Banco Comercial Português, S.A.

Anti-Money Laudering and Counter Financing of Terrorism Policy

Millennium bcp

CONTENTS

I. OBJECTIVES AND SCOPE OF APPLICATION

1. The Anti-Money Laundering and Counter Financing of Terrorism Policy ("MLFT Policy", or "Policy") defines the key principles and establishes the Compliance Global Operating Model for the design and implementation of controls deemed adequate for the prevention of money laundering and financing of terrorism ("MLFT") within the scope of the Banco Comercial Português Group ("Group").
2. The Group transposes onto this policy to the following regulations and best practices:
    a. European regulation – namely through:
        i. Directive 2016/2258.
        ii. Regulation 2015/847/EC.
        iii. Regulation 2018/1672.
        iv. 4th Directive on MLFT (EU Directive 2015/849).
        v. 5th Directive on MLFT (EU Directive 2018/843).
        vi. 6th Directive on MLFT (EU Directive 2018/1673).
    b. Guidelines – including but not limited to the:
        i. EBA Guidelines on MLFT risk factors and due diligence measures (EBA/GL/2021/02).
        ii. EBA Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the MLFT Compliance Officer under Article 8 of Chapter VI of Directive (EU) 2015/849 (EBA/GL/2022/05).
        iii. EBA Guidelines on policies and controls for the effective management of MLFT risks when providing access to financial services (EBA/GL/2023/04).
    c. Recommendations issued by the Financial Action Task Force ("FATF").
3. The MLFT Policy is a key component of the Group control framework, as part of the ethical standards and values for the development of its activity, being considered a fundamental element for the preservation of sustainability, solidity, integrity, reputation and trust of the stakeholders of each Group Entity ("GE").
4. This Policy is directly applicable to the members of the management and supervision bodies, all employees of the Group, trainees and to agents or employees of the outsourcing service providers.
5. All GE must define procedures for the analysis and monitoring of MLFT risks, whether for business relationships or occasional transactions.
6. This Policy sets out minimum standard principles and controls for MLFT prevention to ensure a coherent common ground across the Group. All GE are, however, incentivized to adopt additional controls and to share best practices with BCP and other GE.
7. The provisions defined in this Policy do not supersede or replace the legal and regulatory provisions and the principles established by the supervisory and other legal authorities in the jurisdiction of each GE.
8. The BCP Compliance Office must be informed of all restrictions or limitations identified by each GE that prevent the application of the principles defined in this Policy.

II. APPROVAL & REVISION PROCESS

This Policy is approved by Banco Comercial Português, S.A. Board of Directors, with the opinion of its Audit Committee, by proposal of its Executive Committee.

The BCP Compliance Office must monitor the application and timeliness of this policy, promoting its review, annually or whenever deemed necessary or relevant.

III. GENERAL DEFINITIONS

- Activity with virtual assets – any of the following economic activities, carried out in the name or on behalf of a customer: i) exchange services between virtual assets and fiat currencies; ii) exchange services between one or more virtual assets; iii) services whereby a virtual asset is moved from one address or wallet to another (virtual asset transfer); iv) safeguarding or administration services for virtual assets or tools that allow the control, hold, storage or transfer of such assets, including private cryptographic keys.
- AML Officer – person responsible, within the Compliance Office of each GE, for compliance control of the normative framework on MLFT matters, as well as for the policies and procedures that ensure the adequacy of this control.
- Business Relationship – any relationship established for business, professional or commercial purpose, which, at the time of establishment, is or is expected to be long-lasting, stable and maintained over time, regardless of the number of individual transactions carried out.
- CDD – Customer Due Diligence - is the standard diligence procedure to understand and evaluate the risks posed by a customer or her/his transactions.
- CRR – Customer Risk Rating - is a discrete metric that assigns a MLFT risk score to a customer or its related parties (e.g., ultimate beneficial owners, legal representatives).
- Customer Screening - the process of verifying the identity of a customer and assessing the potential risk they pose to a financial institution or organization by checking their name and other identifying information against various watchlists, sanctions and PEP lists, and other databases to ensure compliance with relevant legislation.
- EDD – Enhanced Due Diligence – is an in-depth diligence on a customer (or related parties), usually adopted when a high-risk factor is identified.
- Electronic money – the monetary value stored electronically, including magnetically, represented by a credit on the issuer and issued upon receipt of bank notes, coins and book currency, to carry out payment transactions and which is accepted by a natural or legal person other than the issuer of electronic money.
- Entity – any natural or legal person, as well as any arrangement without legal personality, including customers and non-customers.
- Fiat money – banknotes and coins designated as being legal tender, scriptural money and electronic money.
- Financing of Terrorism - a collective term for various acts the ultimate purpose of which is to provide the material resources to make terrorist activities possible. Differently from money laundering prevention, controls are not as much enforced towards the provenance of money, but more to its destination and intended uses.
- Group – it comprises BCP and all legal persons in which BCP, directly or indirectly, owns more than 50% of the capital or voting rights, or has the capacity to designate more than half of the managing or supervisory bodies or are included in the Group's consolidation perimeter.
- Group Entity ("GE") – includes all financial institutions, branches and subsidiary companies that are part of the Group in Portugal and other countries.
- High-risk third countries – non-EU countries or jurisdictions identified by the European Commission as having national MLFT regimes that present strategic deficiencies that pose a significant threat to the EU financial system.
- High-risk jurisdictions - means countries that, based on an assessment of the risk factors set out in Appendix I of this policy, present a higher MLFT risk. This includes 'high-risk third countries.

- Jumbo account – an account held by the financial Entity itself and which it uses on behalf of its customers or counterparties.
- KYC – Know Your Customer - is a structured repository of information about the customer or Entity comprised of all elements necessary to comply with the Duty of Identification and Diligence both in the beginning of the contractual relationship as well as during its lifetime whenever the GE must gather further information or review it (periodically or exceptionally).
- MLFT – Money Laundering and Financing of Terrorism.
- Money Laundering – process by which the perpetrators of criminal activities[1] cover up, or try to cover up, the origin of the goods and income (advantages) obtained illegally, transforming the inflows resulting from these activities into legally reusable capital. By disguising the origin or the true owner of the funds. Participation, association, attempt, complicity, as well as the fact of facilitating the execution or advising the practice of criminal activities, jointly imply the crime of money laundering.
- Occasional transactions – means a transaction that is not carried out as part of an already established business relationship (e.g., sale of real estate portfolio, exchange and cash exchange operations).
- PEP – Politically Exposed Person - an individual who is or has been entrusted with a prominent public function.
- Person known as close associate – i) natural person who owns a legal person or arrangement without legal personality; ii) natural person owning the share capital or voting rights of a legal person, or the assets of an arrangement without legal personality, with the customer as the effective beneficiary; iii) natural person with corporate, commercial or professional relationships.
- Pooled account – Pooled account' means a bank account opened by a customer for holding their clients' money. The clients' money will be commingled, but clients will not be able directly to instruct the bank to carry out transactions.
- Private banking – provision of banking and other financial services to high-net-worth entities, as well as to their close family members[2] and entities controlled by them, including the vehicles they use to own or manage assets.
- Remote Communication – any means of communication - telephone, electronic, telematic or otherwise - that allow the establishment of business relationships, the execution of occasional transactions or the carrying out of operations in general, without the physical or simultaneous presence of the financial Entity and its customer, that is, in non-face-to-face situations.
- Risk factors – are the variables that, alone or together, can increase or decrease the MLFT risk represented by a business relationship or occasional transaction.
- Restrictive Measure - essential tool namely in the EU's common foreign and security policy ("CFSP"), through which different authorities can intervene where necessary to prevent conflict or respond to emerging or current crises.

IV. GOVERNANCE STRUCTURES FOR MLFT PREVENTION

1. The MLFT prevention requires the definition of a specific Governance Model to effectively identify, monitor and control the MLFT risks of the Group's activities.
2. The Group establishes a Governance Model for MLFT prevention that comprises two levels:
    a. Group level governance:

[1] For example, corruption; trafficking in drugs, weapons, human organs and tissues; market abuse; fraud; tax crimes.

[2] Close family members refer to: i) the spouse, or a person considered to be equivalent to a spouse; ii) the children and their spouses, or persons considered to be equivalent to a spouse; iii) the parents.

i. Governance structures;

ii. Individual roles;

b. Entity level governance.

IV.1 GROUP LEVEL GOVERNANCE | GOVERNANCE STRUCTURES

3. At a Group level, MLFT prevention is ensured by the fulfilment of responsibilities and coordination amongst the following bodies and entities at BCP:

    a. Board of Directors (BoD);

    b. Executive Committee (ExCo);

    c. Audit Committee (AudCo);

    d. Compliance and Operational Risk Commission (CORC);

IV.1.1 BCP Board of Directors

4. The BCP BoD is responsible for defining the Group's strategy, for the organizational and corporate Governance Model, for the control functions, particularly the Compliance function, and for other elements able of promoting a robust control environment, such as ethical and conduct codes.

5. The BCP BoD ensures consistency in the Group's internal control system.

6. The BCP BoD approves the BCP Compliance Office activity plan and monitors its progress and execution through periodic reports.

7. The BCP BoD approves the regulatory reports on MLFT (on an individual or consolidated basis).

8. The BCP BoD ensures the implementation of the necessary measures to correct deficiencies detected in MLFT issues.

9. The BCP BoD ensures, in compliance with applicable legislation, the existence of reporting lines between the GE Compliance Office and BCP Compliance Office.

10. The BCP BoD delegates in the BCP AudCo the supervision of the Group's internal control system, which includes the activity of the Group's control functions, and the Compliance function in particular.

11. The BCP BoD appoints an executive member to coordinate the Compliance function, and the prevention of MLFT.

12. The BCP BoD monitors the MLFT risks to which each GE is exposed, ensuring that said GE carry out their MLFT risk assessments at the business level in a coordinated manner and based on a common methodology, reflecting, however, on their specificities and considering the risk taxonomy identified by regulators and applicable regulation.

13. The BCP BoD ensures that the GE or branch implements corrective measures in a timely and effective manner, whenever notified by the members of the GE BoD or by the Chief Risk Officer or directly by the BCP Compliance Officer, of supervisory activities carried out on GE by a competent authority, or the deficiencies identified therein.

IV.1.2 BCP ExCo

14. The ExCo ensures the implementation of the internal control system, either individually or as a group, and therefore its Compliance function.

15. The ExCo ensures that sufficient and adequate human and material resources are available to carry the responsibilities intrinsic to the Compliance function.

16. The ExCo ensures the implementation of policies (whose revision periodicity must not exceed 12 months), processes and controls related with MLFT prevention, according with the operating model defined by this Policy.

17. The ExCo proposes to the BCP BoD the approval of regulatory reports on MLFT issues.

18. The ExCo reviews the BCP Compliance Office annual activity plan and monitors its progress and execution level.

19. The ExCo monitors the BCP Compliance Office implementation and remediation of any deficiency that has been identified on MLFT issues from supervisors or from the audit function (internal or external).

20. The ExCo presents to the BCP AudCo any proposal for subcontracting tasks associated with the Compliance function.

21. The ExCo transmits to the BoD, directly or through the AudCo, in the shortest possible time, all relevant information arising from events, whether recorded or foreseeable, that may compromise the fulfilment of Compliance-related regulations or Group policies.

IV.1.3 BCP AudCo

22. AudCo issues, to the BoD, an opinion on MLFT matters, including its assessment on the oversight that is carried out over BCP GE.

23. AudCo is responsible for the oversight of the activity of the Group as whole, periodically monitoring, among others, the following aspects:

    c. Key interactions with supervisors.

    d. Key projects and major control developments.

    e. Implementation of findings and recommendations, issued by internal or external entities (e.g., Internal Audit, Statutory Auditor, Supervisors).

24. AudCo analyses reports on MLFT matters, namely the consolidated regulatory reports that are submitted to MLFT supervisors.

25. AudCo reviews the periodic activity reports of the Compliance function, which include a specific section on the prevention of MLFT.

26. AudCo issues an opinion to the BoD on the adequacy of the BCP Compliance Office annual activity plan, as well as on its progress and execution level.

IV.1.4 Compliance and Operational Risks Commission ("CORC")

27. This Commission has the participation of ExCo Members, including the CRO, and conducts a monthly monitoring activity for each GE:

    f. Key Compliance indicators.

    g. Main interactions with local supervisors.

    h. Relevant on-going projects and control enhancements.

28. CORC analyses MLFT key issues and controls and monitors the evolution and the resolution of the identified internal control deficiencies, namely those related with MLFT.

IV.2 GROUP LEVEL GOVERNANCE | INDIVIDUAL ROLES

29. The Group level governance on MLFT also relies on the intervention of the following specific individual roles at BCP:

    a. Chief Risk Officer ("CRO").

    b. Compliance Officer.

    c. AML Officer.

    d. GE Liaison.

IV.2.1 Chief Risk Officer ("CRO")

30. The BCP BoD delegates on its CRO the responsibility of coordinating the Compliance function, and the prevention of MLFT in particular, across the Group.

31. The CRO participates in GE compliance-related Board Committees, as a non-executive Board Member, where it is discussed relevant information for the management of MLFT Risk (e.g., MLFT Commission of each GE – further detailed on section IV.3).

32. The CRO promotes the alignment of the Compliance function across the Group with the support of the GE ExCo and respective Compliance Officers.

33. The CRO promotes the above-mentioned alignment through the following initiatives:

    a. Oversees the activities developed by each GE Compliance Office and promotes a strong Internal Control and Compliance culture.

    b. Sponsors adequate Compliance tools and controls to ensure a pre-emptive identification, assessment and management of key compliance risks across the Group.

    c. Promotes the alignment of objectives, definitions, processes and risk metrics across the Group.

    d. Ensures the adoption of the Group's policies, principles and procedures set out in this Policy.

    e. Issues an opinion on the appointment of the Compliance Officers of each GE.

    f. Ensures that there is a periodical reporting to the BoD on the activities carried out by the BCP Compliance Officer and that the BoD is provided with sufficiently comprehensive and timely information and data on MLFT risks and MLFT compliance.

    g. Ensures the supervision of BCP Compliance Office and Compliance Officer, periodically reporting to the BoD the activities carried out by them.

    h. Ensures that the Group defines and ensures the effective application of control policies and procedures that prove adequate to address MLFT risks and requirements.

    i. Ensures that the Group identifies, assesses and mitigates specific MLFT risks that exist in the context of their specific operational reality.

    j. Sponsors corrective procedures to the BoD in order to address deficiencies detected in terms of preventing MLFT, ensuring the speedy implementations and sufficiency of the approved measures for this purpose, and continuously inform the BoD of their respective execution status.

    k. Informs the BoD of relevant interactions with Banco de Portugal, the Financial Information Unit ("UIF"), and other authorities responsible for MLFT.

    l. Critically reviews the decisions not to exercise the duty of communication, reporting monthly the results of this review to the BoD.

IV.2.2 BCP Compliance Officer

34. The BCP Compliance Officer is responsible for promoting the adoption of internal and external regulations that frame the Group's activity and for ensuring an adequate Compliance culture.

35. The BCP Compliance Officer is responsible for designing and implementing an annual activity plan that identifies all relevant risk factors, especially those concerning MLFT, and that promotes the adequacy of controls for the prevention and mitigation of risk.

36. The BCP Compliance Officer sponsors and promotes a swift and effective implementation and remediation of any deficiency that has been identified on MLFT issues from supervisors or from the audit function (internal or external).

37. The BCP Compliance Officer promotes a coherent deployment of controls at Group level, supporting GE Compliance teams in the standardization and adoption of best practices in terms of procedures, systems and processes.

38. The BCP Compliance Officer regularly monitors the activity of the Compliance function of every GE, and issues an opinion, whenever required, on the process of selection and appointment of new GE Compliance Officers.

39. The BCP Compliance Officer must determine indicators of assessment to check the effectiveness of training provided.

40. The BCP Compliance Officer issues an annual activity report and submit it to the BoD. Additionally, this report must contain at least the following MLFT elements made available by GE Compliance Officers:

    a. Consolidated statistics at the Group level, namely in terms of risk exposure and suspicious activity.
    b. Monitoring of inherent risks that have occurred in an GE or branch and an analysis of the impact of residual risks.
    c. The results of oversight reviews and assessments, the findings of internal or external audits of GE or branches, including serious deficiencies identified in said institutions MLFT policies and procedures, actions or recommendations for corrective measures.
    d. Information on management and supervision of GE and branches with special emphasis on those located in high-risk countries if applicable.

IV.2.3 BCP AML Officer

41. A BCP AML Officer can be appointed by the BCP ExCo under the management hierarchy of the BCP Compliance Officer.

42. The BCP AML Officer is responsible for ensuring compliance with procedures and the proper evaluation of MLFT risks, including the execution of due diligence activities that result from monitoring systems, screening platforms or any other MLFT controls.

43. The BCP Compliance Officer, or the AML Officer in his/her stead, whenever necessary, reviews, decides, and signs off on suspicious transactions and customers to ensure they are reported to the competent authorities, including those in the scope of restrictive measures imposed by the European Union or Security Council of the United Nations, or other credible sources (e.g., Bank of England, OFAC).

44. The BCP AML Officer is responsible for liaising with competent authorities for any ongoing investigations or judicial processes that are deem required and that imply the cooperation of BCP.

45. The BCP AML Officer designs and enforces all necessary activities and procedures to implement and remediate any deficiency that has been identified on MLFT issues from supervisors or from the audit function (internal or external).

IV.2.4 BCP GE Liaison

46. The BCP GE Liaison, which can be appointed by BCP Compliance Officer, establishes an operational and communication link between each GE and the BCP Compliance Office.

47. The BCP GE Liaison is responsible for engaging with GE to support the BCP Compliance Officer in the identification of growing concerns or any relevant trend or risk factor.

48. The BCP GE Liaison facilitates the exchange of relevant information with each GE, especially on MLFT issues (e.g., best practices) including the production of benchmarking analyses as well as critical and effectiveness testing analyses.

49. The BCP GE Liaison collaborates with the Compliance Officer and the AML Officer (if applicable) in the analysis, review and monitoring of each GE activity plan and ongoing initiatives.

50. The GE must send the Annual Action Plan of its Compliance Office to the BCP Compliance Officer, prior to its approval, in order to promote best practices and controls coherence.

IV.3 LOCAL GOVERNANCE (AT GE LEVEL)

51. Each GE must design a local MLFT Governance Model for MLFT prevention, identifying key governing bodies, its organizational structure, roles and responsibilities.

52. The local Governance Model for MLFT issues, must include at least the following structures:
    a. ExCo or its equivalent management structure.
    b. Audit Committee (or Supervisory Board, whenever applicable).
    c. Commission on MLFT.
    d. Compliance Control Conference.
    e. Compliance Office.

IV.3.1 GE ExCo

53. The GE ExCo shall implement an appropriate and effective organizational operational structure necessary to carry out the MLFT strategy adopted by the BoD, paying special attention to the sufficiency and adequacy of the human and technical resources assigned to the role of Compliance Officer, including the need for a dedicated MLFT unit to assist the Compliance Officer.
54. The GE ExCo is responsible for proposing and implementing the GE strategy, policies, procedures and organizational model, to ensure that the Compliance function is effective.
55. The GE Exco must ensure adequate, timely and sufficient detailed information on MLFT is communicated to the competent authority.
56. The GE ExCo is responsible to liaise with BCP ExCo to ensure the full alignment of its Compliance function (and MLFT prevention in particular) with the Group's policies.
57. The GE ExCo ensures that sufficient and adequate human and material resources are available to perform the functions and tasks inherent to the Compliance function, and MLFT in particular, promoting its consistency with the applicable policies.
58. Each GE ExCo should be responsible for approving the GE overall MLFT strategy and supervise its implementation.
59. The GE ExCo must collectively possess adequate knowledge, skills, and experience to be able to understand the risks of MLFT related to the activities and business model of GE, including knowledge of the national legal and regulatory framework on MLFT prevention.
60. The GE ExCo must be informed of the results of the MLFT risk assessment at the business level.
61. The GE ExCo must oversee and monitor the extent to which the MLFT policies and procedures are adequate and effective considering the MLFT risks to which the GE is exposed and take the appropriate initiatives to ensure that corrective measures are taken, if necessary.
62. The GE ExCo must, at least annually, review the Compliance Officer's activity report and obtain more frequent interim updates on activities that expose the GE to higher MLFT risks.

IV.3.2 GE AudCo (or Supervisory Board whenever applicable)

63. The GE AudCo in addition to other responsibilities assigned by law, has the responsibility of overseeing the efficiency of the risk management system regarding MLFT.
64. The GE AudCo assesses the main risk factors and threats that need special attention and monitoring.
65. The GE AudCo will, at least annually, assess the effective functioning of the MLFT compliance function, namely considering the conclusions of any internal and/or external MLFT related audit that have been carried out, including concerning the adequacy of human and technical resources attributed to the Compliance Officer.
66. The GE AudCo assesses the annual report produced by the GE Compliance Office in matters of MLFT and more frequent interim updates on activities that expose the GE to higher MLFT risks.
67. The GE AudCo monitors the implementation of MLFT related recommendations, findings and interactions with local supervisors.

68. The GE AudCo guarantees the existence of a whistleblowing mechanism and an adequate process, with the highest form of anonymity legally available, to ensure the management and analysis of all situations reported under that channel.

69. The GE AudCo must be informed of the results of the MLFT risk assessment at the business level.

70. The GE AudCo must oversee and monitor the extent to which the MLFT policies and procedures are adequate and effective considering the MLFT risks to which the GE is exposed and take the appropriate initiatives to ensure that corrective measures are taken, if necessary.

71. The GE AudCo must oversee and monitor the implementation of the internal governance and internal control framework to ensure compliance with applicable requirements in the context of the MLFT prevention.

72. The GE AudCo must ensure that the ExCo or GE CRO:

    a. Has the knowledge, skills and experience necessary to identify, assesses and manage the MLFT risks to which the GE is exposed as well to apply MLFT policies, controls and procedures.

    b. Has a good understanding of the GE business model and the sector in which it operates as well as the extent to which this business model exposed the GE to MLFT risks.

    c. Is informed in a timely manner of decisions that may affect the risks to which the GE is exposed.

73. The GE AudCo have access and take into account data and information of sufficient detail and quality to be able to effectively perform their MLFT duties, including direct and timely access to the Compliance Officer activity report on MLFT, the report of the internal audit functions, the conclusions and observations of the external auditors as well as the conclusions of competent authorities, the relevant communications with the Financial Investigation Unit ("FIU") and the supervisory measures or sanctions imposed.

IV.3.3 GE Commission on MLFT

74. The GE Commission on MLFT prevention has the following main competences:

    a. Ensure the adoption of the principles and controls set out on this Policy.

    b. Analysis and monitoring of key MLFT controls (such as the CRR model, due-diligence criteria and procedures, onboarding screening process, transactions screening and monitoring, customer information update program).

    c. Analysis and treatment of relevant information relating to customers, accounts and specific operations.

    d. Monitor the implementation and remediation of any deficiency that has been identified on MLFT issues from supervisors or from the audit function (internal or external).

    e. Assessment of the global MLFT risk.

75. For the fulfilment of these objectives the Commission develops the following initiatives:

    a. Analyses on performance and risk indicators and other relevant information compiled by the GE Compliance Office.

    b. Deep-dive investigations on concrete situations of increased or emerging risks.

    c. Specific projects to enhance controls that are deemed necessary by the Commission.

76. The Commission on MLFT is expected to deliver:

    a. An assessment of all automated controls and its parameters, including the CRR model, the monitoring tool and the screening engines.

    b. An evaluation and interpretation of major MLFT risk factors, trends and suspicions, that have been detected by Compliance controls.

c. An analysis and relevant takeaways from quality control reports issued by the Compliance Office staff, or by any other external unit.

d. An assessment on the global MLFT risk of its activity.

77. The Commission should meet with a monthly frequency.

78. The Commission should have as its members (or permanent invitees) at least:

a. BCP CRO responsible for the MLFT prevention.

b. GE Executive Board Member responsible for the MLFT prevention.

c. BCP Compliance Officer and BCP GE Liaison.

d. GE Compliance Officer.

IV.3.4 Compliance Control Conference

79. The Compliance Control Conference is a deliberative structure, composed of Compliance Office managers or senior team leaders, as well as other members of the GE deemed adequate (e.g., audit members).

80. The Conference meets with a pre-defined frequency, adjusted to the operational dimension and complexity[3] of respective the GE.

81. The Compliance Control Conference has the following responsibilities:

a. Decide on the report of suspicious transactions and customers or operations subject to restrictive measures to the competent authorities.

b. Analyse emerging trends and risks and propose the enhancement or implementation of new controls.

IV.3.5 Compliance Office

82. The Compliance Office ensures the adequacy and enforcement of the Compliance function across all lines of defence of each GE and is headed by a Compliance Officer.

83. Besides the Compliance Officer there may also be an AML Officer, who is responsible for enforcing internal MLFT regulations and policies.

84. The Compliance Office may also appoint a person responsible for the operational and reporting liaison with BCP.

85. Each GE Compliance Office is responsible for:

a. Promoting the specialization of its resources, ensuring that topic expertise and knowledge is developed for compliance skills, and MLFT in particular, and transversal capabilities (e.g., systems, monitoring, reporting).

b. Identifying requirements regarding the size and experience of the team.

c. Promoting a compliance culture across the GE.

d. Supporting the processes carried out by the first line of defense in terms of MLFT prevention.

e. Monitoring and deciding the closure of authorities' findings and recommendations.

86. The GE Compliance Office have the following main responsibilities:

a. Streamline the adoption of internal and external legislation and ensure compliance with them.

b. Analyse and assess the risk factors associated with its activity and promote the appropriate controls for their mitigation.

[3] In Portugal, BCP Compliance Control Conference holds weekly meetings.

c. Reporting to the management body of all non-compliant situations detected that may cause the institution to undertake an administrative offence or any other illicit action and incur in significant asset or reputation losses.

d. Promote the employee training Policy, namely by providing training sessions on compliance and maintain a high level of knowledge on MLFT related matters.

e. Ensure compliance with entities ethical values and the existence of a culture of internal control, in order to contribute to the mitigation of risk, especially the reputational and legal ones.

f. Articulates and interacts with other control functions to reinforce MLFT controls.

g. Refers specific transactions or clients to BCP Compliance Office for analysis, as established and applicable in each geography.

V. MLFT RISKS

1. The identification, management and control of MLFT follows a Risk-Based Approach ("RBA").
2. Under this approach each GE must ensure that the MLFT prevention policies, procedures and controls are based on and reflect a systematic and documented risk assessment for the MLFT risk factors that affect its activity.
3. GE should differentiate between the risks associated with a particular category of customers and the risks associated with individual customers that belong to this category, and that the implementation of these policies, procedures and controls does not result in the blanket refusal or termination of business relationships with entire categories of customers that they have assessed as possessing a higher MLFT risk.
4. GE ensure that all lines of defence understand the MLFT risk factors inherent to its activity.
5. GE ensure the nature of the credit or financial institution's business and the MLFT risks associated therewith, taking into account its geographical exposure, customer base, distribution channels and products and services offering.

V.1 SCOPE OF MLFT RISKS

6. The scope and variety of MLFT risk factors depend on the complexity, size and business characteristics of the activity carried out by each GE.
7. Each GE must assess the scope of MLFT risks under 3 different perspectives:
    a. GE global activity.
    b. Individual business relationships.
    c. Occasional transactions (if existent).

GE Activity Risk

8. Each GE must have a vision of the aggregate MLFT risk according to the geography it operates in, its business structure and target customer segments and the transaction or delivery channels it uses to service its customers.
9. For the particular identification of high MLFT risks, all risk factors mentioned by GE local legislation must be considered. Additionally, each GE must evaluate the existence and impact of risk factors provided in the Appendix I of this Policy.

10. For the assessment of the activity risk (as a whole), GE may take into account national and international reports, deemed of good repute, as well as any external regulatory or supervisory assessment on its business model, customers segments or jurisdictions.

11. Each GE must update or review its risk assessment periodically, and at any moment when:

    a. There is a material change in the activity profile (e.g., new business segment).

    b. A market event occurs that may impact the MLFT risk profile (e.g., a MLFT event that affects the reputation of the jurisdiction).

    c. A new systemic threat is detected (e.g., recurrent suspicious reports issued to authorities about a particular MLFT risk factor).

12. Each GE must calibrate its controls according to the risk of specific business activities, segments and operations.

Individual Business Relationship Risk

13. Each GE must identify, assess, and manage the MLFT risk associated with business relationships adopting an RBA methodology.

14. When establishing these business relationships, the GE must obtain information on their purpose and nature, as well as gather sufficiently detailed information about the characterization of the activity (specifically, information on its nature, the level of income, or the volume of business generated, as well as about the countries or geographical areas associated with it), the source of funds and wealth for a specific segment of clients that enables the GE to check if the transactions carried out under said relationship are consistent with the knowledge they have of the client. Additionally, considering any detected shortcomings, the GE must also obtain this information, when missing, for already established business relationships.

15. Each individual business relationship must be assigned with an overall customer risk rating ("CRR") that is the result of the assessment of multiple risk factors.

16. The isolated presence of specific risk factors and types referred to in Annex I of this Policy does not necessarily determine the automatic attribution of a high CRR to the business relationship.

17. The existence of high MLFT risks in the establishment of a new business relationship or the maintenance of a business relationship with high-risk customers, should entail a prior analysis and confirmation by the GE Compliance Office, per the Bank's internal risk based internal MLFT policies.

18. Whenever an established business relationship presents a higher MLFT risk, the GE must adjust the controls applicable to that business relationship (more detail on Chapter VII).

19. Each GE provides a communication channel for any employee to notify the GE Compliance Office of situations or operations that they consider suspicious and that may impact the risk assessment for a business relationship.

20. Each GE should ensure that the consideration of risk factors does not lead to a situation where it is impossible for any business relationship to be classified as high-risk.

21. Applying a RBA does not require any GE to refuse or terminate business relationships with entire categories of customers that pose a higher MLFT risk.

22. GE should set out in their policies and procedures the criteria they will use to determine on which grounds they will decide that a business relationship may be rejected or terminated or that a transaction may be denied. These options should at least include adjusting the level and intensity of monitoring and, where this is permitted under national law.

23. Each GE must ensure that all of its automated controls, such as CRR assignment, monitoring, or transaction screening, incorporate the MLFT risk factors of its business.

24. All individual business risk assessments must be registered and archived, in order to ensure future auditability and consultation.

Occasional Transactions Risk (if existent)

25. If existent, the GE must understand and identify MLFT risks of occasional transactions.
26. In an occasional transaction, the GE should consider the same risk factors indicated for business relationships, namely identifying UBOs and representatives, adapting the nature and extent of the information available on such transactions.
27. All occasional transactions risk assessments must be registered and archived, in order to ensure future auditability and consultation.

V.2 RISK FACTORS IDENTIFICATION AND ASSESSMENT

28. Each GE must identify the risk factors (taking into account the non-exhaustive list of factors presented in Appendix I) relating to:
    a. Its customers (individual and business), including the customer ownership structure (applicable only to business customers) and its UBOs.
    b. The products and services that are offered.
    c. The distribution channels that are used between the GE and its customers.
    d. The jurisdictions that are involved in customers activities and transactions.
    e. The correspondent banking relationships that are maintained.
    f. The type of activity performed.
29. Each GE should take a holistic view of the identified MLFT risk factors that, together and in a cumulative way, will determine the level of MLFT risk associated with an individual business relationship or an occasional transaction.
30. Each GE should note that, unless legislation or supervisory measures provides otherwise, the presence or absence of isolated risk factors does not necessarily imply a higher or lower risk category.
31. Each GE must be able to enforce the manual aggravation of the CRR level when in the knowledge of a particular risk situation that is not automatically factored in the CRR model. Manual adjustments to CRR levels can only be applied to increase the risk level.
32. When assessing MLFT risk, the GE may decide to weigh factors differently depending on their relative importance.
33. When weighting risk factors, the GE should ensure that:
    a. Weighting is not unduly influenced by just one factor.
    b. Economic or profit considerations must not influence the CRR.
    c. Weighting does not lead to a situation where it is impossible for any business relationship to be classified as high-risk.
    d. It is possible to make manual adjustments to the risk score when necessary.
    e. Changes in weighting are properly tested, approved and documented.
34. Some factors may contribute to reducing risk (e.g., knowledge of a long-standing customer).

35. Each GE must document how the weighting system works and how it weighs risk factors.
36. The weighting system must be auditable when changes are promoted.
37. The combined weighting of the various risk factors must lead to a discrete MLFT risk level.
38. While MLFT risk levels may vary with the nature and size of GE business, as well as the types of risk each GE is exposed to, there must be a minimum of 3 levels: Low, Medium and High.
39. The procedures and controls of each GE must be designed and formalized according to the risk levels defined in the previous point, and in accordance with an RBA methodology.

VI. COMPONENTS OF COMPLIANCE GLOBAL OPERATING MODEL

1. GE must implement and develop an operating model to manage MLFT risks following an RBA.
2. The operating model must include, at least, the description of key:
    a. Control duties;
    b. Systems and tools;
    c. Policies.

VI. 1 MLFT CONTROL DUTIES

3. Each GE must define and document the duties that are enforced in order to identify, manage and control the key MLFT risk factors that affect its activity and business relationships.
4. GE must include, at least, the following duties:
    a. **Duty of Control** - GE are required to effectively establish and maintain policies, procedures, and controls to manage the risks of MLFT they face, ensure compliance with legal and regulatory standards for MLFT prevention and adhere to international and EU restrictive measures on freezing assets related to terrorism and weapons proliferation. These measures should be proportional to the complexity, nature of activities and consistent across the Group, ensuring the sharing of relevant information to combat MLFT.
    b. **Duty of Identification and Diligence** - GE must collect identification elements and additional data that allow them to unequivocally identify its customers, representatives, and UBO, and to understand their motivations, intentions and financial behaviour. The GE must perform this duty whenever they establish new business relationships, conduct occasional transactions or perform financial transactions, as well as during periodic reviews of the relationship. New elements or relevant insights must be archived and updated in a KYC (and may imply a CRR revision), whose update frequency must be directly correlated with the clients risk.
    c. **Duty of Examination** – GE must ensure this duty performance whenever a suspicious conduct, activities or operations are detected, which may be in any way related with funds and other assets that come from criminal activities or destined towards criminal activities, namely MLFT.
    d. **Duty of Abstention** – GE must have in place procedures and mechanisms that enables them to abstain from carrying out any current or future operation or set of operations that it is aware of, or suspects may be linked to funds or other assets derived from or related to criminal activities or the financing of terrorism. This duty extends to the clients' UBO, whereby the Entity must have mechanisms in place to identify common UBOs across clients.

e. **Duty of Refusal** – GE must not engage in new business relationships or transactions if they fail to acquire necessary identifying details and proofs for clients and UBO, or lack of information about the business relationship's nature and purpose as mandated by specific legislation.

f. **Duty of Report** - GE must communicate to the competent authorities specified by local legislation the execution, or its attempt, of transactions that are suspicious of being involved or derived from criminal activities, namely MLFT. These communications must be made regardless of whether the operations are in progress or have already taken place. Additionally, GE must observe that the execution of the Duty of Abstention or Refusal does not derogate the need for the Duty of Report.

g. **Duty of Non-Disclosure** - GE are responsible for not sharing, with customers or third parties, any information related with the reporting of suspicious activities, internal analysis or ongoing investigations from the competent authorities. GE must guarantee, in particular, the adequate confidentiality and access control to information pertaining all examination duties carried out in the analysis of MLFT suspicions, unless otherwise required by the competent authority or court order.

h. **Duty of Record Keeping** – GE must keep all client-related documents, records, and electronic data, including business correspondence and compliance documents, for a period established in local legislation after client identification or the end of a business relationship. Additionally, they are required to retain all transaction documents and records for seven years to enable transaction reconstruction.

i. **Duty of Collaboration** – GE must promptly and fully cooperate with any requests made by the judicial and police authorities, sectoral authorities, or GE.

j. **Duty of Training** – GE must ensure that their members of the management and supervisory bodies, employees, and other collaborators or service providers involved in roles critical for preventing MLFT are well-informed about the obligations arising from applicable regulation. This is achieved by conducting regular and specific training sessions tailored to each sector of activity. Such training enables them to consistently identify operations potentially related to MLFT and to act in accordance with the current regulatory framework.

VI.2 SYSTEMS AND TOOLS

5. Each GE must have a set of IT systems and tools for the prevention of MLFT that are intended to be aligned at Group, whenever possible, and that allow for the adoption of common standards and international best practices.
6. GE must consider, at least, the following systems and tools:
    a. An onboarding screening platform.
    b. An *ex-post* monitoring platform that analyses transactions and customer behaviour.
    c. A screening system that allows both real-time transaction screening and batch screening for listed entities.
    d. External data and information sources of good repute, considered suitable, credible, and diverse, both in terms of their origin and their nature. This includes independent and credible information coming from public knowledge or international organizations.
    e. An automated CRR assignment system.
7. A workflow/system for onboarding analysis must be in place to identify, prior to the establishment of a new business relationship, which factors may prevent the establishment of such relationship, whether they by the risk factors of the intervening entities, or from external information obtained from credible sources (e.g., sanctions or embargo lists, adverse media from verified sources). This system should allow the intervention of

the Compliance Office, under a RBA methodology, and whenever high-risk factors are identified that may justify the duty of refusal.

8. A MLFT monitoring system must be adopted to monitor financial transactions (ex-post control) that seem unusual with the customer's profile or that present any suspicion of being associated with criminal activities, and MLFT practices in particular. A monitoring system from a vendor of good repute is strongly favoured, and should present the following characteristics:
    a. A high diversity of algorithms/scenarios to detect a large spectrum of threats and risk factors.
    b. The ability of being frequently updated with novel detection features and algorithms.
    c. Flexibility to allow the configuration and fine-tuning from local GE teams.
    d. A workflow-type organization that allows the generation of alerts and the intervention of more than one employee in their analysis and examination.
9. A screening system must be in place to ensure the following permanent automated controls:
    a. A real-time transaction screening to identify, prior to operations completion, MLFT risk factors associated with the intervenients (customers, counterparties and correspondent banks) or with the involved jurisdictions (ensuring the timely detection of entities or jurisdictions that are subject to sanctions or embargoes).
    b. A batch-mode entities filtering system to identify any entities (customers, representatives or UBO) that may subject to sanctions or embargoes.
    c. In addition to the customer database, GE must also promote the filtering of other entities to which the implementation of restrictive measures should apply, including external service providers and shareholders (when external to the Group).
    d. Quick and secure mechanisms that ensure immediate, full, and effective execution of restrictive measures and allow for the blocking of accounts or the suspension or execution of transactions, sets of transactions, or business relations when compliance with freezing obligations arising from restrictive measures is required.
10. GE must possess external databases and data sources with information for specific purposes and MLFT controls (such as identification of PEP, negative news or adverse media, companies' registries and information on their UBO). GE must ensure that the providers of such information are credible and of good repute.
11. Each GE should have an automated platform or system to model and assign a CRR to each individual business relationship. The CRR system must automatically generate an initial risk score at the onboarding stage and must be continuously updated/ refreshed whenever there are changes in the factors that are included in its calculation. The CRR system must be able to include, at least, the following data:
    a. The Entity's key jurisdictions (nationality, country of residence, and any other country where it holds relevant commercial relationships).
    b. The PEP status (current or former).
    c. The nature and risk profile of its activities.
    d. The association with any other high-risk MLFT entities (such as co-account holders or UBO).
    e. The input from previous events (such as previous suspicions or reports).
12. Specific tools may be used to assess MLFT risks for specific operations or products (e.g., in credit granting operations to assess the risk of UBO and other relevant participants).
13. Robotic process automation tools may be applied to improve the system's efficiency, but its adoption must be properly tested and documented, including the auditable record-keeping of all robotic interventions.

14. Each GE must monitor and ensure the data quality of its record keeping, namely of all inputs that influence MLFT controls, especially in what regards entities, transactions and suspicious activity reports.

VI.3 POLICIES

15. Each GE must have and keep updated a set of minimum policies regarding the identification, management and control of MLFT risks, namely:

    a. Customer Acceptance Policy with the principles and categories of entities that present a risk profile where the establishment of a business relationship, or its maintenance, should be conditioned or refused.

    b. Customer Identification and Due Diligence Policy specifying the particular situations in which the establishment and maintenance of a business relationship or occasional transaction must be subjected to CDD or EDD procedures, and the way in which these procedures must be carried out[4].

    c. An Irregularities Communication and Whistleblowing Policy that outlines the channels and the protection mechanisms that GE make available for the reporting of any irregularity or malpractice, including situations that may be in any way related with MLFT risks.

VII. CUSTOMER DILIGENCE MEASURES

1. To effectively manage MLFT risk associated with a client GE monitoring must include at least the following steps:

    a. Establish clear expectations regarding client behaviour, such as the likely nature, amount, source, and destination of transactions, to enable the detection of unusual transactions.

    b. Regular review of client accounts to understand if changes in the client's risk profile are justified, thus ensuring continuous and effective monitoring.

    c. Any changes to information previously obtained under the KYC process are taken into account, particularly those that might affect the GE assessment of MLFT risk associated with the individual business relationship.

2. Within the scope of the operational model, each GE must devote special attention to the duty of diligence and to the procedures that it should entail (CDD and EDD).

3. GE must detail and document the procedures that must be carried out in order to ensure the adequate understanding of the financial behaviour and risk profile of its customers database and associated funds and assets.

4. The due diligence (referred below as diligences) measures should consider in particular the following aspects:

    a. The timing of diligence (scheduled or non-scheduled).

    b. The extension of diligence (standard or enhanced).

    c. The specificity of diligence.

[4] Policies on customer identification should guide handling applications from individuals who cannot provide traditional identity documentation due to seeking asylum, being refugees, or lacking a residence permit but are legally or factually unable to be expelled. The Entity should specify acceptable alternative forms of ID and options for postponing full identification until the business relationship is established.

VII.1. TIMING OF DILIGENCE

5. GE are entitled to promote diligence measures either under a pre-planned and scheduled program of customer information revision or by spontaneous and unplanned necessity, brought forward by the analysis or examination of a financial transaction or by any external information or event that may affect the risk profile of a particular Entity or set of Entities.

Scheduled Diligences

6. Each GE must develop a periodic customer review program, in order to ensure updated customer information and documentation for its customer base, which must highlight the scheduling requirements following an RBA methodology.
7. The periodic review must include missing information, as well as information that needs to be confirmed or that is out of date (specifying what supporting documentation needs to be collected and archived for each type of information).
8. The update schedule must not exceed 5 years for MLFT low-risk customers and 1 year for MLFT high-risk customers (PEP inclusive).
9. Whenever, during the review of a customer, the existence of new increased risk factors becomes evident, the Compliance Office must be notified to evaluate the need for an EDD.
10. All diligences and customer revisions must be adequately documented and archived for future consultation and auditability.

Unscheduled Diligences

11. Extraordinary or spontaneous diligences must be carried out whenever a GE has a reason to doubt the veracity, accuracy, or timeliness of the information collected from the customer.
12. A diligence must also be triggered immediately whenever there is knowledge of:
    a. Change in the management body, UBO, legal representative and the nature of the activity or business model.
    b. Expiration of the validity period for identification documents.
    c. When there are suspicions of malpractice, raised by credible news related to MLFT.
    d. When there are suspicions that the Entity is referenced in international sanctions lists.
13. When a customer changes its PEP status, namely by acquiring a new PEP position, during the business relationship with GE, GE must involve a senior manager to assess and decide on the continuation of the business relationship. This decision should be based on a comprehensive analysis of the inherent risk associated with maintaining the relationship.
14. All unscheduled diligences must be adequately documented and archived, including the motivation that gave rise to the diligence and whether there was a confirmation of any MLFT suspicion.

VII.2 EXTENSION OF DILIGENCE

15. The extension of the diligence procedures to be applied (CDD or EDD) depends on the MLFT risks that are assessed in the establishment, maintenance or review of a business relationship or an occasional transaction.

16. The CDD procedure concerns the simplified or standard measures adopted for customer identification and diligence when the overall MLFT risk associated with the customer, or the operation is not assessed as high.
17. CDD procedures are standard in nature and are usually carried out by the first line of defence.
18. The EDD procedure is applied to strengthen standard CDD measures when high MLFT risk situations are detected.
19. EDD measures are more thorough than CDD procedures and are usually performed by the Compliance Office (in articulation with the first line of defence).
20. Both CDD and EDD procedures may imply the revision and update of a customer's CRR.

Customer Due Diligence

21. Each GE must follow CDD procedures to identify who the customer is and, where applicable, the UBOs or their legal representatives.
22. Within the scope of the CDD the GE may collect information on the products and services that are part (or admissible) of the business relationship.
23. Each CDD must verify and confirm the nature and purpose of the business relationship or transaction.
24. The CDD must validate and document the source or destination of funds (or assets) and the source of wealth involved in the transaction or business relationship under analysis.
25. During a CDD, the GE must also verify when a series of occasional transactions should become a business relationship.
26. Each GE should document how CDD measures are proportionate to MLFT risks.

Enhanced Due Diligence

27. Each GE must, in addition to CDD measures, apply EDD measures in MLFT high-risk situations in order to adequately manage and mitigate these risks.
28. GE must consider the enforcement of EDD procedures for the following entities/operations that present a higher MLFT risk profile:
    a. When the customer, representative or the UBO, is a PEP.
    b. When a correspondence relationship involves payments with a third-country institution located in high-risk jurisdictions.
    c. When the GE maintains a business relationship or conducts transactions involving high-risk jurisdictions.
    d. Transactions that have the following characteristics:
        i. complex or conducted in an unusual pattern.
        ii. a particularly high amount.
        iii. without obvious economic or lawful purpose.
        iv. involving entities with high MLFT risk (assessed through the CRR).

VII.3 SPECIFITY OF THE DILIGENCE

29. GE must detail specific diligence procedures that are appropriate for certain customer segments, products, or services.

30. Given the higher MLFT risk associated with such customers or products and services, GE must define the context-specific procedures that will be carried out for the following categories:

    a. Correspondence banking services.

    b. PEP customers.

    c. Private banking services.

    d. Pooled accounts.

    e. Trade finance services.

    f. Virtual assets.

Correspondence banking services

31. GE must adopt specific EDD measures in cross-border correspondence relationships with respondents based in a third country, applying controls provided for in GR0045 - Selection and Relationship with Correspondent Banks Policy.

PEP customers

32. When exercising EDD measures over PEP customers, GE should take into account the list of prominent public functions published by the European Commission in Directive (EU) 2015/849, as well as all functions provided for by applicable legislation and regulation.

33. Each GE should use external suppliers of PEP lists, understand any limitations of those lists, and set additional controls to address these limitations.

34. The specific measures that must be adopted for PEP customers must include:

    a. Adequate measures to establish the origin of the assets and funds involved in the business relationship, removing suspicions of corruption or other criminal activities related to the PEP status.

    b. Confirmation of the approval by a member of the Senior Management to maintain the PEP business relationship.

    c. An increased frequency of monitoring of PEP transactions (e.g., using lower thresholds).

    d. A detailed review of historical transaction profile to identify unusual transactions.

35. The above measures should also be applied to close family members and persons known to be closely associated, adjusting the extent of these measures on a risk sensitive basis.

Pooled accounts

36. Whenever pooled accounts are used to manage funds that belong to the customer's own clients, GE must apply specific diligence measures, including treating the customer's own clients as the UBOs of the funds held in the pooled account, verifying their identity.

37. The diligence for pooled accounts must ensure that the transactional profile of the account is thoroughly analysed to ensure its consistence with the purpose and objective of such type of account.

Private banking services

38. The EDD must verify that the transactional profile and product ownership is consistent with the customer's segment and activity profile.

39. The EDD for private banking customers must ensure detailed knowledge of the source of wealth and funds, including documentary support (e.g., recent salary receipts, contracts for the sale of financial assets or assets, evidence of wills or granting of probate).

Trade finance services

40. The EDD process for services and operations associated with Trade Finance must always:
    a. Perform the complete identification of customers, their legal representatives, and their UBO.
    b. Check whether the operations profile is consistent with the customer's history and economic activity.
    c. Carry out the identification and analysis of the MLFT risk associated with the counterparties of commercial transactions.
    d. Understand the ownership and background of all related parties in the transaction, particularly when they are established in a higher-risk jurisdiction or when dealing with high-risk goods.
    e. Confirm the economic rationale that legitimizes the operation by checking the consistency of the invoice or equivalent document, verifying that there is no overvaluation or undervaluation, taking into account the unit price/market value of the commodity.
    f. Identify very structured, fragmented, or complex operations, involving multiple parties without apparent justification (dismissing the participation or involvement of any entities with sanctions and embargoes issued by the UN or EU).

Virtual assets

41. As for the issuance, holding, or distribution of virtual assets, GE should consider the high MLFT risks of this activity, which remains largely unregulated, and should apply EDD measures both to business relationships and to all individual transactions that result from the conversion of these assets into fiat currency and destined for its customers.
42. GE should also identify the nature of the business carried out by their customers and the origin of the funds that result from the exchange of virtual assets in fiat currency, as well as their legitimacy.
43. GE should verify if the companies that use the initial coin offering ("ICO"), and where the funds for their customers originate, are legitimate or regulated.

VIII. TRAINING AND CONTINUOUS IMPROVEMENT

1. This Policy aims to promote the constant updating of MLFT knowledge and skills of all GE employees and to develop an organization culture that seeks the continuous improvement of the quality and effectiveness of MLFT prevention processes and controls.
2. The ExCo of each GE ensures the necessary training and communication initiatives to foster a robust Compliance culture.
3. In addition to the Compliance Global Operating Model described in this Policy, each GE must consider the following initiatives:
    a. Communication Plan – a structured program should be planned in advance to schedule communication initiatives that ensure an adequate understanding and knowledge of MLFT prevention policies and controls in the entire organization, and especially by the first line of defence.

b. Training Program - A structured training program, applicable to all GE Employees and in particular to the Compliance team, to ensure the renewal of knowledge and respond to the specific needs of the different lines of defence.

c. Standards and technical documentation on MLFT controls - A set of up-to-date documents that describe all the configurations and features of processes and controls that lead to MLFT prevention and risk management.

d. Scheduling periodic reviews – A set of periodic and pre-scheduled events for the maintenance and review of analytical parameters and limits of platforms, tools, and controls.

e. Quality Assurance and Monitoring Methodology - A structured process to assess the effectiveness and coherence of MLFT risk prevention and management processes and support systems.

4. The above measures should be included and updated in each GE Compliance Office annual activity plan.

5. The execution of these initiatives, along with other measures that strengthen the Compliance culture, must be monitored by the adequate governance structure at each GE.

6. BCP and each GE will cooperate to identify priority areas for further training and will cooperate on identifying opportunities for shared training actions and initiatives.

IX. GROUP OVERSIGHT AND COOPERATION

1. All GE should, within its legal context, cooperate with the BCP Compliance Office, namely through the BCP GE Liaison, providing the information that is relevant for control and responding in an accurate, complete, current and timely manner to what has been requested.

2. Monitoring and reporting is fundamental to assess the adequacy and quality of controls of the Compliance function, as well as to raise concerns/alerts and to identify potential threats.

3. The BCP Group shares information between its entities pertaining to the prevention and combat of MLFT. Namely, it shall strive to ensure that each Group management body, business area, and the internal unit has the necessary information to perform its functions. Additionally, BCP shall ensure the necessary exchange of adequate information between business units and the Compliance Office of the GE, and the respective communication between the GE Compliance Office and BCP Compliance Office.

4. The BCP Compliance Officer shall:

   a. Create a group wide MLFT risk assessment where it will take into account both the individual risks of the various GE and the possible interrelationships that may have a significant impact on risk exposure at the Group level. Special attention should be given to the risks to which the Group's branches or GE established in third countries are exposed, especially if they present a high-risk of MLFT.

   b. Define Group-level MLFT standards and ensure that the EG policies and procedures comply with MLFT laws and regulations that apply individually to each EG and are also aligned with defined Group standards.

   c. Monitor the activities of EG Compliance Officers across the Group thus ensuring that they function in a consistent manner.

   d. Monitor the EG and branches, located in third countries, compliance with EU based MLFT regulation, namely when these requirements are less stringent than those set out in applicable EU Regulation.

   e. Establish Group-wide procedures and measures, namely regarding data protection and information sharing within the Group for MLFT purposes.

f. Ensure that GE have adequate procedures in place and share information appropriately, including information that a suspicious transaction report has been issued.

5. Each GE should observe 3 principles in its risk monitoring and reporting framework:
    a. Report with respect to a risk control framework:
        i. identifying and assessing key compliance risks to be monitored and mitigated.
        ii. defining risk controls and analysis for key processes.
    b. Build a systematic reporting process:
        i. with systematic collection of Compliance Key Performance Indicators ("KPI") and Key Risk Indicators ("KRI").
        ii. with periodic reports that provide analysis and insights for all relevant risks.
    c. Define quality control and testing mechanisms:
        i. to assess the accuracy of existing information (and design new data gathering processes) for key risks.
        ii. to report on quality assurance tests for key processes and systems.
6. For GE located in third countries (as defined in EU regulation[5]), the acceptance of new business relationships and subscription of products that present a high risk in terms of MLFT must be preceded by a prior and individualized opinion from BCP Compliance Officer.
7. GE are required to notify the BCP Compliance Office of any report submitted to supervisory authorities or other legal entities concerning MLFT matters related to its customers and counterparties.
8. Each GE should proactively identify new indicators or information that is deemed relevant to be shared with the BCP Compliance Office.
9. In order to strengthen its risk management model at the Group level, the BCP Compliance Office will annually conduct, in coordination with GE, a risk assessment for each GE on MLFT risk. This assessment will take into consideration the Inherent and residual risk levels for the different risk factors categories - countries, customers, and products (e.g., safety-box rentals, anonymous products, trade finance, customers with frequent interactions with high-risk jurisdictions, volume of cash transactions).
10. In addition to the structured reporting mentioned above, the BCP Compliance Office must have access to all Compliance and MLFT screening and monitoring tools, policies, and procedures in place in each GE. This includes granting access to the core systems and applications, which allows for the full identification of deficiencies and opportunities for improvement in each, as well as the monitoring of corresponding corrective measures.
11. GE engage with BCP whenever any relevant change is planned or promoted to key MLFT controls, including systems, policies, or procedures that affect the overall performance of controls.
12. GE adopt a set of standard reporting elements to share with BCP (identified in Appendix II).

X. CONTROLS ON INTRA GROUP RESTRICTIONS

[5] Namely article 9 of Directive (EU) 2015/849 of the European Parliament and of the Council.

1. Under EU Regulation 2019/758 BCP needs to permanently diagnose restrictions on access to information from its GE[6] located in third country jurisdictions.
2. The diagnose on existing restrictions must ensure the application of policies and procedures that are necessary to:
    a. adequately identify and assess the MLFT risk with a business relationship.
    b. identify and assess occasional transactions, namely due to restrictions on access of information concerning relevant customers and their respective beneficial ownership information.
    c. address restrictions on the use of such information for CDD purposes.
    d. address any prohibition or restriction on the sharing, processing, transfer, or record-keeping measures of data for MLFT purposes.
3. Whenever restrictions on information sharing are identified, each GE will seek customers' consent, or any other equivalent legal permit, to overcome applicable restrictions or prohibitions within the terms of its jurisdiction's law.
4. Should the above paragraph prove to be not possible, the GE and BCP must implement additional measures to its standard MLFT measures[7].
5. BCP will promptly notify the regulator of the situation identified in paragraph 1 and implement the necessary measures[8].

XI. FINAL PROVISIONS

1. Without prejudice to the general disclosure that is made to all employees through the internal portal, the new version will be disclosed and made available to all employees whose functions are relevant for the purposes of MLFT, giving special relevance to controls enunciated by the new version.
2. The control duties described in this Policy must be addressed in the MLFT training contents to ensure their understanding by all employees.

[6] Applicable to BCP subsidiaries located in Mozambique and its branch in Macau.

[7] As identified in article 8 of the Commission Delegated Regulation (EU) 2019/758 of 31 January 2019.

[8] In accordance with the terms of paragraph 1 of article 3 to 5 of Commission Delegated Regulation (EU) 2019/758 of 31 January 2019.

APPENDIX I - NON-EXHAUSTIVE LIST OF HIGH MLFT RISK FACTORS

NON-EXHAUSTIVE LIST OF HIGH-RISK FACTORS AND INDICATIVE TYPES	
Private Entities	Entities involved in the transactions are referred to in news, with association with terrorist organizations, money laundering, international sanctions or other crimes and infractions;
	Entities that have been subject to measures or sanctions of an administrative or judicial nature for violation of the regulatory framework related to MLFT;
	PEP, close family members, holders of other political or public positions, or persons recognized as strictly associated;
	Entities that attempt to conceal or cover up i) the source or destination of funds or ii) the intended purpose or nature of the business relationship
	Entities with financial activity incompatible with their professional activity or with the entity's known sources of income;
	Entity provides an unknown address, considered false or uncertain;
	An entity is a third-country national who requests residency or citizenship rights in exchange for capital transfers, acquisition of assets or public debt securities, or investment in corporate entities established in GE territory;
Collective Entities	Entity tries to hide the identity of the beneficial owner or requests that the transaction be structured to hide the identity of the true customer;
	Entities that have been subject to measures or sanctions of an administrative or judicial nature for violation of the normative framework related to MLFT;
	Lack of business and operational activity;
	Ownership or control structures of Entity(ies) that appear unusual or excessively complex, taking into account the nature of the activity pursued;
	Companies with nominee shareholders or whose capital is represented by bearer shares;
	Legal persons or collective interest centres without legal personality that are structures for holding personal assets;
	Asset holding vehicles and Asset Management vehicles;
	Newly created entity and the transaction value is high in relation to its assets;
	Entities that are newly created legal persons and without a known or adequate business profile for the declared activity;
	Entity has ties to PEP or Persons recognized as closely associated with PEPs and their family members;
	The commercial company is made up of partners who are somehow related to terrorist organizations or money laundering activities;
	The directors, managers and shareholders of an entity all reside in a country other than the country of operation and registration of the entity, there are no direct contact persons for the entity in their region of operation;
	The managers of an entity are likely to be front men, for example, lack of business management experience, lack of interest in commerce, lack of knowledge of transactions, etc., designed to disguise the beneficial owners;
	The name of an entity appears as a likely copy of the name of a known society or is too similar to a known name, probably with the aim of appearing as part of the known society, although not linked to it.;
	Transactions, products or services associated with virtual assets and electronic currencies;
	Private Banking Relationship;

Product, service, operation or business line	Trade Finance Operation;
	High Risk Goods
	Goods or operations that favour the entity's anonymity;
	Activities carried out by the Entity involving frequent cash transactions;
	Purchase of goods, through a legal person, with no appearance of interest in relation to its corporate purpose;
	Amount of goods acquired apparently disproportionate to the size of the entity;
	Business relationships or operations without the physical presence of the customer and without recourse to secure electronic or remote identification mechanisms;
	Credit operations in which the entity is headquartered in jurisdictions that make it difficult or impossible to obtain information regarding the identity and legitimacy of the parties involved (and respective UBO), including offshore jurisdictions;
	Credits guaranteed by goods that are located in jurisdictions that make it difficult or impossible to obtain information regarding the identity and legitimacy of the parties involved (and respective UBO) in providing the guarantee;
	Entities that carry out economic activities in sectors prone to tax evasion or that are considered, by reputable and credible sources, as having a high MLFT risk (e.g. real estate, gambling, transport, auctions, among others);
	Entities that carry out economic activities in sectors often associated with high levels of corruption;
	One-off operations of high value, taking into account what is expected for the product, service, operation or distribution channel used;
	Transactions relating to oil, weapons, precious stones and metals, tobacco products, cultural artefacts and other items of archaeological, historical, cultural and religious relevance or of rare scientific value, as well as ivory and protected species;
	The value of an entity's registered imports reveals a significant inconsistency in relation to the volume of foreign bank transfers with regard to imports;
	The amount of foreign bank transfers for an entity's imports reveals a significant incongruity with the taxes paid for import activities;
Correspondent Banking	Correspondence relationships in which the respondent – or the financial group he is part of – has been subject to measures or sanctions relevant to MLFT;
	Situations in which the respondent develops a significant segment of their business in activities or sectors often associated with the MLFT;
	Correspondence relationships with entities that hold an offshore banking license;
Jurisdiction	Entities resident or active in jurisdictions associated with a higher risk of MLFT;
	Entities with a nationality or known passage through jurisdictions associated with a higher risk of MLFT;
	Entities that use intermediaries or agents with broad powers of representation, for the purpose of initiating or managing the business relationship, especially when they are headquartered in jurisdictions associated with a higher MLFT risk;
	Jurisdictions identified by reputable and credible sources as having ineffective judicial systems or deficiencies in the investigation of crimes associated with the MLFT;
	Countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity;
	Jurisdictions that do not implement reliable and accessible UBO registries (or other equivalent mechanisms);

	Jurisdictions that have not implemented the Common Reporting Standard developed by the Organization for Economic Cooperation and Development (OECD) on the automatic exchange of information ("Common Reporting Standard");
	Jurisdictions known for offering simplified or non-existent relevant administrative procedures or clearly more favourable privileged taxation regimes;
	Jurisdictions with legal regimes that establish prohibitions or restrictions that prevent or limit compliance, by the financial entity, with the legal and regulatory rules that govern the respective activity, including in terms of the provision and circulation of information.

APPENDIX II – REPORTS ISSUED FROM EACH GE TO BCP

1. In order to ensure a coherent control and monitoring of MLFT risks across the Group, each GE must prepare and submit to BCP a standard set of reports, with a predefined frequency and structure.
2. The standard required reports are the following:
    a. Monthly Reports:
        i. a set of KPI/KRI that must be collected and reported, not only referring to MLFT but also with other activities and risk natures, such as market abuse, training, etc. The structure and methodology of quantification of these indicators is accorded between the BCP Compliance Office and all GE.
        ii. all relevant interactions with supervisors, especially regarding MLFT concerns or supervisory actions.
        iii. risk Appetite Statement indicators, namely those regarding the internal control system with information on the status of the Internal Control findings and recommendations, the monitoring of MLFT high-risk customers and the business relationships that have been closed for MLFT reasons.
        iv. the status of Group policies adoption.
    b. Quarterly Reports - qualitative quarterly assessment, that must include an opinion from GE Compliance Offices on the highlights, high-risk factors and major projects that have been concluded during the quarter.
    c. Annual Reports - MLFT risk factors self-assessment, considering inherent risk levels and the quality of existing controls. The risk factors under assessment must include at least the following three categories: i) countries, ii) customers and iii) products and distribution.
    d. As part of the ongoing monitoring and cooperation between BCP and all GE, a set of ad-hoc reports will be shared with BCP:
        i. the execution of the annual activity plan of the Compliance function.
        ii. the monitoring and follow-up of sanctions and fines issued by supervisors and other local authorities regarding compliance.
        iii. the monitoring and follow-up of specific findings issued by internal or external auditors.
        iv. others that prove necessary.

Approval Date: 31/07/2024

Body that approved: Conselho de Administração

Main changes to previously published content:

In Chapter I: Inclusion of EBA Guidelines - EBA/GL/2022/05 in the list of regulations in which GR0006 is based on. We highlight that most of the provisions of these guidelines were already incorporated during prior revisions of GR0006; Inclusion of Recommendations issued by the Financial Action Task Force ("FATF").

In Chapter II: Correct the definitions in alphabetical order; Corrected the definition of KYC;

In Chapter IV: For easier referencing sub-paragraphs has been clearly labeled; A clarification has been done on the roles of the Compliance Officer and AML Officer, regarding suspicious transactions and customers to ensure they are reported to the competent authorities; In the Compliance Control Conference, the duty to report customers of operations subject to restrictive measures has been included.; It was included a sub-paragraph that created the obligation of GE to report to BCP Compliance Office specific transactions.

In Chapter V: Inclusion of the duty for GE to differentiate between risks associated with a category of customer from the specific customer itself, this inclusion comes from EBA Guidelines; Inclusion of the geographical exposure, customer base, distribution channels and products and services offered as risk criteria; Inclusion of the duty of GE to obtain detailed information on the purpose and nature of the business relationship; Creation of the duty for GE to set out in their policies and procedures the grounds in which a business relationship may be rejected or terminated. This comes from EBA Guidelines.

In Chapter VI: Reorganization of the MLFT duties and inclusion of two new duties (Duty of Control and Duty of Training). This comes from European MLFT Directives; Included a clarification in which the screening system must be quick and based on secure mechanisms; Included footnote 4 that arises from EBA Guidelines.

In Chapter VII: Included a paragraph with some steps regarding MLFT risk associated with a client monitoring; Included a clarification of the diligence that GE must adopt when a clients' PEP status changes during the business relationship.

In Chapter IX: Included the duty for GE to obtain the prior opinion from BCP Compliance Officer before accepting new business relationships and subscription of products that present a high risk; Included the duty for GE to notify BCP Compliance Office of any report submitted to the supervisory or other legal authorities; Included the power for BCP Compliance Office to have access to the core systems and applications for MLFT screening and monitoring in GE.


Millennium
bcp