United Taiwan Bank S.A.

Guidelines Governing Anti-Money Laundering and Countering the Financing of Terrorism

APPROVAL LOG

Management Committee	Board of Directors	Remarks
29.09.2025	11.12.2025	• To make adjustments to the wording in the definitions of politically exposed persons (PEPs) and their family members, and to include the link to the single list of PEP as published by the European Commission.
21.06.2024	04.11.2024	According to the latest update of the NBB AML/CFT website, we have included the followings: • the submission of responses to the periodic questionnaire and the copy of the AMLCO's annual activity report have been revised to a general text, as the due date may vary each year. • the Board shall first verify the suitability of the individuals to be appointed as AML Supervisor or AMLCO. • the NBB's expectations regarding the AMLCO's language skills and the measures expected of financial institutions in the event of a vacancy.
02.05.2024	15.05.2024	• According to the latest update of the NBB AML/CFT website, the list of PEP functions defined by the European Commission is included under the definition of PEP. • To be more specific on the place of birth, the city and country of birth are included. • Amend the method to report suspicious transaction to CTIF.
11.10.2023	20.12.2023	• Adding an annex under Article 24 with the full description of the statute/ tasks of the AML Supervisor and the AMLCO, as well as to the AML responsibilities of the Board and the MC according to the latest AML/ CFT website of the NBB.
24.10.2022	19.12.2022	Review: no change
12.11.2021	16.12.2021	• To in line with TCB's group policy, to amend Article 1 to address the implementation of this guideline shall be on risk-based approach and it shall be documented properly. • To amend Article 11, to allow the establishment of the relationship with NPO which is set up and controlled by the Republic of China (Taiwan). • To amend "corporate entity" as "corporate and other legal entity" to in line with the amendment of Article 11.
01.12 2020	23.12. 2020	• The main changes are as the following: • To streamline the corporate governance, the relevant procedures are approved by the Management Committee, as authorised by the NBB, to better respond to the evolving situations. • Update of the Belgian AML Law of 18.09.2017, amended by the AML Law of 20.07.2020. • Update NBB's circular regarding transposing of the AML V EU Directive. • Insert "7." in Article 17. Article 29 of the AML Law of 18.09.2017, as amended by the AML Law of 20.07.2020 requests to collect evidence of the registration of the UBO in the UBO register. • Include "negative news" to be defined by the relevant methodology as the overriding factor. • Insert "6" in Article 12, due to the business nature of correspondent banking is far away from retail deposit and corporate lending business. It is indeed necessary to have separate procedures to deal with this kind of business and this in accordance with article 40 of the AML Law of 18.09.2017, as amended by the AML Law of 20.07.2020. • due to the fact that article 38 of the AML Law of 18.09.2017, as amended by the AML Law of 20.07.2020 have earmarked the customers located in high risk countries as the customers for which special measures of increased vigilance are applicable.
28 Mar 2019	07 May 2019	The main changes are as the following: • Refuse to create correspondent banking business with the credit institution seeking to open an account with UTB. (Article 6, 2 to 8) • Include if the beneficial owners and the senior managers of the customers are regarded as "PEPS". (Article 12, 2 (1) and 4) • Obtain the necessary information, such as name, date of birth, nationality, of the senior managers of the legal entity. (Article 14, 4) • Obtain the necessary information of the "High Risk profile Customer" when implementing the enhanced customer due diligent measures and create business relationship. (Article 17,1 and 5) • Stipulate the training schedule and minimum hours for AML/CFT supervisor AMLCO and personnel. (Article 25, 2)
15 Oct 2018	18 Dec 2018	The major updates are the following: • Appointment of a member of the management committee responsible for supervising the implementation of and compliance with the AML Law. • AML whistle blowing procedure. • Annual review of the overall risk assessment. • Updated definition of UBO. • Update of the identification and verification requirements of natural persons and legal entities, their proxies and UBO's.

13 Apr 2018	14 May 2018	• We have added under a new article 3, an overview of the AML policies, procedures and internal control measures which have to be in place. • Article 4, elaborates on the AML overall risk assessment which has to be done on a yearly basis. The first one was submitted on Mar 29, 2018 to the National Bank of Belgium. • Under article 20, we have described more in detail the processing of a-typical transactions and under article 21, the reporting of suspicious ML/TF transactions. • We have included under article 22, the requirements of the Belgian privacy law with regard to the protection of personal data. • We have included under article 24, the need to appoint a member of the management committee to be responsible for supervising the implementation of the AML Laws.
30 Oct 2017	12 Dec 2017	• The criteria defined in article 10 to classify the customers in low risk, medium risk and high risk, have been changed in order to comply with the European Union IV AML Directive. • A new "Money Laundering and Terrorism Financing Risk Assessment Table" (referred to in article 10.1) has been created, also in line with the European Union IV AML Directive and the risk-based approach requested in this Directive. • . A new "increasing risk" section has been created under article 10. The "increasing risk" factors under this section were taken from the NBB AML questionnaire sent to the banks this year.
11 Apr 2017	09 May 2017	• With the aim to make more detailed guidelines governing anti- money laundering and countering of terrorism, a new separate document has been drafted. Before, these guidelines were included in the Guidelines for Deposit and Remittance activities. • These guidelines follow/include the Belgian and Taiwanese laws and regulations in these matters.

Table of Contents

Chapter One- General Rules

Article 1 Introduction

The Guidelines are formulated for the bank employees to obey in order to prevent the money laundering and counter the financing of terrorism.

The implementation of this Guideline shall be on the risk-based approach and it shall be documented properly.

The relevant procedures or methodology for implementing the Guidelines are approved by Management Committee.

Article 2 Reference

These guidelines are in accordance with following Laws, Regulations and Circulars from both the Belgium and Taiwanese Authorities:

1. The NBB circulars concerning the NBB Periodic Questionnaires on the prevention of money laundering and terrorist financing are issued annually to financial institutions under NBB supervision. These circulars include detailed instructions on how to complete the questionnaire, the deadline for submission, and the platform to be used.
2. The NBB circulars related to the AMLCO's annual activity report are issued annually to financial institutions under NBB supervision. These circulars provide detailed guidelines on how to make the report, the submission deadline, and the platform to be used.
3. Belgian AML Law:
   (1) 18 September 2017 Law on the prevention of money laundering and terrorist financing and on the restriction of the use of cash
   (2) 20 July 2020 AML Law amending the Belgian AML Law of 18 September 2017.
4. Regulation of the National Bank of Belgium ("NBB AML Regulation")
   (1) 21 November 2017 on the prevention of money laundering and terrorist financing.
   (2) 15 September 2020 Circular NBB_2020_36 on the transposing of the AML V EU Directive 2018/843 into Belgian Law by the AML Law of 20 July 2020.
5. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (the "5th Anti-Money Laundering Directive").
6. Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated by the Financial Supervisory Commission
7. Specimen of "Guidelines Governing Anti-Money Laundering and Combating the Financing of Terrorism by the Banking Sector" Bank Association, ROC.

Article 3 Elements of policies and procedures

The Bank shall develop and implement the policies, procedures and internal control measures related to money laundering and financing of terrorism, "ML/FT", that are efficient and commensurate with its nature and size. The policies, procedures and internal control measures shall include:

1. Overall risk assessment;
2. Customer acceptance policy;
3. Due diligence towards customers and transactions;
4. Reporting of suspicions;
5. Record-keeping;
6. Appointment of Anti-Money Laundering Compliance Officer, AMLCO and of Member within Management Committee to be responsible for supervising the implementation of and the compliance with the provision of the AML Law of 18 September 2017
7. AML "whistle blowing" procedure

8. Training;
9. Cross-border Correspondent Banking relationships (Please refer to 5 Cross-border correspondent banking of the "Guidelines for Deposit and Remittance activities of United Taiwan Bank") ; and
10. European Regulation on transfers of funds. (European Regulation (EU) 2015/847, and refer to 4.5.3 and 4.5.4 of the "Guidelines for Deposit and Remittance activities of United Taiwan Bank".)

The Bank shall submit the policies, procedures and internal control measures implemented to the Management Committee and to the Board of Directors for approval pursuant to paragraph 1.

Article 4 Overall risk assessment

The Bank shall take measures that are appropriate and commensurate with the nature and the size of operations to identify and assess the ML/FT risks exposed, by taking into account in particular the characteristics of the customers, the products, services or transactions offered, the countries or geographical areas concerned and the distribution channels used.
When performing the overall risk assessment referred to in the first paragraph, the Bank shall take into consideration not only all the activities carried out, but also the variables such as the purpose of an account or relationship, the level of assets deposited by a customer or the expected size of transactions undertaken, and the regularity or duration of the business relationship. The Bank shall also take into account the factors that are indicative of a potentially lower risk or higher risk.
The overall risk assessment referred in the first paragraph shall be carried out, documented, updated, kept and done annually under the responsibility of the AML compliance officer, AMLCO. The Bank must be able to ensure that the policies, procedures and internal control measures developed in accordance with Article 3 are appropriate in view of the ML/FT risks identified.

Article 5 Definitions:

1. Beneficial Owner: means the natural person(s) who ultimately own(s) or control(s) the customer, and/or the natural person(s) on whose behalf a transaction is carried out or a business relationship is established.
   Are considered to be persons who ultimately own or control the customer, the customer's agent or the beneficiary in the case of corporate or other legal entities:
   (1) The natural person(s) who ultimately own(s) or control(s) a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings.
   A natural person holding more than twenty five percent of the voting rights or more than twenty five percent of the shares or ownership interest in the company shall be an indication of direct ownership within the meaning of the first subparagraph.
   A corporate or other legal entity which is under the control of (a) natural person(s), or by multiple corporate or other legal entities, which are under the control of the same natural person(s), holding more than twenty five percent of the voting rights or more than twenty five percent of the shares or ownership interest in the company shall be an indication of indirect ownership within the meaning of the first subparagraph.
   (2) The natural person(s) that exercise(s) control over this corporate or other legal entity via other means.
   (3) If, after having exhausted all possible means and provided there are no grounds for suspicion, no person under point (1) or (2) is identified, or if there is any doubt that the person(s) identified are the beneficial owner(s), the natural person(s) who hold the position of senior managing official(s) shall keep records of the actions taken in order to identify the beneficial ownership.

2. Politically exposed person (PEPs): a natural person who is or used to be entrusted with prominent public functions, listed in Annex IV of the Anti-Money Laundering Law of 18.09.2017, as amended on 08.02.2023, which is regularly updated and also mentioned in the single list published by the European Commission (**http://data.europa.eu/eli/C/2023/724/oj**), and includes the

following (non-exhaustive list):

(1) Heads of State, heads of government, ministers and deputy or assistant ministers;
(2) Members of parliament or of similar legislative bodies;
(3) Members of the governing bodies of political parties;
(4) Members of supreme courts, of constitutional courts or of other high-level judicial bodies[1];
(5) Members of courts of auditors or of the boards of central banks;
(6) Ambassadors, consuls, chargés d'affaires and high-ranking officers in the armed forces;
(7) Members of the administrative, management or supervisory bodies of State-owned enterprises;
(8) Directors, deputy directors and members of the board or persons in an equivalent function of an international organization[2].

3. Family members of a PEP includes the following:
   (1) The spouse, or a person considered to be equivalent to a spouse.
   (2) The children and their spouses, or persons considered to be equivalent to a spouse.
   (3) The parents.
   (4) The First-degree lineal relatives by marriage.
   (5) The siblings.
   (6) Siblings of spouse.

4. Persons known to be close associates with PEP: means
   (1) Natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person.
   (2) Natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

Chapter Two- Customer Acceptance Policy

Article 6 Conditions to refuse

Under following conditions, the bank should refuse those who ask for having a business relationship:

1. Credit institutions that have no offices in the country where their statutory office is established and that are not affiliated to a financial group submitted to a regulation following the recommendations of the GAFI or that are not subject to an effective consolidated supervision.
2. Credit Institutions that seek to open and to keep of anonymous and fictitious named accounts.
3. Unlicensed banks and/or NBFIs who seek to open and to keep accounts.
4. Credit institutions that provide banking services to unlicensed banks.
5. Shell banks who seek to open accounts or to establish business relationships.
6. Credit institutions that provide services to shell banks.
7. Credit institutions designated by section 311 who seek to open and to keep an account.
8. Credit institutions, such as unlicensed/unregulated remittance agents, exchanges houses, money transfer agents, seek to open and to keep accounts.
9. The customer is suspicious to open an Anonymous account or under a pseudonym or false name.
10. The customer refuses to provide related documents for verifying identity, or provides incorrect or incomplete identification information attempting to conceal his/her own identity or the customer's beneficial owner identity.
11. In the case that any person acts on behalf of a customer, it is difficult to verify that the person purporting to act on behalf of the customer is so authorized and it is difficult to verify the identity of that person.

---

[1] Other high-level judicial bodies include administrative judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances.

[2] International organisations are defined in Article 4, 32°, of Anti-Money Laundering Law as associations of means or interests established by means of an international agreement between States, with joint bodies if necessary, with legal personality and subject to a legal system which is different from the one of its members.

12. The customer uses forged or fraudulent identification documents or only provides photocopies of the identification documents.
13. The customer provides suspicious or unclear documents, refuses to provide other documents, or the documents provided cannot be authenticated.
14. The customer procrastinates in providing identification documents in an unusual manner.
15. The bank cannot verify the beneficiary owner of the account.
16. A legal entity or an organization that does not have a business location.
17. The legal entity issued the bearer shares.
18. Other unusual circumstances exist and the customer fails to provide a reasonable explanation.
19. The customer is an individual, legal entity or organization sanctioned under the Terrorism Financing Prevention Act of Belgium or Taiwan, or a terrorist or terrorist group identified or investigated by a foreign government or an international anti-money laundering organization.

The bank has to refuse to establish business relationship with private individuals/ corporate or other legal entities falling under conditions 1 to 19. Besides, the bank has to report to CTIF-CFI via the platform goAML.

Article 7 Face to Face

The bank may refuse applications without "face to face" presence of the applicants. Here, the "face to face" presence of the applicants means that the applicants are personally present in the bank or that the bank's employee goes to applicants' place and helps them to finish the application.

Article 8 The services that UTB does not provide

The bank will not provide the following services:
1. Any service for occasional customer or customer asking for occasional transaction.
2. Cash transaction.
3. Transaction related to insurance policy or pension, superannuation or similar scheme.
4. Numbered Account, Pooled Account, Assets management service or Private banking service.

Article 9 Customer identity verification procedure finished first

Before completing customer identity verification procedure, the bank shall not establish a business relationship with the applicant or provide any account numbers to the applicant.

Article 10 Third-party services

The bank won't use the service of third-party business introducers, such as services from non-exclusive insurance intermediaries, intermediaries in banking and investment services or other financial institutions whether or not belonging to its group, to fulfill its obligations of identifying or verifying the identity of customers, their proxy and beneficial owners.

Article 11 Prohibition and exemption

The Bank will not establish any business relationship with a legal entity other than a corporate company, such as a foundation or a non-profit organization, or a trust, de facto associations, fiduciary or any similar legal arrangements.

The non-profit organization which is set up and controlled by the government of the Republic of China (Taiwan) is exempted from the prohibition described in the above paragraph, provided the establishment of the business relationship is approved by the Management Committee.

Article 12 Three Risk Level

Based on the criteria of Relationship establishing channel, Type of Product and services, Customer Type, Type of Business/ Occupation, Geographic Locations, and Purpose of funds, customers are classified into three risk categories: low risk, medium risk and high risk.

1. When accepting a new customer or performing the customer due diligence according to article 16 of this Guidelines for the existing customers, the bank shall fill in the "Money Laundering and Terrorism Financing Risk Assessment Table of UTB" to classify customers' risk category.

2. When customers meet one of the following conditions, they are classified as "high risk" customers:
   (1) The customer or their beneficial owners, senior management is a PEP and the family members and persons known to be close associates.
   (2) Customers who hold dual nationality or are residents in GAFI non cooperative countries, or in the sanction list country published by EU, UN or Belgium.
   (3) Customers who are celebrities involved in financial dispute.
   (4) The purpose of account opening is unclear, or customers are considered to attempt to do money laundering or terrorist financing.
   (5) Customers used to be reported to be suspicious of money laundering transaction.
   (6) Financial Institutions from outside EEA countries which are not GAFI equivalent countries and ask for opening a correspondent bank account.
   (7) The customer is registered in/is residing in/his or her nationality is of the high-risk country defined by the European Commission.
   (8) The customer is subject of negative news. The definition of negative news is determined in the relevant methodology.

3. The following factors should be taken into account and be identified as an increasing risk criterion when classifying the risk category of a customer:
   (1) The customer is not physically present at the time of the identification.
   (2) It is impossible to verify the identity of the beneficial owners, and/or to identify their place and date of birth, and/or to gather relevant information about their address.
   (3) The customer is a non-resident of Belgium.
   (4) Transactions related to petroleum, arms and precious metals.

4. Customers or their beneficial owners, senior management who were used to be PEPs but have left that position for more than 12 months will be classified into medium risk. But after assessing the risks based on the level of influence that the individual could still exercise, the seniority of the position that the individual held as a PEP, etc, the Bank shall classify the former PEP into "high risk" category.

5. Review frequency related to the customers' risk profile are classified as below:
   (1) For category of "high risk profile", their risk profiles should be reviewed at least once a year.
   (2) For category of "medium risk profile", their risk profiles should be reviewed at least every two years.
   (3) For category of "low risk profile", their risk profiles should be reviewed at least every three years.

6. In order to be able to properly evaluate the AML/CFT Risk on Nostro/Vostro correspondent banking relationships, a special, separate assessment table and procedures can be set by applying risk based approach for the business nature of this kind.

Chapter Three- Identification and Verification of Customer Identity

Article 13 Timing to conduct CDD

The Bank should undertake customer due diligence measures when:

1. Establishing business relationship;
2. Carrying out an occasional transaction that amounts to EUR 10 000 or more, whether that transaction is carried out in a single operation or in several operations which appear to be linked;
3. There is a suspicion of money laundering or terrorist financing;
4. There are doubts about the veracity or adequacy of previously obtained customer identification documents.
5. There is doubt that a person, within the framework of a business relationship, is in fact the client with whom there is a business relationship or his/her authorized and identified proxy.

Article 14 Contents of CDD

The implementation of customer due diligence measures shall comprise:

1. Identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

2. Investigating the proxy fact if the account opening or transaction is done through a proxy, and verifying the proxy's identity with reliable, independent and original documents, data or information, and keeping the copy of the proxy's identity document for record. The proxy should show the power of attorney. After investigating and verifying the proxy's identity and the authorized facts, the bank should retain copies of all the related documents.

3. Identifying the beneficial owner and taking reasonable measures to verify that person's identity
   (1) For natural person, the bank should make sure that the account is for the customer's own use.
   (2) For corporate or other legal entity, the bank should identify its beneficiary owner in accordance with Article 5, item 1 in this Guideline.
   (3) For easement, the bank should check if the beneficiary owner and the collateral owner are the same. If not, the bank should verify the collateral owner's identity as well.
   (4) The duty to take reasonable measures to verify the identity of the UBO especially applies when the identified UBO is a senior management staff, referred to under article 5.1(3)

4. When the customer is a legal entity, the bank should obtain the name, date of birth and nationality of their senior management. (The senior management shall include the director, supervisor, counsellor, President, Chief Financial Officer, representative, manager, partner, authorized signatory, or natural person who is considered to be the senior management. The bank has to implement the risk-based approach to decide who the senior management is.).

5. Understanding and, as appropriate, obtaining related information on the purpose and intended nature of the business relationship and the expected size of transactions;

6. Conducting ongoing monitoring of the business relationship, including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the bank's knowledge of the customer, the business and risk profile and where necessary the source of funds, and ensuring that the documents, data or information held are kept up-to-date.

7. Implementing adequate risk management systems to determine whether the customer with whom they enter or have business relationship, a proxy or beneficial owner of the customer is or has become a politically exposed person (PEP) , a family member of a PEP or a person known to be closely associated with a PEP.

Article 15 Identification and Verification

Identification and Verification of the identity of the customer, the representative/ proxy and the ultimate beneficial owner (UBO) (customer due diligence: CDD)

1. The customer due diligence has as objective to :
   (1) Identify and verify the customer identity on the basis of information obtained from a reliable and independent source.
   (2) Identify and verify, where applicable, the representative/ proxy of the client's identity on the basis of information obtained from a reliable and independent source.
   (3) Identify and verify, where applicable, the ultimate beneficial owner (UBO) of customer on the basis of information obtained from a reliable and independent source.
   (4) Obtain information on the purpose and type of intended transaction of the business relationship.

2. Implementation of the Identification and verification of the customer identity:
   (1) Natural person
      (a) The identification information required shall be included but not limited to the following data:
         a. Surname;
         b. First name;
         c. Date of birth;
         d. Place of birth (City, Country);
         e. If possible, where relevant, the address.
      (b) Documents to be used for verification:
         a. Belgian residents: identity card;
         b. Non-Belgian residents: passport;
         c. Belgian residents that are foreign citizens without ID card: valid inscription in register of foreigners and valid documents that attest the legality of stay in Belgium.

   (2) Legal entity:
      (a) The identification information required shall be included but not limited to the following data: :
         a. Full legal name and legal form of the applicant
         b. Address of the registered office of the applicant;
         c. Names of the directors of the applicant
         d. Certified articles of incorporation ;
         e. Powers of representations
      (b) Documents to be used for verification
         a. The verification must be performed using documents that have probative value pursuant to law of the country in which the legal entity is established or registered.
         b. The documents can be obtained from customers, official sources or other sources considered as reliable. If the documents are provided by the customer (or his/her representative), reasonable measures must be taken to ensure reliability of the information contained in the documents.
         c. The documents must be provided in a language that allows the performance of the verification and the execution of internal control measures.

3. Identification and verification of the representative/proxy identity:
   (1) The identification information required shall be included but not limited to the following data:
      (a) Natural person:
         a. Surname;
         b. First name;
         c. Date of birth;
         d. Place of birth (City, Country);
         e. Address of the place of residence (to the extent possible);
         f. Powers of representation.
      (b) Legal entity:
         a. Full legal name and legal form of the applicant;

b. Address of the registered office of the applicant;
c. Names of the directors of the applicant;
d. Certified articles of incorporation;
e. Powers of representation.

(2) Documents to be used for verification:
(a) Depending on the method identification (face-to-face identification vs non-face-to-face identification), different verification measures must be applied.
(b) In case of face-to-face identification, reasonable measures must be applied to verify the reliability of the provided documents, such as checking the security features of documents and performing a loss/theft check on the documents (if possible).
(c) The documents that are provided must be valid.

4. Identification and verification of the Ultimate beneficial owner (UBO) identity:
(1) The identification information required shall be included but not limited to the following data:
(a) Surname
(b) First name
(c) Date of birth (to the extent possible)
(d) Place of birth (City, Country, to the extent possible)
(e) Address of the place of residence (to the extent possible)
(2) Documents to be used for verification
(a) Belgian residents: identity card;
(b) Non-Belgian residents: passport;
(c) Belgian residents that are foreign citizens without ID card: valid inscription in register of foreigners and valid documents that attest the legality of stay in Belgium.

5. Verify by other means other than document
(1) By phone or mail
(2) Customer invoices such as gas, electricity, and bank statement, etc.
(3) Information provided by other financial institutions
(4) Cross-checking all the information provided by the customer with other reliable information and non-free data base.

6. When conducting customer due diligence, the bank should use self-established database or information obtained from external sources to determine whether the customer, proxy, beneficial owner, senior management or counterparty is a person who is or used to be entrusted with a prominent function by a domestic, foreign government or an international organization, and check if is on the money laundering, financing of terrorism, embargo or sanction lists published by the authorities.

7. With regard to the UBO, the UBO register should be consulted, if applicable, in order to collect evidence of the registration of the UBO information.

Chapter Four—Ongoing monitoring measures

Article 16 Ongoing CDD

The bank shall conduct customer due diligence in accordance with Article 14 to the business relationship of existing customer:
1. When a customer opens an additional account or establishes new business relationships.
2. When conducting a regular review of a customer in accordance with in Article 12, item 5 of this Guidelines.
3. When the identity of customer and the background information changed significantly.
4. Unusually large transactions in the light of the bank's knowledge of the customer's profile and the business relationship.
5. Transfers of funds received for the benefit of customers which are not accompanied by the necessary information on the payer.
6. Customers for whom transactions deemed suspicious by the bank has been reported to the CTIF-

CFI or have been transmitted by the first-line or second-line monitoring system to AML officer of the bank, without these internal reports having given to any reporting of a suspicious transaction to the CTIF-CFI.

7. When the transaction is involved of huge cash movement.
8. Other circumstances which create a situation of high risk of money laundering or terrorist financing considered necessary by the bank.
9. Customer due diligence also includes the updating of the characteristics of the customer, the intended transaction and the purpose of the business relationship.

Article 17 For high-risk profile customer

The verification of identity of High-risk profile customer, including the customers located in high-risk countries determined by European Commission, and ongoing monitoring measures must include the following steps:

1. Measures for implementing enhanced customer due diligence and reviews:
   (1) Obtaining additional the information in relation to account opening and the purpose of establishing business relationships: expected usage of accounts (e.g. expected transaction values, objectives and frequencies) and the reasons for the transactions envisaged.
   (2) Obtaining additional information on the customer and on the beneficial owner.
   (3) Adopting reasonable measures to understand the wealth and capital sources of the customer. The capital sources refer to the substantive sources of funds (e.g. salaries, investment incomes, real estate transactions).
      (a) Obtaining the information regarding the sources of wealth, inflows and outflows of funds, types and quantities of assets for individual customers. If the capital sources are from deposits, it is necessary to get further understanding for the sources of these deposits.
      (b) Obtaining further commercial information on legal entity customers. It is necessary to understand the most recent financial status, business activities and business relationships of the customer in order to establish a profile regarding its assets, capital sources and capital destinations.
   (4) Obtaining the explanations and information regarding transactions ongoing or completed.
   (5) Conducting on-site visits or telephone interviews depending on customer types to confirm the customer's operational status.
2. It should get the approval from Managing Director before establishing or adding new business relationship.
3. The bank has to take necessary actions to analyze the sources of customers' wealth and funding, and special attention should be given that no money laundering activities are involved.
4. The bank must conduct enhanced ongoing monitoring to maintain its business relationship with high risk profile customers.
5. For a natural person who is classified as a high-risk customer, the bank should obtain at least one of the following information when establishing business relationships:
   (1) Any other previous names or alias;
   (2) Work address, post office box address, e-mail address (if any);
   (3) Landline or mobile phone numbers.

For those ongoing monitoring measured mentioned above, the Bank may implement the following enhanced verification. For example:

1. Obtaining a duly signed reply letter, sent to the address provided by customer, from the customer or the authorized signatory of the customer, or contacting the customer by telephone.
2. Obtaining the document that supports an individual's sources of wealth and sources of funds.
3. On-site visit.
4. Obtain trading information from other financial institutions that used to have business relationship with the customer.
5. Ensure, where appropriate, that the first payment is made through an account in the client's name with a credit institution which is subject to standards of vigilance with regard to clients that are no less stringent than those laid down in the Belgian AML Law.

6. Carry out enhanced monitoring of the business relationship by increasing the number and frequency of controls and by selecting transaction patterns that require further information.

Article 18 Requirements of ongoing monitoring

1. The bank shall conduct ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the bank's knowledge of the customer, the business and risk profile, including where necessary the source of funds.

2. The bank shall routinely review and identify the adequacy of identification information obtained with respect to customers, proxies and ultimate beneficiaries and ensure that the information is kept up to date, particularly for high-risk profile customers, who shall be reviewed at least once annually. For other risk profile customers, the frequency of review is decided based on the risk-based approach.

3. The bank is entitled to rely on the identification and verification steps that it has already undertaken, therefore the bank is allowed not to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction unless it has doubts about the veracity of that information. Examples of situations that might lead a banking business to have such doubts could be where there is a suspicion of money laundering or the financing of terrorism in relation to that customer, or where there is a material change in the way that the customer's account is operated that is not consistent with the customer's business profile.

4. When the verification of the identity of customers cannot be reasonably effected, the bank shall document the measures having been implemented. The bank should refuse to enter into a business relationship or perform the transaction requested, or terminate any already established business relationship, in order to unreasonably aggravate the risk of money laundering or financing of terrorism.

Article 19 Internal Procedures regarding ongoing monitoring

1. Based on the risk-based approach, the bank shall establish its internal procedure of ongoing monitoring measures of accounts and transaction by using the information system to discover the suspicious transaction.

2. When discovering or reasonably suspecting that the customer, funds, assets, or transaction implemented are related to money laundering or terrorists financing, the bank shall re-verify the customer's identity no matter whatever the amount or value is or whether the transaction is completed.

3. For the warning transaction which is suspicious of or showing the signs of terrorism financing, the bank needs not only to check if the transaction (i) does not appear to be commensurate with the customer's status, income or business scale, or (ii) is unrelated to the nature of the customer's business or not compatible with the customer's business model, (iii) does not have reasonable economic purpose or explanation, and (iv) has unknown or unclear origin of funding, it also needs to keep the checking record. If the transaction is not suspicious of or showing no signs of terrorism financing, the bank needs to keep a record and document the reason why the transaction is not suspicious; however, if the transaction is suspicious of or showing the signs of terrorism financing, the bank should not only confirm the customer's identity and retain the transaction documents, but also need to report to CTIF-CFI after confirmation.

4. The Bank shall establish the procedures for a complete monitoring system, and carrying out the setting of parameters, threshold amounts, alerts and monitoring operations, the procedures for checking the monitored cases and reporting standards, and shall be documented. The monitoring procedures and the standard mentioned shall be updated periodically. The implementation status shall also be recorded and preserved.

Chapter Five- Others

Article 20 First-line monitoring

1. The personnel in charge of the business or his/her replacer is responsible for the first-line monitoring, while the department manager or managing director conducts the second-line monitoring.

2. First-line monitoring personnel must determine the atypical transactions which require their special attention according to those criteria applied in the context of the customer acceptance policy (Chapter two of Guidelines). If that is the case, first-line monitoring personnel has to transmit his/her written reports on atypical transactions to the anti-money laundering officer of the bank.

3. The bank conducts its second-line monitoring as follows:
   (1) It must cover all accounts and transactions of the customers.
   (2) It is based on precise and relevant criteria, determined by the bank, among other things, the characteristics of the services and products it offers and those of the customers to whom it applies, and sufficiently discriminating in order to be able to effectively detect atypical transactions. Transactions which are complex or unusually large or show an unusual pattern or do not have a clear economic or legitimate purpose and have to be examined have to be given special attention.
   (3) When detecting atypical transaction, a written report has to be done and transmitted to the anti-money laundering officer, describing the atypical transactions detected and the criteria referred to, on the basis of which they are regarded as atypical transactions.
   (4) Due to its simple business model and low volume of transactions to be monitored, the bank conducts second-line monitoring manually.
   (5) The bank updates its monitoring criteria at least once a year.

4. The processing for atypical transactions.
   (1) When an atypical transaction is detected by the first-line or second line monitoring system, the AMLCO of the bank should be informed.
   (2) After receiving the atypical transaction, the AMLCO shall carefully examine the transactions carried out over the course of the business relationship as well as, where necessary, the origin of the funds, in order to verify whether these transactions are consistent with the customer's characteristics, with the nature and purpose of the business relationship, and with the customer's risk profile, in order to detect atypical transactions that should be subjected to an in-depth analysis. A written report on the analysis performed shall be drawn up.
   This obligation of information exists as soon as one thinks an operation or a fact is linked to money laundering or financing of terrorism. Anyhow, save exceptions, CTIF-CFI must be informed before execution of the operation.

Article 21 Reporting of a suspicious ML/TF transaction

1. The AML Compliance Officer of the Bank shall report to CTIF-CFI via the platform goAML, when he knows, suspects or has reasonable grounds to suspect:
   (1) That funds, regardless of the amount, are related to money laundering or terrorist financing;
   (2) That transactions or attempted transactions are related to money laundering or terrorist financing. This obligation also applies when the customer decides not to carry out the intended transaction;
   (3) That a fact of which the Bank knows, is related to money laundering and terrorist financing.

2. The information relating to a transaction, referred to in the first paragraph, shall be reported to CTIF-CFI prior to carrying out the transaction. Where appropriate, the period of time is mentioned during which the transaction must be carried out.
   In case the Bank is unable to inform CTIF-CFI prior to carrying out the transaction, either because

it is not possible to delay carrying out the transaction due to its nature, or because doing so could prevent prosecution of the individuals benefiting from this transaction, the Bank shall report this transaction to CTIF-CFI immediately after carrying out the transaction. In such a case, the reason why it was not possible to inform CTIF-CFI beforehand should be indicated.

3. The Bank shall respond to the requests for additional information sent by CTIF-CFI within the periods determined by CTIF-CFI.

4. When receiving a report of a suspicion or information, CTIF-CFI may freeze the execution of any transaction related to this report. CTIF-CFI shall immediately inform the Bank in writing within maximum five working days from the time of notification.

   In case of not being notified of a decision within the time period referred to in subparagraph 1 by CTIF-CFI, the Bank may carry out the transaction(s).

Article 22 Reporting obligation

1. The reporting obligation exists when transactions are initiated by entities established in countries with insufficient legislation concerning prevention of money laundering and terrorism. CTIF-CFI and NBB inform the banks of these countries/territories list. CTIF-CFI has to be informed by the anti-money laundering officer via the platform goAML.

2. In case of a positive match with the sanctions lists published by the competent authorities, such as EU, United Nations and Belgium, the bank has to inform the Minister of Finance (at the address of the General Treasury Administration) and has the obligation to freeze the funds and economic resources of these persons and entities. If necessary, the CTIF-CFI must also be informed if the bank knows or suspects that the transactions carried out the customer in respect of whom a positive match with the sanctions list has been found, are linked to money laundering or terrorist financing.

3. Confidentiality of the reporting documentation and information:
   (1) All the personnel have to keep confidentiality of the information related to the suspicious anti-money or terrorism financing transaction.
   (2) The reporting documentation should be handled as secret files.
   (3) The compliance officer or the auditing staff should have access to the client information and transaction records in time, but still need to exercise care to ensure the confidentiality of the information.

4. The processing of personal data is subject to the provisions of the EU Directive 2016/679 and the Belgian GDPR law of 30 July 2018 regarding the protection of privacy in relation to the processing of personal data. The Bank will only process personal data in accordance with the EU Directive 2016/679 and the Belgian GDPR Law of 30 July 2018 and does not subsequently process this data in a way that is incompatible with these purposes.

5. The Bank shall provide its customers with the required information in accordance with Article 9 of the aforementioned Law of 8 December 1992 prior to establishing a business relationship.

Article 23 Record retention period

The bank shall keep records on all business relations and transactions with its clients in accordance with the following provisions:

1. The bank shall maintain all necessary records on transactions effected for ten years. The aforementioned necessary records include:
   (1) Names, account numbers or identification numbers of all parties in the transactions.
   (2) Transaction date
   (3) Type of currency and amount.
   (4) The method to deposit or withdraw the funds.

(5) The destination of the funds.
(6) The method of instruction or authorization.

2. The bank shall keep the following information for ten years after the business relationship has ended:
   (1) All records obtained through the measures of checking and verifying the identity of customer, such as passports, identification cards, copies of similar official documents or records and documents with information on any difficulties encountered during the verification process.
   (2) Account files.
   (3) Business correspondence including inquiries to establish the background and purpose of complex, unusual transactions and the results of any analysis undertaken.

3. For the reporting of suspicious money laundering or terrorism financing transactions, the declaration records and transaction vouchers shall be archived for ten years in the original manner.

4. The bank shall ensure compliance with the requests of the Competent Authority to provide relevant information and

5. All the related records of transactions kept by the Bank shall be used to reconstruct the individual transaction and as evidence to identify the illegal activities.

Article 24 AML Supervisor and AMLCO

1. The Bank shall appoint, among the members of the Board of Directors or, where appropriate, of the Management Committee, the person responsible for supervising the implementation of the Guidelines and compliance with the provisions of the Belgium AML Law, the related European Regulations and the restrictive measures referred to the mandatory provisions on financial embargoes.

   The person appointed referred in paragraph 1 is the Deputy Managing Director, the supervisor of AML, who supervises the implementation of the issues related to AML/CTF, and performs the self-inspection jobs.

2. Compliance officer is appointed as the AMLCO of the bank. Annually, the compliance officer has to present a report concerning AML of the bank to Managing Committee and then submit it to the Board of Directors for approval. The report also has to be sent to NBB.

   The report shall enable the senior management to be aware of the evolution of the ML/FT risk is exposed and to ensure the adequacy of the policies, procedures and internal control measures implemented properly.

3. A full description of the statute/tasks of the AML Supervisor and the AMLCO, as well as to the AML responsibilities of the Board and the MC is annexed to this guideline according to the latest AML/CFT website of the NBB.

Article 25 Employment and Training

1. The bank should employ appropriate personnel, including checking if the personnel has integrity character and professional knowledge to exercise his/her duty.

2. The AML/CFT supervisor, the AML/CFT compliance officer and personnel shall possess professional knowledge on AML/CFT, be familiar with local regulations, and attend at least 12 hours of training on AML/CFT offered by competent authorities or relevant institutions annually. If the training is not available, the personnel may attend the training courses offered by internal or external training units consented by the chief compliance officer of the parent bank, Taiwan Cooperative Bank.

3. The Bank must provide its new manager and staff with 3 hours anti money laundering and counter

terrorism financing related initial training courses.

4. The bank should hold compliance training for its personnel at least once every six months.

Article 26 Escalation and Reporting

Every personnel member who, in the exercise of his/her function, acknowledged of non–compliance with the obligations of the Law, has the right to immediately inform, on a confidential basis if he chooses so, the ALMCO and/or the member of the management responsible for supervising the implementation of the AML Law, without passing via his/her hierarchical superiors.

As long as the personnel member is acting in good faith, the personnel member having informed the AMLCO and the AML Officer shall be protected from any threats, any reprisal, or hostile action, and in particular from adverse or discriminatory employment actions.

Individuals exposed to threats, retaliatory or hostile acts, or harmful or discriminatory employment measures for reporting a suspicion of money laundering or terrorist financing, internally or to the CTIF or to the National Bank of Belgium, have the right to lodge a complaint with the National Bank of Belgium.

Each personnel member has to acknowledge receipt of the policy.

Article 27 Approval Level

This Guidelines and any amendments hereto, shall come into in force after adoption by a resolution of the Board of Directors.

Annex to Article 24 of the Guidelines Governing Anti-Money Laundering and Countering the Financing of Terrorism

Description of the statute and the tasks of the Senior Officer responsible for AML/CFTP (Anti-Money Laundering and Countering the Financing of Terrorism and Proliferation), the same as AML/CFT, and of the AMLCO within the bank, as well as of the AML/CFT responsibilities of the Management Committee and the Board of Directors with regard to AML/CFT. This description reflects the NBB requirements as stipulated in the NBB AML website (**AML/CFT site)**

1. Senior Officer responsible for AML/CFT (AML Supervisor)

A) Statute

(1) Article 9 §1 of the Anti-Money Laundering Law stipulates that financial institutions should appoint, among the members of their statutory governing body or, where appropriate, of their senior management, the person responsible, at the highest level, for supervising the implementation of and compliance with the provisions of this Law
(2) Within UTB, the senior officer responsible for AML/CFT is the member of the management committee who is also responsible for compliance. This arrangement is to avoid conflicts of interest with business generating tasks.
(3) The senior officer responsible for AML/CFT is expected to act with integrity, to possess general AML/CFT-related knowledge so as to be able to critically review the measures taken by the AMLCO, and to ensure compliance with the provisions of the Anti-Money Laundering Law.
(4) Financial institutions shall verify, in the first instance, the AML/CFTP suitability of the person they are considering to appoint as AML Supervisor.
(5) The appointment has to be approved by the NBB after a ”fit & proper“ review.

B) Tasks

The statutory obligation to appoint a senior officer responsible for AML/CFT is meant to enhance the involvement of the highest hierarchical level of financial institutions in the prevention of ML/FT risk. The NBB therefore expects the senior officer responsible for AML/CFT to raise awareness, among the entire management committee of the importance of such prevention and, in particular, to perform at least the following tasks:

(1) Ensure that AML/CFT policies, procedures and internal control measures are adequate and proportionate, taking into account the characteristics of the financial institution and the ML/FT risks facing it. In this respect, the senior officer responsible for AML/CFT is expected to pay particular attention to (i) the coherence between the AML/CFT procedures and the more operational procedures for each activity, and (ii) the coherence between the AML/CFT policy and the policies implemented within the group;
(2) Assess, together with the management committee, whether the rule to appoint a separate AMLCO can be deviated from on the basis of the principle of proportionality;
(3) Support the management committee in assessing whether it is necessary to establish an AML unit to assist the AMLCO in carrying out his/her duties;
(4) Ensure regular reporting to the management committee and to the board of directors on the activities carried out by the AMLCO, and provide them with sufficiently comprehensive and timely information and data on AML/CFT risks and compliance with AML/CFT regulations, which is necessary to enable them to perform the role and functions entrusted to them. Such information should also include arrangements between UTB and the AML/CFT supervisor as well as communication with CTIF-CFI - without prejudice to the confidentiality of reports of suspicious financial transactions - and findings of the AML/CFT supervisor regarding UTB, including any measures or sanctions imposed;
(5) Notify the management committee and the board of directors of serious or significant AML/CFT problems or violations and recommend measures to remedy them; and
(6) Ensure that the AMLCO (i) has access to all the information necessary to perform his/her tasks, (ii) has sufficient human and technical resources and tools to be able to adequately

perform the tasks assigned to him/her, and (iii) is well-informed of the AML/CFT-related incidents brought to light by the internal control systems and of the shortcomings found by the national and foreign supervisory authorities while implementing the AML/CFT provisions.

The senior officer responsible for AML/CFT serves as the main point of contact for the AMLCO within management. This person should also ensure that any AML/CFT-related concerns of the AMLCO are properly addressed and, where this is not possible, that they are duly taken into account by the management committee. Where the management committee decides not to follow the AMLCO's recommendation, such decisions should be duly justified and recorded in the light of the risks and concerns raised by the AMLCO.

2. AMLCO

A) Statute

(1) Article 9 §2 of the Anti-Money Laundering Law stipulates that financial institutions should appoint one or more persons tasked with implementing and steering the AML/CFT policy ("AMLCO").
(2) The third subparagraph of Article 9 §2 of the Anti-Money Laundering Law stipulates that the AMLCO function should be effective, independent and autonomous, and that the person tasked with this function should have:
   - the professional integrity needed,
   - adequate expertise, including knowledge of the Belgian statutory and regulatory AML/CFT framework,
   - the availability, and
   - the hierarchical level and the powers within the institution to be able to propose, on the AMLCO's own initiative, all necessary or useful measures to guarantee the compliance and efficiency of the internal AML/CFT measures to the board of directors and to the management committee.
(3) The ALMCO should be part of the compliance function and can thus be, as in UTB, the compliance officer himself. Being the compliance officer, he is subject to the NBB " fit & proper " review. However, the financial institutions are expected to verify the AML/CFTP suitability of the persons they intend to appoint as AMLCO.
(4) The AMLCO should be physically based in Belgium, without prejudice to the principle of proportionality. This condition is derived from the territorial scope of application of the Anti-Money Laundering Law, compliance with which the AMLCO is responsible for ensuring, and from the requirement set out in Article 9 §2, third subparagraph, point 2° of the Anti-Money Laundering Law, pursuant to which the AMLCO must have, in particular, knowledge of the Belgian statutory and regulatory AML/CFTP framework and the necessary availability to ensure the effective, independent and autonomous performance of his or her tasks. If this requirement is derogated from on the basis of the principle of proportionality, the financial institution should have in place the necessary systems and controls to ensure that the AMLCO has access to all information and systems required to perform his or her duties and that the AMLCO is available to meet with CTIF-CFI and the supervisory authority without delay. The financial institution must also be able to provide the supervisor with evidence that the measures put in place by the institution are adequate and effective.
(5) UTB's internal procedures should ensure that the AMLCO at all times has unrestricted and direct access to all information necessary for the performance of his/her duties. The AMLCO decides what information he/she needs access to in this respect.
(6) In case of a major incident, the AMLCO should be able to report and have direct access to the board of directors.
(7) The AMLCO should have sufficient time to perform his/her tasks correctly. UTB should ensure that the AMLCO works on an ongoing basis as part of its overall business continuity management. It should consider the possibility that the AMLCO may exit their position and ensure that there is an available replacement with the required AML/CFTP expertise to whom the AMLCO's duties can be delegated should the AMLCO be absent for a period of time or should their integrity be called into question. Financial institutions are expected to

report such circumstances and the identity of the person acting for the AMLCO immediately to the competent authority by e-mail.

(8) The Management Committee and the Board should ensure that the AMLCO at all times has adequate human and material resources that enable him to comply effectively with the statutory and regulatory AML/CFT obligations. The resources allocated to AML/CFT should be proportionate to the ML/FT risks

(9) The AMLCO is expected to demonstrate a sufficient professional command of one of Belgium's national languages, having regard in particular to the knowledge of the Belgian statutory and regulatory AML/CFTP framework required of AMLCOs and in view of the tasks with which the AMLCO is entrusted. It may be acceptable for the AMLCO to have only a command of a language that is customary in international circles when the financial institution concerned can demonstrate, on the one hand, that the conditions to apply the principle of proportionality are met and, on the other hand, that this command alone is not such as to jeopardise the AML/CFTP suitability of the AMLCO, including the requirement of knowledge of the Belgian statutory and regulatory framework, or the effective performance of the AMLCO's duties.

B) Tasks

As part of the second line of defence, the AMLCO is responsible for effectively steering AML/CFT policy in the financial institution. The AMLCO's role and responsibilities should be clearly defined and documented. In particular, the AMLCO is responsible for the following tasks:

(1) Developing and maintaining an ML/FT risk assessment framework for the purpose of carrying out overall and individual risk assessments;

(2) Effectively implementing the organisational measures listed in Article 8 of the Anti-Money Laundering Law, and ensuring that they are regularly reviewed and, where necessary, amended or updated (this is mainly: develop and implement policies and procedures, internal control measures, training of staff);

(3) Proposing a course of action in the event of changes in statutory or regulatory requirements or in ML/FTP risks, and how best to address deficiencies and shortcomings revealed by monitoring and supervision;

(4) Monitoring the effective implementation of AML/CFT control measures by business units and internal units, which act as the first line of defence;

(5) Providing advice before employees at an appropriately high hierarchical level make a final decision on the acceptance or continuation of a business relationship with high-risk customers in accordance with the financial institution's risk-based internal AML/CFT policies. Where these employees do not follow the AMLCO's advice, they should properly record their decision and establish how they intend to mitigate the risks raised by the AMLCO;

(6) Analysing atypical transactions and situations in which the due diligence obligations could not be fulfilled (in accordance with Articles 45 and 46 of the Anti-Money Laundering Law);

(7) Deciding, where necessary, to report suspicions to CTIF-CFI (in accordance with Article 47 of the Anti-Money Laundering Law and the provisions adopted in implementation of Article 54 of the Law) and to provide it with any other information required by application of the Law. In this regard, the AMLCO makes the autonomous decision to report to CTIF-CFI without submitting this decision to the senior officer responsible;

(8) Responding to requests for additional information addressed to the financial institution by CTIF-CFI (in accordance with Articles 48 and 49 of the Anti-Money Laundering Law);

(9) Educating and training the staff and, where applicable, the agents and distributors of the financial institution on AML/CFT-related matters;

(10) Developing an annual AML/CFT monitoring programme covering, in particular, the application of the required measures to prevent ML/FTP by the employees, agents and distributors who are in contact with customers, and implementing this programme;

(11) Ensuring a proper flow of AML/CFT-related information within the financial institution and guaranteeing feedback to the management bodies (board of directors and management committee/senior management) and to the supervisory authorities. In this regard, the AMLCO should establish an activity report and send it to the management committee (or to the senior management if there is no management committee) and to the board of directors at least once a year. In addition, the AMLCO should in any case bring the following to the

attention of the senior officer responsible for AML/CFT: (a) areas where AML/CFT control measures should be implemented or improved; (b) proposals for appropriate improvements in line with point (a); (c) a progress report of major remediation programmes, at least once a year as part of the above-mentioned activity report, and information provided on an ad hoc basis or periodically - depending on improvements – on the level of exposure to ML/FTP risks and the measures taken or recommended to manage these risks effectively; (d) whether sufficient human and technical resources have been allocated to the AMLCO and, if not, whether they need to be supplemented.

(12) To establish an activity report, in the format/template requested by the NBB, and send it to the management committee and to the board of directors at least once a year. A copy of this report should be sent to the NBB.

3. The Board of Directors

A financial institution's board of directors has the following AML/CFT tasks:

(1) Deciding on the overall ML/FT risk management strategy of the financial institution concerned. The board of directors should therefore have appropriate knowledge, skills and experience to form an overall view of the policy implemented and the ML/FT risks associated with the activities performed and the business model, including knowledge of the statutory and regulatory framework for the prevention of ML/FTP;
(2) Validating the institution's AML/CFT policy;
(3) Being informed of the results and updates of the institution's overall ML/FT risk assessment;
(4) Reviewing the AMLCO's activity report at least once a year and, more frequently in the interim, taking note of activities that expose the financial institution to higher ML/FTP risks;
(5) Assessing at least once a year the proper functioning of the compliance function, including its AML/CFT component - inter alia on the basis of the conclusions of any internal and/or external audits performed on it - ensuring in particular the adequacy of the human and technical resources allocated to the AMLCO function.

The board of directors should have access to and consider high-quality and detailed data and information so that it is able to perform its AML/CFT tasks effectively. At a minimum, the board of directors should have timely and direct access to the AMLCO's activity report, the report of the internal audit function, the findings and conclusions of external auditors where applicable, as well as findings of the supervisor, relevant communications with CTIF-CFI and supervisory measures or administrative sanctions imposed.

4. The Management Committee

A financial institution's management committee or, if it does not have a management committee, its senior management has the following AML/CFT tasks:

(1) Implementing, at the instigation of the senior officer responsible for AML/CFT, the organisational and operational AML/CFT structure necessary to comply with Article 8 of the Anti-Money Laundering Law and with the AML/CFT strategy defined by the board of directors, paying particular attention to the adequacy of the human and technical resources allocated to the AMLCO function;
(2) Approving the internal AML/CFT procedures. Minor changes to these procedures could be validated by the senior officer responsible for AML/CFT;
(3) Implementing adequate AML/CFT-related internal control mechanisms;
(4) Approving the AMLCO's annual activity report and being in regular contact with the AMLCO;
(5) Annually assessing the efficiency of its governance system, including the AML/CFT policy;
(6) Ensuring proper AML/CFT reporting to both the board of directors and the NBB;
(7) Ensuring that any outsourcing of the AMLCO's operational tasks complies with applicable regulations and that it receives regular reports from the service provider.

5. Adherence to compliance rules

Since the AML/CFT policy should be integrated into the compliance function, the principles included in Circular NBB_2012_14 are applicable. Moreover, the prudential rule stipulating that all independent

control functions should form a coherent whole, also applies, requiring a good interaction between the compliance function and the risk management function with respect to ML/FT risks (but without creating a hierarchy between these independent control functions).

Although ML/FT risk management is the subject of specific reports submitted to the NBB, the NBB expects the compliance function to also cover this aspect in the context of its reporting on compliance. However, the use of cross-references is allowed in this reporting for AML/CFT related aspects.