tailored to employees' roles and the compliance risks they face; b) assessed for effectiveness; c) periodically reviewed. Training is also extended to third parties like outsourcing employees or temporary employees, based on their job's compliance risk as assessed by the Compliance Division. The Human Resource Department keeps records of all training. Additionally, all BoC Control Functions (Risk Division, Information Security, and Internal Audit Division), receive periodic training on CMS processes.

5.3. Awareness [Clause 7.3]

BoC mandates that all employees understand their role in maintaining a strong compliance culture. According to Section 4 of this Policy, every employee, regardless of position, is responsible for compliance. This includes committing to the three lines of defense and demonstrating responsible corporate behavior. Non-compliance can lead to fines, litigation, and disciplinary action.

Training emphasizes each employee's role in effective compliance, reducing legal risk and reputational damage. Employees receive specific guidance on relevant regulations, procedures, and best practices, communicated through gap analyses, presentations, newsletters, and daily updates. Clause 8.3 of ISO 37301 highlights BoC’s confidential Whistleblowing policy, encouraging employees to report potential violations via multiple secure channels, safeguarding them from retaliation.

Compliance training, both online and in-person, is approved annually by the AC through the Annual Action Plan.

5.4. Communication [Clause 7.4]

BoC determines internal and external communications regarding the CMS based on the conveyed information, appropriate timing, relevant counterparties, and communication methods. It considers all necessary communication requirements such as diversity and potential barriers to ensure interested parties are well-informed. BoC considers compliance culture and ensures information reliability and consistency during the establishment of the CMS communication process. Documented information is retained as proof of communications. These procedures allow employees to contribute to system improvements and communicate BoC's compliance culture, objectives, and responsibilities externally as determined by its’ communication processes. Additionally, according to Section 4 of this Policy, Management and Compliance Liaisons ensure that staff members understand their obligation to adhere to compliance guidelines.

BoC ensures, through effective policies, procedures, communication, training, and other monitoring measures, that management and staff:

1. Understand regulations, standards, and best practices related to their duties.
2. Recognize associated compliance risks and their responsibility to manage these risks.
3. Appreciate the importance of internal control functions in managing compliance risks and support their work.
4. Identify, assess, and manage key compliance risks with the help of compliance staff (CLs, SCOs, LCOs, & other CD staff).

5.5. Documented information [Clause 7.5]

5.5.1. General [Clause 7.5.1]

BoC's Compliance Policy encompasses various key documents such as compliance policies and procedures, system manuals, applicable regulations, review methodology, action plan, charter, internal and external training, time management tools, new product checklists, report templates, gap analysis, assurance reviews, and meeting minutes.

5.5.2. Creating and updating documented information [Clause 7.5.2]

BoC includes identification details (like the author's name, date, or reference number), format (language, software version, graphics), and medium (paper, electronic) when creating and updating documents. They also ensure approval and evaluation for suitability. BoC follows **OE001** guidelines to maintain alignment.

5.5.3. Control over data that has been documented [Clause 7.5.3]

Both the CMS and this document require controlled documented information to ensure it is accessible, appropriate, and safeguarded against misuse, loss of integrity, or confidentiality breaches. BoC manages its use, distribution, access, retrieval, storage, preservation, legibility, modification control (version control), and disposition and retention.

6. Compliance Monitoring and Evaluation [Clause 8]

6.1. Operational planning and control [Clause 8.1]

BoC plans, executes, and maintains control over necessary processes, establishes criteria, and implements them correctly. Documentation is available to ensure adherence to the plan.
The Compliance Division makes ad-hoc changes and reviews the outcomes. Third-party processes are controlled if they relate to compliance management. Appendix 4 of this Policy lists various related policies and procedures, including Compliance Division manuals and operational frameworks, accessible via the portal and website. According to Section 3, the Annual Action Plan uses a risk-based approach, covering planned compliance activities such as policy implementation, risk assessments, assurance reviews, testing, staff education, and corrective actions for identified weaknesses.

6.2. Establishing controls and procedures [Clause 8.2]

BoC has robust procedures and controls to manage its compliance risks and obligations and ensure the effective implementation and maintenance of the CMS. These controls and processes are regularly reviewed and updated to reflect changes in the external and internal context, including legal and regulatory requirements.; they are communicated to all relevant personnel via the corporate portal, ensuring that roles and responsibilities are well understood.

As per Appendix 2 of this Policy, BoC control functions—such as Internal Audit, Compliance, Risk Management, and Information Security—prepare monthly, quarterly, and annual reports for their respective Committees aiming effective monitoring and reporting. The control functions also conduct internal investigations and identify risks through departmental KRIs. BoC uses RCMS, an Operational Risk/Loss Database, to centralize risks, incidents/losses, and KRIs. This application aims for efficient risk identification, measurement, management, and monitoring. Additionally, KPIs and OKRs are considered in appraisals, ensuring operational independence through reporting lines.

The above, enable the effective monitoring and reporting mechanisms to track compliance performance and address any deviations promptly; adhering to these guidelines, BoC strengthens its compliance framework and foster a culture of integrity and accountability.

6.3. Raising Concerns [Clause 8.3]

BoC establishes, implements, and maintains a procedure to report attempted, suspected, or actual compliance violations when there are reasonable grounds for accuracy. This accessible procedure ensures confidentiality, acknowledges anonymous reports, protects against retaliation, and allows employees to seek advice. According to Section 5 of this Policy, an internal alert system enables employees to confidentially report concerns or potential policy, legal, regulatory, business, or ethical violations. The system protects personal data according to Data Protection Law and comply with Union law protection regulations, N. 6(I)/2022. Employee protection from retaliation is detailed in the Group Whistleblowing policy. BoC ensures all employees know and can use these procedures through annual training.

6.4. Investigation processes [Clause 8.4]

BoC has established procedures to assess, evaluate, investigate, and close reports of noncompliance, ensuring fair and impartial decision-making. Investigations are conducted by competent personnel independently, avoiding conflicts of interest. BoC sends periodic reports to upper management detailing investigation numbers and findings via a Quarterly Report, maintaining documentation of these investigations. Section 4 of this Policy permits the Compliance Function to investigate policy breaches, appoint outside experts, if necessary, seek Internal Audit assistance, and access all BoC records. Section 5 of this Policy states compliance risks are recorded when new laws or regulations, major organizational changes, new initiatives, processes, systems, products, services, markets, acquisitions, or outsourcing arrangements occur, along with significant regulatory breaches or KRI threshold breaches. Relevant documents include the 90.2 Risk and Control Self-Assessment (RCSA) Methodology, RCMS Manual, and ORM Risk Assessment Scoring Methodology.

7. Performance evaluation [Clause 9]

7.1. Monitoring, measurement, analysis and evaluation [Clause 9.1]

7.1.1. General [Clause 9.1.1]

Specific metrics have been set for every monitoring task to gauge control effectiveness and spot compliance gaps. Examples include:

1. Compliance Division Review methodology for compliance assessments

2. KPIs to track activities, processes, and controls
3. KRIs to identify risks related to compliance obligations
4. Audit findings
5. Timeliness of corrective actions
6. Regulatory violations
7. Risks within departments
8. Investigations by Competent Authorities

The Board and ACRC usually conduct monitoring on a monthly or quarterly basis, while the Regulatory Steering Group does so biweekly.

Critical areas monitored include:

1. Regulatory Updates
2. FATCA/CRS client counts
3. Compliance Reviews
4. Ad hoc Investigations
5. Transaction monitoring reports
6. Compliance Risks
7. Customer complaints
8. Subsidiary regulatory updates
9. Breach reports

All findings and reports are documented in the division's internal records.

7.1.2. Sources of feedback on compliance performance [Clause 9.1.2]

BoC diligently adheres to ISO 37301 compliance clause 9.1.2 by implementing a robust framework for monitoring, measurement, analysis, and evaluation. This clause mandates organizations to ensure the compliance management system (CMS) remains effective, efficient, and aligned with BoC's commitments and objectives. Some of the sources for feedback are:

1. Compliance Reviews
2. Results stemming from Root Cause Analysis (by IT and Compliance Division personnel) performed for significant issues, repeated errors, failed actions, or similar problems across units, major incidents, including significant IT system issues, incidents with damages over €50K, new legal actions with similar damages, regulatory fines, and supervisory investigations.
3. Comprehensive performance indicators and metrics.
4. Internal Audits audits.

In general, BoC engages in transparent reporting and consistent stakeholder communication, ensuring all compliance measures are well-documented and accessible, demonstrating its unwavering commitment to maintaining the highest standards of governance and regulatory adherence.

7.1.3. Development of indicators [Clause 9.1.3]

BoC assesses compliance performance using specific indicators. Per Section 5 of this Policy, the Compliance Division monitors regulatory risks through Key Risk Indicators (KRIs), which are tracked monthly. KRIs are tied to risks in RCMS and report within thresholds set by management. KRI owners must report their KRIs based on the set frequency. If thresholds exceed limits, KRI and risk owners create an action plan to reduce the risk. KRIs are included in Monthly and Quarterly reports to senior Management, Executive Committees, and Audit and Risk Committees.

7.1.4. Compliance reporting [Clause 9.1.4]

Each policy under the Compliance Policy has specific reporting criteria. Compliance reports are submitted to Senior Management, the Board, and relevant authorities, covering compliance risks, key risk indicators, regulatory impact, incidents, etc. These reports follow a set schedule of monthly and quarterly submissions to the Board and the Audit and Risk Committee. Information is shared within the organization on a need-to-know basis, respecting confidentiality. Final reports are protected from alterations by a designated department, and accuracy is verified through an accuracy form signed off by the report preparer. Section 5 of this Policy includes an exception reporting system for documenting significant deviations or issues requiring resolution.

7.1.5. Record-keeping [Clause 9.1.5]

Accurate and up-to-date records of BoC’s compliance activities are properly maintained in the corporate portal and systems to aid the monitoring and review process and show adherence to the CMS.

7.2. Internal audit [Clause 9.2]

7.2.1. General [Clause 9.2.1]

BoC conducts audits utilizing internal or external staff at scheduled times to ensure that the CMS meets its internal standards and fulfills the requirements outlined in this document. These evaluations follow the audit procedures.

7.2.2. Internal audit program [Clause 9.2.2]

BoC plans, establishes, implements, and maintains an audit program. In developing internal audit programs, BoC considers the significance of processes and past audit outcomes. BoC sets the scope, criteria, and objectives for each audit, selects auditors, and ensures impartiality and objectivity in audits, and keeps managers informed of results. Documented data supports audit program implementation and results. Section 6 of this Policy mandates periodic assessments of the Policy, internal controls, corporate governance, and risk management by internal audits, reported to AC. The Internal Audit Function also receives regular training on CMS requirements to include CMS reviews.

7.3. Management review [Clause 9.3]

7.3.1. General [Clause 9.3.1]

BoC's governing body and top management evaluate the Compliance Policy using reporting feedback. They are ultimately responsible for implementing the policy effectively and setting the tone from the top. They ensure reliable, secure internal procedures are in place for compliance and monitor its

implementation through Control Functions. They also consult Compliance on regulatory developments and issues.

7.3.2. Management review inputs [Clause 9.3.2]

The management review encompasses the following inputs. Although these are delivered to Top Management through multiple reports due to the organization's scale and the unique responsibilities of each division:

A/A	Issues	Report title	Sender	Origin
a)	The status of actions from previous reviews	• Compliance Division Quarterly Report • Compliance Division Annual Action Plan	Compliance Division	CD records
b)	Changes in relevant external and internal issues			
	• Political	• Group Annual Financial Report - Risk & Capital Management Report Section https://www.bankofcyprus.com/globalassets/group/investor-relations/annual-reports/greek/20240328-boc-group-annual-financial-report-2023.pdf). • RSG Biweekly reports	• Finance Division • RSG	• Website • RSG records
	• Economic	• Group Annual Financial Report - Risk & Capital Management Report Section https://www.bankofcyprus.com/globalassets/group/investor-relations/annual-reports/greek/20240328-boc-group-annual-financial-report-2023.pdf). • RSG Biweekly reports	• Finance Division • RSG	• Website • RSG records
	• Social	• Sustainability Report (https://www.bankofcyprus.com/en-gb/group/sustainability/disclosures/sustainability-reports/) • Corporate Governance Report https://www.bankofcyprus.com/en-gb/group/who-we-are/our-governance/governance-reports/ • RSG Biweekly reports	• ESG • Compliance Division • RSG	• Website • RSG records
	• Environmental	• Sustainability Report https://www.bankofcyprus.com/en-gb/group/sustainability/disclosures/sustainability-reports/) • RSG Biweekly reports	• ESG • RSG	• Website • RSG records
	• Technological	• Information Security Update Report (Monthly) • RSG Biweekly reports • Group Annual Financial Report - Risk & Capital Management Report Section https://www.bankofcyprus.com/globalassets/group/investor-relations/annual-	• Information Security • Finance Division • RSG	• InfoSec records • RSG records • Website

A/A	Issues	Report title	Sender	Origin
		reports/greek/20240328-boc-group-annual-financial-report-2023.pdf).		
	• Legal	• Group Annual Financial Report - Risk & Capital Management Report Section https://www.bankofcyprus.com/globalassets/group/investor-relations/annual-reports/greek/20240328-boc-group-annual-financial-report-2023.pdf). • Key Regulatory Highlights • Annual Reports to CBC (RCD, FCSCD) • RSG Biweekly reports • Compliance Division Quarterly Report	• Finance • Compliance Division • RSG	• Website • CD records • RSG records
	• Culture	• ETHOS Risk Culture Report • RSG Biweekly reports	• ETHOS Agile Team • RSG	• CD records • RSG records
c)	Changes in the needs and expectations of interested parties	• Compliance Division Quarterly Report • Compliance Division Annual Action Plan • RSG Biweekly reports • Ad-hoc reports	• Compliance Division • RSG	• CD records • RSG records
d)	Compliance performance information, including trends in: • Nonconformities, non-compliances, and corrective actions • Monitoring and measurement results • Audit results	• Compliance Division Quarterly Report • RSG Biweekly reports	• Compliance Division • RSG	• CD records • RSG records
e)	Opportunities for continual improvement			
	Adequacy of the compliance policy	• Annual Review of the Compliance Policy • Compliance Assurance Reviews	Compliance Division	CD records
	Independence of the compliance function	Annual Report to CBC (RCD)	Compliance Division	CD records

A/A	Issues	Report title	Sender	Origin
	Achievement of compliance objectives	Annual Action Plan	Compliance Division	CD records
	Adequacy of resources	Annual Action Plan	Compliance Division	CD records
	Adequacy of compliance risk assessment	Compliance Division Quarterly Report	Compliance Division	CD records
	Effectiveness of controls and performance indicators	Compliance Division Quarterly Report	Compliance Division	CD records
	Communication from concerned individuals and interested parties, feedback, and complaints	• Compliance Division Quarterly Report • Annual Report to CBC (RCD)	Compliance Division	CD records
	Investigations	• Internal Audit Reports of the Compliance Division • On-Site Inspection Reports	• Internal Audit • ECB/CBC	CD records
	Effectiveness of the reporting system	• Compliance Division Quarterly Report • External Auditors assessment reports on the ISO37301 • Internal Audit Reports of the Compliance Division	Compliance Division	CD records

7.3.3. Management review results [Clause 9.3.3]

The Compliance Division regularly reviews the CMS to evaluate its effectiveness, suitability, and adequacy, identifying areas for improvement. BoC is committed to continuous improvement through periodic assessments (quarterly or annually) to ensure regulatory compliance and mitigate risks. These reviews include findings, incidents, regulatory updates, and stakeholder feedback. Breaches are followed up with mitigation actions such as investigations, root cause analysis, and corrective measures to prevent recurrence, which are then evaluated for effectiveness. Additionally, BoC anticipates potential weaknesses when adopting new technologies to address knowledge gaps.

The outcomes of the aforementioned reviews are regularly communicated to the governing body and top management, accompanied by suitable recommendations for CMS adjustments. Feedback from these management reviews entails decisions and these are recorded in the meeting minutes.

8. Compliance Improvement [Clause 10]

8.1. Continual improvement [Clause 10.1]

To effectively implement the requirement for continual improvement, BoC adopts various strategies and best practices. These strategies include:

1. Establishing a Continuous Improvement Culture

Creating a culture that values and prioritizes continual improvement is essential for BoC for the long-term success of a compliance management system. This involves:

- Leadership Support: Securing strong support and commitment from top management to drive continual improvement initiatives.
- Employee Engagement: Encouraging employees at all levels to actively participate in identifying and implementing improvement opportunities.
- Recognition and Rewards: Recognizing and rewarding employees who contribute to continual improvement efforts.

2. Leveraging Technology and Tools

Technology can play a significant role in facilitating continual improvement. BoC leverages various tools and technologies, such as:

- Compliance Management Software: Implementing software solutions that streamline compliance processes, track performance metrics, and facilitate reporting.
- Data Analytics: Utilizing data analytics to identify trends, patterns, and areas for improvement in compliance activities.
- Automation: Automating routine compliance tasks to reduce the risk of human error and improve efficiency.

3. Benchmarking and Best Practices

Benchmarking against industry standards and best practices assists BoC to identify improvement opportunities and stay ahead of regulatory changes. This involves:

- Industry Benchmarking: Comparing compliance performance and practices against industry peers.
- Best Practice Sharing: Participating in industry forums and networks to share and learn from best practices.
- Regulatory Updates: Staying informed about regulatory changes and updates to ensure ongoing compliance.

4. Regular Monitoring and Evaluation

BoC establishes mechanisms for monitoring and evaluating its compliance management system on an ongoing basis. This includes:

- Performance Metrics: Developing and tracking key performance indicators (KPIs) related to compliance activities and outcomes.
- Internal Audits: Conducting regular internal audits to assess the effectiveness of compliance policies, procedures, and controls.
- Management Reviews: Periodically reviewing the compliance management system at the management level to ensure it aligns with organizational objectives and regulatory requirements.

5. Addressing Non-conformities and Incidents

When compliance issues or incidents arise, BoC takes prompt and effective action to address them. This involves:

- Root Cause Analysis: Identifying the underlying causes of non-conformities and incidents to prevent recurrence.
- Corrective Actions: Implementing corrective actions to address identified problems and mitigate risks.
- Reporting and Documentation: Ensuring that all non-conformities, incidents, and corrective actions are thoroughly documented and reported.

6. Stakeholder Engagement

Engaging with stakeholders, including employees, customers, regulators, and other relevant parties, is crucial for continual improvement. For BoC this involves:

- Feedback Mechanisms: Establishing channels for stakeholders to provide feedback on compliance-related matters.
- Collaboration: Working collaboratively with stakeholders to identify and address compliance challenges and opportunities.
- Transparency: Maintaining open and transparent communication with stakeholders about compliance efforts and outcomes.

7. Training and Development

Continual improvement requires ongoing training and development of employees to ensure they have the knowledge and skills necessary to uphold compliance standards. This includes:

- Regular Training Programs: Providing regular training sessions on compliance topics, including updates on regulatory changes and emerging risks.
- Skill Development: Offering opportunities for employees to develop and enhance their compliance-related skills.
- Awareness Campaigns: Conducting awareness campaigns to reinforce the importance of compliance and ethical behavior.

8.2. Nonconformity and corrective action [Clause 10.2]

Non-conformity actions are critical to maintain the integrity and effectiveness of the CMS. Below is a description of BoC non-conformity actions based on various sources of findings:

1. Findings by ISO Auditors

ISO auditors play a crucial role in identifying non-conformities within an organization's CMS. Their findings typically include gaps in compliance with the ISO37301 standards, such as lack of proper documentation, ineffective risk assessments, and insufficient training for compliance officers. Non-conformity actions in this context involve:

- Rectifying Documentation Issues: Ensuring all compliance-related documents are accurate, up-to-date, and accessible.
- Improving Risk Assessments: Implementing more robust risk assessment procedures to identify and mitigate compliance risks effectively.
- Enhancing Training Programs: Providing comprehensive training to all employees, particularly those in compliance roles, to ensure they understand their responsibilities and the importance of compliance.

2. Findings by Regulators

Findings by Regulators often focus on financial compliance and regulatory adherence. Non-conformity actions based on ECB findings might include:

- Strengthening Financial Controls: Enhancing internal controls to prevent financial misconduct and ensure regulatory compliance.
- Ensuring Regulatory Reporting: Implementing procedures to ensure timely and accurate reporting to regulatory authorities.
- Conducting Regular Audits: Performing regular financial audits to identify and address any discrepancies or areas of non-compliance.

3. Findings by Internal Audit (IA)

Internal auditors assess the effectiveness of an organization's internal controls, risk management, and governance processes. Their findings often result in the following non-conformity actions:

- Enhancing Internal Controls: Strengthening internal control mechanisms to prevent and detect non-compliance.
- Improving Governance Practices: Implementing best practices in governance to ensure accountability and transparency.
- Conducting Risk Assessments: Regularly assessing risks to identify potential areas of non-compliance and taking proactive measures to address them.

4. Complaints and Whistleblowing

Complaints and whistleblowing provide valuable insights into potential areas of non-conformity. Actions based on these findings include:

- Establishing a Whistleblower Policy: Developing and implementing a robust whistleblower policy to encourage reporting of non-compliance without fear of retaliation.
- Investigating Complaints: Thoroughly investigating all complaints and whistleblower reports to identify and address any non-conformities.
- Implementing Corrective Actions: Taking corrective actions to address the root causes of non-conformities identified through complaints and whistleblowing.

5. CMS Manager Findings

The CMS Manager is responsible for overseeing the compliance management system and identifying areas of non-conformity. Actions based on his/her findings may include:

- Reviewing Compliance Policies: Regularly reviewing and updating compliance policies to ensure they align with the latest regulations and best practices.
- Monitoring Compliance Activities: Implementing monitoring mechanisms to ensure ongoing compliance with policies and procedures.
- Providing Compliance Training: Offering targeted training sessions to address specific areas of non-conformity identified by the CMS Manager.