AXA Bank Belgium

POLICY ON THE FIGHT AGAINST MONEY LAUNDERING AND THE FINANCING OF TERRORISM AND SANCTION COMPLIANCE

Policy information

Applicability:	This Policy must be adhered to by the senior management (incl. contractors), staff members, tied agents and the employees of tied agents of AXA Bank Belgium to the extent it is relevant for the carrying out of their assigned duties.
Owner:	Compliance
Approved by and Date of Approval:	Management Board: November 26th 2019 Board of Directors: December 5th 2019
Effective Date:	January 1th 2020
Next mandatory revision due:	

TABLE OF CONTENT

1. INTRODUCTION

In order to facilitate their criminal activities, criminals and financers of terrorism may use financial institutions and the financial system to disguise the origin of criminal proceeds or to channel lawful or illicit money for terrorist purposes. As such usage can damage the integrity, stability and reputation of the financial sector and threaten international development, many countries have enacted legislation to prevent the use of the financial system for money laundering and the financing of terrorism ("Anti") and to criminalize such illicit behaviour.

The requirements in Belgium for the prevention of money laundering and the financing of terrorism ("AML/CFT") are set out in *the Law of 18 September 2017 on the prevention of money laundering and the financing of terrorism and on the limitation of the use of cash, EU Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds implementation legislation*[1] *and their implementation legislation*. Entities subject to the supervision of the National Bank of Belgium are additionally required to comply with detailed supervisory requirements and expectations in this area[2].

With a view of promoting international peace and security, protecting human rights, preventing proliferation of weapons of mass destruction (WMDs) and fighting terrorism, international organisations (such as the UN and EU) and countries have enacted sanctions targeted at state governments or non-state entities, organizations and individuals, such as terrorist groups and terrorists. These sanction can include:

a. Arms embargoes;
b. Trade restrictions, such as import and export bans;
c. Financial restrictions such asset freezes and a prohibition to provide financial services to sanctioned state governments or non-state entities, organizations and individual; and
d. Restricting movement, such as visa or travel bans.

As a Belgian credit institution supervised by the National Bank, AXA Bank Belgium is required to comply with the abovementioned requirements and supervisory expectations and any applicable sanctions.

[1] Wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten / Loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces

[2] See *https://www.nbb.be/nl/financieel-toezicht/voorkoming-van-het-witwassen-van-geld-en-de-financiering-van-terrorisme* or *https://www.nbb.be/fr/supervision-financiere/prevention-du-blanchiment-de-capitaux-et-du-financement-du-terrorisme*. An overview of the key reference documents can be found here: *https://www.nbb.be/nl/financieel-toezicht/voorkoming-van-het-witwassen-van-geld-en-de-financiering-van-terrorisme/nuttig-0* or *https://www.nbb.be/fr/supervision-financiere/prevention-du-blanchiment-de-capitaux-et-du-financement-du-terrorisme/liens-0.*

2. PURPOSE AND OBJECTIVES OF THE POLICY

The purpose of this policy document is to set out the standards that must be complied with to allow AXA Bank Belgium to:

- adequately identify, measure and manage the money laundering and the financing of terrorism risk ("ML/FT risk") and sanction risk to which it is exposed so it can effectively contribute to combatting money laundering and the financing of terrorism and to the implementation of sanctions (incl. the prevention of sanction evasion); and
- comply with the applicable regulatory requirements and supervisory expectations, sanction measures and the relevant Group Standards (i.e. the AXA Group Anti-Money Laundering Policy and the AXA Group Sanctions Policy).

AXA Bank Belgium and AXA Group are committed to maintaining high standards with regard to AML/CFT and sanction compliance. Consequently, senior management, staff members (incl. contractors), tied agents and the employees of tied agents of AXA Bank Belgium are required to comply with the present Policy and all implementing procedures and manuals.

3. DEFINITIONS

For the purpose of this Policy, the following definition apply:

1. ***Money laundering:***
    a. *the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action*
    b. *the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity*
    c. *the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity*
    d. *participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).*

    For the application of the above definition it does not matter in which country the criminal activities which generated the property to be laundered were carried out.

2. ***Terrorism financing:*** *the provision or collection of funds and other assets, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, by a terrorist organisation or a terrorist acting alone. It is not necessary that the financing has any connection to a specific terrorist act.*

3. ***Proliferation of weapons of mass destruction (WMDs):*** *Provision of support (incl. financial assistance, financing and investment) for the development, acquisition, manufacture, transport, transfer or use of nuclear, chemical or biological weapons and their delivery systems*

4. ***Proliferation financing:*** *the provision of funds or financial services that are used for the development, acquisition, manufacture, transport, transfer or use of nuclear, chemical or biological weapons and their delivery systems.*

5. ***Anti-Money Laundering Compliance Officer ("AMLCO"):*** *The person or persons that have been assigned the responsibilities set out in section 7.1.1.2 .of this Policy.*

6. ***Business relationship:*** *a professional or commercial relationship with a certain duration that is established with a customer. Such as relationship will exist in the following situations:*
    a. *An agreement is concluded between AXA Bank Belgium and execution of this agreement entails the carrying out of several successive transactions by the parties during a specific or indefinite period;*
    b. *An agreement is concluded between AXA Bank Belgium and a customer which gives rise to a number of ongoing obligations for the parties; or*
    c. *A customer regularly uses AXA Bank Belgium for the carrying out of several successive transactions without the conclusion of an agreement in sense of points a) or b) above.*

7. ***Occasional transaction:*** *a transaction that will be executed outside the context of a business relationship*

8. ***Politically exposed person:*** *a natural person who is or who has been entrusted with prominent public functions and includes the following:*
    a. *heads of State, heads of government, ministers and deputy or assistant ministers;*
    b. *members of parliament or of similar legislative bodies;*
    c. *members of the governing bodies of political parties;*
    d. *members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;*
    e. *members of courts of auditors or of the boards of central banks; (*
    f. *ambassadors, chargés d'affaires and high-ranking officers in the armed forces;*
    g. *members of the administrative, management or supervisory bodies of State-owned enterprises;*
    h. *directors, deputy directors and members of the board or equivalent function of an international organisation*

9. ***Transfer of funds:*** *any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same, including:*
    a. *a national or cross-border transactions consisting of crediting a payee's payment account with a payment transaction or a series of payment transactions from a payer's payment account by the payment service provides which holds the payer's payment account, based on an instruction given by the payer ("credit transfers");*
    b. *a national or cross-border transactions consisting of debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the payer's consent ("direct debits");*
    c. *transfer of funds from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee;*
    d. *transfers carried out using a payment card, an electronic money instrument, or a mobile phone, or any other digital or IT prepaid or post-paid device with similar characteristics.*

10. ***Payer:*** *a person that holds a payment account and allows a transfer of funds from that payment account, or, where there is no payment account, that gives a transfer of funds order.*

11. ***Payee:*** *a person that is the intended recipient of the transfer of funds.*

12. ***Payment account:*** *an account held in the name of one or more payment service users which is used for the execution of payment transactions*

4. STANDARDS TO BE ADHERED TO WITH REGARD TO AML/CFT

4.1. Prohibitions

1 It is prohibited to:

- engage in and/or participate in, commit, aid, abet, facilitate or counsel the commission of actions that constituted (attempted) ML/FT;
- engage in and/or participate in, commit, aid, abet, facilitate or counsel the commission of actions that constitute an (attempted) breach or evasion of sanctions;
- breach the standards set out in this Policy and the procedures and manuals that implement them;
- open or maintain anonymous accounts and accounts under a fake name or pseudonym; and
- take actions which could directly or indirect notify a customer and any other third party (excluding supervisory authorities in the area of AML/CFT, entities of the AXA Group and, under certain conditions other financial institutions) of the fact that information or intelligence has been or will be provided to the Financial Intelligence Unit CTIF-CFI and/or that the analysis with regard to possible ML/FT is ongoing or could be initiated.

Breaches of the above prohibitions can result in:

- criminal and/or administrative sanctions for AXA Bank Belgium and/or the individual(s) committing the breach; and/or
- internal disciplinary and/or legal actions in accordance with the applicable contractual framework and labour regulations.

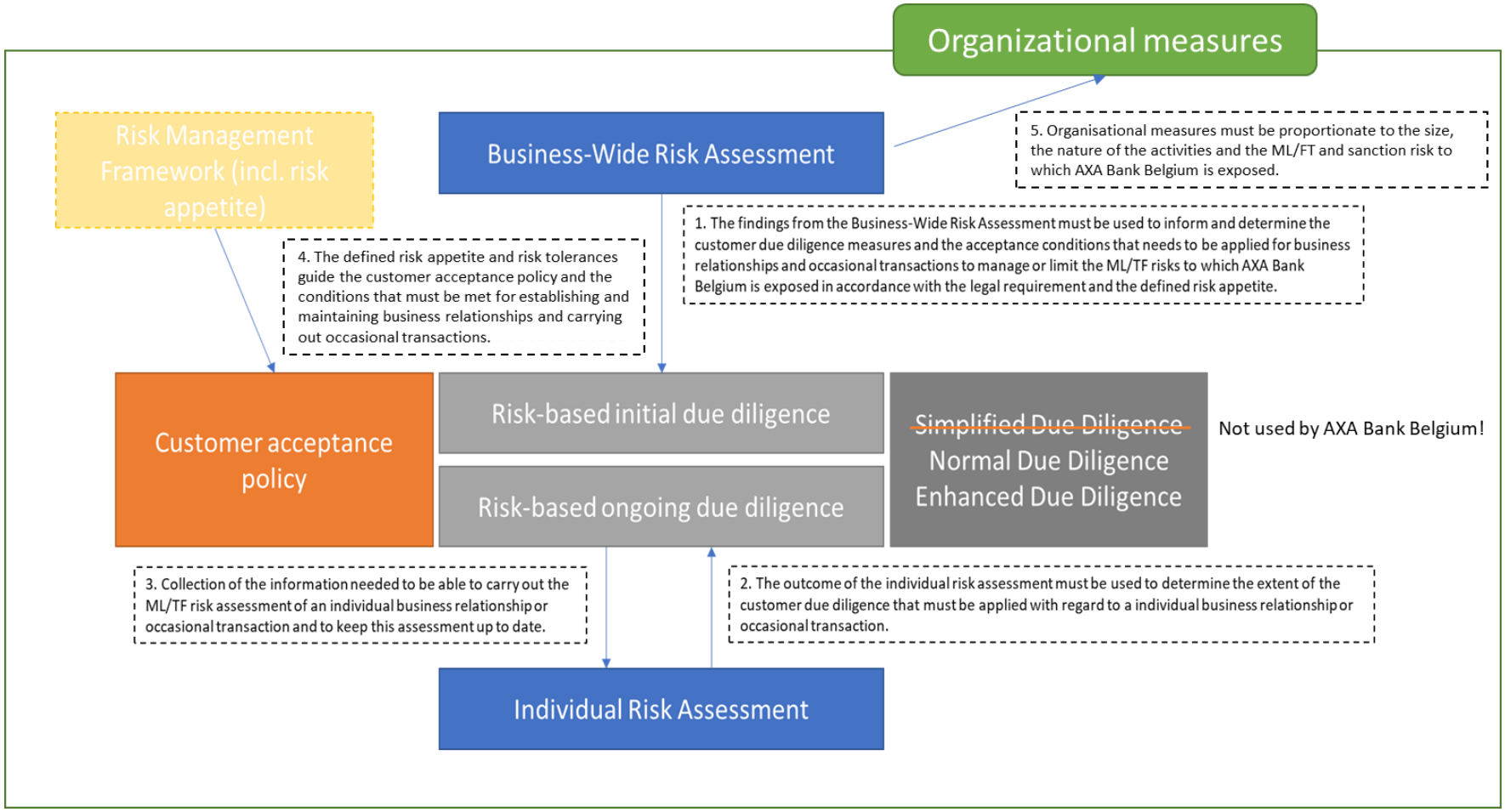
4.2. Risk-based approach to AML/CFT

4.2.1. Principles

2 AXA Bank Belgium must employ a risk-based approach to AML/CFT. This entails that the bank must identify, assess and understand the ML/FT risks to which it is exposed and take risk mitigation measures that are proportionate to those risks.

3 The application of the risk-based approach to AML/CFT and its associated measures described above must take place within and comply with the framework of AXA Bank Belgium for the management of operational and reputational risk.

4 The risk-based approach to AML/CFT within AXA Bank Belgium must be organized in accordance with the following model:



5 The above model must be built around the following components:

1. The Business-Wide Risk Assessment:
A Business-Wide Risk Assessment must be carried out to obtain a thorough understanding of:

1. the inherent ML/FT present in AXA Bank Belgium's customer base, products and services, delivery channels and services offered (including products under development or to be launched) and the jurisdictions within which it or its customers do business;
2. the residual ML/FT, i.e. the amount of risk that remains after the implementation of risk controls.

The Business-Wide Risk Assessment and its outcome must form the basis for the management of ML/FT risk at the level of AXA Bank Belgium. This entails that the findings of the Business-Wide Risk Assessment must be used:

- to determine the customer due diligence measures and the acceptance conditions that needs to be applied for business relationships and occasional transactions to manage or limit the ML/FT risk to which AXA Bank Belgium is exposed in accordance with the legal requirements and the defined risk appetite; and
- to monitor, in an ongoing manner, whether the overall exposure to ML/FT risk does not exceed the defined risk appetite and, where necessary, trigger remediation actions.

The Standards that must be adhered to for the performance of the Business-Wide Risk Assessment are set out in section 4.2.2. of this Policy.

2. The individual risk assessment:
A risk assessment of the (envisaged) individual business relationships and occasional transactions must be performed to develop and maintain a thorough understanding of the ML/FT risk associated with the (envisaged) business relationship or occasional transaction.

The individual risk assessment and its outcome must be used as the basis for the management of ML/FT risk at the level of individual business relationships and occasional transactions. This entails that the finding of the Business-Wide Risk Assessment must be used:

- to determine the extent of the customer due diligence measures that must be applied before the establishment and during the business relationship or before the carrying out of the occasional transaction to ensure that AXA Bank Belgium knows its customers and it can reasonably assume that its products and services will only be used or are only being used for legitimate purpose.
- to monitor, in an ongoing manner, whether the exposure to ML/FT risks associated with (envisaged) business relationships or occasional transactions does not exceed the defined risk appetite.

The Standards that must be adhered to for the performance of the Individual risk assessment are set out in section 4.3.2. of this Policy.

3. The Customer acceptance policy

A customer acceptance policy must be adopted which sets out the conditions for the acceptance and maintenance of business relationships and the carrying out of occasional transactions. These conditions must be designed and implemented to adequately control the identified inherent ML/FT risks identified as part of the Business-Wide Risk Assessment.

The above conditions must ensure that:

- business relationships are only established and maintained and occasional transactions are only carried out when AXA Bank Belgium knows its customers and it can reasonably assume that its products and services will only be used or are only being used for legitimate purpose;
- business relationships are only established and maintained and occasional transactions are only carried out when the residual ML/FT risk associated with the (envisaged) business relationship or occasional transaction does not exceed the risk appetite of AXA Bank Belgium; and
- The establishment and maintenance of business relationships and the carrying out of the occasional transactions is duly approved at hierarchical level that is appropriate taken into account the ML/FT associated with the business relationships and the carrying out of the occasional transactions.

While taking into account the defined risk appetite in the area of ML/FT risk, the customer acceptance policy may not be so restrictive that it results in a denial of access to banking services for people who are financially or socially disadvantaged (incl. asylum seekers).

The customer acceptance policy is set out in section 4.3. of this Policy.

4. Customer due diligence measures

Customer due diligence measures must be applied to ensure that AXA Bank Belgium knows and continues to know its customers and it can reasonably assume that its products and services will only be used or are only being used for legitimate purpose. These measures must be applied before the establishment of a business relationship or the carrying out of an occasional transaction (“initial due diligence”) and after the establishment of a business relationship or the carrying out of an occasional transaction (“ongoing due diligence”).

Customer due diligence measures must include a “basic due diligence” for all customers and a “risk based due diligence” the extent of which depends on the ML/FT risk associated with the (envisaged) business relationship or occasional transaction as determined by the individual risk assessment. This entails that:

- the amount and type of information obtained, and the extent to which this information is verified must be increased and the extent and depth of the monitoring of business relationships and transactions must be enhanced where the risk associated with the business relationship or occasional transaction is higher (“Enhanced Due Diligence”)
- the amount and type of information obtained, and the extent to which this information is verified may be decreased and the extent and depth of the monitoring of business relationships and transactions must be lowered where the risk associated with the business relationship or occasional transaction is lower (“Simplified Due Diligence”)

AXA Bank Belgium has decided not to make use of the possibility to apply Simplified Due Diligence measures in lower risk situations.

For the purpose of the above, it can be reasonably assumed that the products and services of AXA Bank Belgium will only be used or are only being used for legitimate purpose when there are no indications on the basis of which AXA Bank Belgium knows, suspects or has reasonable grounds to suspect that customers is engaging or attempting to engage in illicit activities related to ML/FT.

The Standards that must be adhered to for the performance of the customer due diligence measures are set out in sections 4.3.4. and 4.3.5. of this Policy. Standards that must be followed to align the extent of the customer due diligence measures with the ML/FT risk associated with the (envisaged) business relationships or occasional transactions are set out in 4.3.3.3. of this Policy.

5. The Risk Management Framework

The management of ML/FT risk must be integrated in the general Risk Management processes (and the processes for the management of Operational and Reputational Risk within AXA Bank Belgium. As part of this integration, a specific appetite with regard to ML/FT and risk tolerance limits have been defined.

The risk appetite and risk tolerance limits with regard to ML/FT risk are set out in section 4.2.3. of this Policy.

6. Organisational measures

AXA Bank Belgium must development and implement organisational measures to comply with the AML/CFT legislation and sanction measures that are proportionate to its size, the nature of its activities and the ML/FT and sanction risk to which it is exposed.

These measures must include appropriate and effective governance arrangements, policies, procedures and internal control measures.

The Standards that must be adhered to with regard to organisational measures are set out in Chapter 7 of this Policy.

4.2.2. Performance and maintenance of a periodic Business-Wide Risk Assessment

6 The Business-Wide Risk Assessment must consist of the following assessments:

1. Assessment of the inherent ML/FT risk to which AXA Bank Europe is exposed;
2. Assessment of the internal control environment (both the design and operating effectiveness) in place for the management of ML/FT risk;
3. Determination of the residual ML/FT risk based on the outcome of the above assessments.

7 The procedures or manuals implementing the present Policy must define how the above Business-Wide Risk Assessment must be performed. These procedures or manuals must adhere to the standards and requirements set out in the below sections.

4.2.2.1 Standards with regard to the risk assessment methodology to be used for the performance of the Business Wide Risk Assessment

8 In order to identify and assess the inherent ML/FT risk, the assessment must at least cover the following risk categories:

1. Risks associated with the customer base;
2. Risks associated the products and services offered by AXA Bank Belgium;
3. Risks associated with delivery channels used by AXA Bank Belgium to market its products and services; and
4. Risks associated with the countries and geographical areas within which AXA Bank Belgium or its customers do business.

The above risk categories must be further sub-divided into quantitative and qualitative risk factors that are derived from regulatory or supervisory requirements, guidance and supra-national and national risk assessment as well as AXA Group and industry practices. These risk factors should reflect causes or circumstances that, either on their own or in combination, may increase or decrease the ML/FT risk to which AXA Bank Belgium is exposed.

9 For the purpose of the above assessment, risk categories and risk factors must be assigned a weight which reflects the degree to which they contribute to the overall ML/FT risk.

10 The Business-Wide Risk Assessment must be performed in an holistic manner and cover all the activities of AXA Bank Belgium.

4.2.2.2. Monitoring and review

11 The Business-Wide Risk Assessment must at all times provide an accurate, up-to-date and relevant view of ML/FT risk to which AXA Bank Belgium is exposed. To this end, the assessment as well as the underlying risk factors must be reviewed (each year or when situations or circumstances occur which have a significant impact on the risk exposure of AXA Bank Belgium.

The above situations or circumstances include but are not limited to the following:

- significant strategy and operational changes effecting the inherent risk to which AXA Bank Belgium is exposed such as the introduction of a major new product or service, a merger or acquisition, opening a branch or subsidiary in a new location or closing a branch or subsidiary in a location, decisions to significantly grow the number of customers or accounts and changes to delivery channels.
- significant changes to the ML/FT risk associated with jurisdictions affecting the inherent risk to which AXA Bank Belgium is exposed. Such changes can for example be caused by significant changes to the legal and regulatory framework with regard to AML/CFT, material adverse information with regard to the effectiveness of the AML/CFT framework and socio-economic changes;
- new forms of criminal activities and new typologies affecting the inherent or residual risk to which AXA Bank Belgium is exposed; and
- significant changes to internal processes or controls or issues affecting the residual risk to which AXA Bank Belgium is exposed such as the identification of internal

control deficiencies during external/internal audits and changes in legal and regulatory requirements, supervisory expectations and/or industry practices

In addition to the above, measures must in place to identify emerging ML/FT risks and assess whether these risks need to be incorporated in the Business-Wide Risk Assessment described in section 4.2.3. of this Policy and the individual risk assessment described in section 4.3.2. of this Policy.

4.2.2.3. Reporting and communication of the outcome of the Business-Wide Risk Assessment

12 The outcome of the Business-Wide Risk Assessment and any revisions thereof must be communicated to the management of AXA Bank Belgium, business stakeholders and the competent authority. It must be approved by the Management Board.

4.2.2.4. Response to the outcome of the Business-Wide Risk Assessment

13 Appropriate remedial action must be taken when during the Business Wide Risk Assessment:

- gaps or deficiencies in the internal control environment are identified; and/or
- when the residual ML/FT risk exceeds the defined risk appetite with regard to the ML/FT risk.

4.2.3. Risk appetite and risk tolerance limits related to ML/TF

14 AXA Bank Belgium has a low risk appetite related to ML/TF and is thus unwilling to enter into business relationships with customers or maintain such relationships or to carry occasional transactions unless it has a reasonable assurance that the (potential) customer involved will not use or is not using its products and services to engage in ML/FT.

Based on an holistic and broad view on the management of the risks associated with ML/TF, the following two risk tolerances must be adhered to ensure that the above risk appetite is met:

1. The ML/FT risk associated with the customer base

ML/FT risk is the risk that customers may use the products and services of AXA Bank Belgium to engage in ML/FT.

The ML/FT risk associated with the customer basis in terms of aggregated residual ML/FT risk may not exceed:

Retail segment:	**Commercial Segment:**
Low Risk	Low Risk

Taking into account the nature of the products and services it offers as a general retail and commercial bank, its commercial approach and its target market, AXA Bank Belgium is of the view that it is appropriate and sufficient to set its risk appetite with regard to ML/FT risk at the level of its two main customer segments, namely its retail customer and its commercial customers.

The above risk tolerance must be measured using the methodology of the Business-Wide Risk Assessment described in section 4.2.2. of this Policy. Consequently, compliance with the risk tolerance must also be monitored by means of the Business-Wide Risk Assessment.

The classification of ML/FT risk foresee in the following 5 (residual) risk levels: 1) Very Low Risk, 2) Low Risk, 3) Medium Risk, 4) High Risk and 5) Very High Risk.

2. Compliance risk in the area of ML/FT

Compliance risk is the risk that a legal, administrative or regulatory sanction is imposed on an institution and/or on its staff member(s) because of the non-compliance with the legal and regulatory integrity rules and rules of conduct, resulting in a loss of reputation and a possible financial damage.

Compliance risk in the area of ML/FT may not exceed Medium Risk on an aggregated basis.

This tolerance statement acknowledges the inherent limitations with regard to the effectiveness of any AML/CFT compliance program (such the possibility of human error) and the high frequency with which actions to which compliance risk events relate are carried out.

The above risk tolerance must be measured using the methodology of the Compliance Risk Assessment. Consequently, compliance with the risk tolerance must also be monitored by means of the Compliance Risk Assessment.

The classification of Compliance Risk foresee in the following 5 (residual) risk levels: 1) Low Risk, 2) Medium Risk, 3) High Risk, 4) Very High Risk and 5) Extremely High Risk.

4.3. Customer acceptance policy

4.3.1. Conditions for establishment and maintenance of business relationships and the carrying out of occasional transactions

15 A business relationship with a (prospective) customer may only be established and maintained and an occasional transaction may only be carried out if the following conditions are met:

1. **Performance of an initial due diligence:** The customer and, when relevant, his beneficial owners have been subjected to a risk-based initial due diligence before the establishment of the business relationship in accordance with section 4.3.4. of this Policy;
2. (Only for business relationships) **Performance of an ongoing due diligence of the business relationship:** The business relationship with the customer is subjected to a risk-based ongoing due diligence after its establishment in accordance with section 4.3.5;
3. (Only for occasional transactions) **Monitoring of the occasional transaction and the customer involved:** The occasional transaction and customer are subjected to a risk-based monitoring that is appropriate given the occasional nature of relationship in accordance with Section 4.3.5. of this Policy;
4. **Performance of an individual risk assessment:** The ML/FT risk associated with the business relationship or occasional transaction has been accurately assessed in accordance with section 4.3.2. of this Policy as part of the initial due diligence and is kept up-to-date as part of the ongoing due diligence;
5. **Acceptable risk:** The ML/FT risk associated with the (envisaged) business relationship or occasional transaction must be acceptable taking into account the risk appetite and risk tolerances defined by and the customer acceptance policy of AXA Bank Belgium;
6. **Approval at an appropriate hierarchical level**: The establishment and maintenance of the business relationship and the carrying out of the occasional transaction has been duly approved at hierarchical level that is appropriate taken into account the ML/FT risk associated with the business relationship or occasional transaction;
7. The customer is deemed to fall within the target audience of AXA Bank Belgium.

Unless specified otherwise in this Policy, the same standards apply with regard to business relationships and occasional transactions.

For the avoidance of doubt, the above conditions (and in particular the requirement to perform an initial due diligence) must be complied with for each envisaged occasional transaction regardless of the amount, service or product involved. AXA Bank Belgium has chosen not to make use of the possibility provided by article 21, §1, 2° of Law of 18 September 2017 on the prevention of money laundering and the financing of terrorism and on the limitation of the use of cash not to perform the identification and identity verification of the customer and, when relevant, his beneficial owners or authorized representatives in case of certain low risk occasional transactions[3].

[3] 1) One or more occasional transactions which appear to be linked amounting to a total of less than EUR 10 000 and 2) One or more credit transfers or transfers of funds within the meaning of Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May

16 An authorized representative of a (prospective) customer may only be allowed to exercise and continue to exercise his powers of representation if the following conditions are met:

1. **Performance of an initial due diligence:** The authorized representative was been subjected to a risk based initial due diligence before exercising his powers of representation in accordance with section 4.3.4. of this Policy;
2. **Performance of an ongoing due diligence:** He is subjected to a risk-based ongoing due diligence after being accepted as an authorized representative in accordance with Section 4.3.5 of this Policy;
3. **Assessment of connected party risk:** The ML/FT associated with the authorized representative has been assessed as part of the initial due diligence and is kept up-to-date as part of the ongoing due diligence. This risk is duly taken into account for the assessment of the ML/FT risk associated with the business relationship or occasional transaction; and
4. **The authorized representative is a natural person.**

In case it is not possible to successfully perform the initial or ongoing due diligence with regard to an authorized representative of a (prospective) customer in accordance with the present Policy and the procedures and manuals implementing it, the authorized representative may not be allowed or may no longer be allowed to exercise his powers of representation. The aforementioned element must also be taken into account for the assessment of the ML/FT risk associated with the business relationship or occasional transaction involved.

17 The procedures or manuals implementing the present Policy must define the situations in which a business relationship will be established between AXA Bank Belgium and a customer and the situations in which AXA Bank Belgium will be considered to carry out occasional transactions (incl. when occasional transactions for a particular customers can be considered to be carried out with such regularity that a business relationship can be considered to have been established).

4.3.2. Individual risk assessment of business relationships and occasional transactions

18 The objective of the individual risk assessment is to develop and maintain a thorough understanding of the inherent ML/FT risk associated with a (envisaged) business relationship or with respect to occasional transactions.

19 The procedures or manuals implementing the present Policy must define how the above individual risk assessment must be performed. These procedures or manuals must adhere to the standards and requirements set out in the below sections.

2015 on information accompanying transfers of funds that appear to be linked and that amount to a total of EUR 1.000 or less and where AXA Bank Belgium does not receive the funds concerned in cash or in the form of anonymous electronic money.

4.3.2.1 Standards with regard to the risk assessment methodology to be used for the performance of individual risk assessments

20 In order to identify and assess the inherent ML/FT risk associated with a particular business relationship or occasional transaction, the assessment must at least cover the following risk categories:

1. Risks associated with the (potential) customer and parties connected to the (potential) customer in the context of the business relationship or occasional transaction ("connected parties");
2. Risks associated with the products and services that the customer wishes to use or is using;
3. Risks associated with the delivery channels through which the customer obtains or will obtain products and services and/or is introduced.
4. Risks associated with the countries and geographical areas with which the (potential) customer and connected parties have business and personal links.

The above risk categories must be further sub-divided into risk factors that are derived from regulatory or supervisory requirements, guidance and supra-national and national risk assessment as well as AXA Group and industry practices. These risk factors should reflect causes or circumstances that, either on their own or in combination, may increase or decrease the ML/FT risk associated with the business relationship or occasional transaction.

For the purpose of the above, the presence of the following risk factors must in all circumstances result in an increased ML/FT score being associated with the business relationship or occasional transaction:

- a business relationship cannot be terminated and alternative restrictive measures have been taken;
- the (potential) customer, an authorized representative of the customer and/or a beneficial owner of the customer is a politically exposed person, a family member of a politically exposed person or a person known to be a close associate of a politically exposed person after the establishment of the business relationship;
- the (potential) customer is residing or established in a third country with a high ML/FT risk;
- occasional transactions that are linked to tax havens; and
- business relationships in the context of which transactions that are linked to tax havens will be or are being carried out; and
- business relationships that involve persons or legal arrangements residing or established in a tax haven or that are governed by the law of such country.

The manner in which the individual risk assessments is performed must be aligned with the Business-Wide Risk Assessment.

21 For the purpose of the above assessment, risk categories and risk factors must be assigned a weight which reflects the degree to which they contribute to the overall ML/FT risk.

When weighing the risk categories and risk factors the following must be ensured:

- The weighting is not unduly influenced by just one factor;
- Economic (incl. staffing) or profit considerations may not influence the risk rating;
- The weighting may not lead to a situation where it is impossible for any business relationship to be classified as high risk;
- Legally prescribed situations that always present a high ML/FT risk cannot be over-ruled by the weighting; and
- It must be possible to over-ride any automatically generated risk scores where necessary. The rationale for the decision to over-ride such scores must be documented appropriately. Any downgrades of the identified risk must be approved at appropriate hierarchical level taking into account the original identified ML/FT risk.

4.3.2.2. Categorising business relationships and occasional transactions into risk categories

22 Based on the outcome of the individual risk assessment, business relationships and occasional transactions must be categorised into one of following risk categories:

1. Standard Risk;
2. Medium Risk;
3. High Risk; and
4. Very High Risk.

The above risk categories reflect that extent of the initial and ongoing due diligence or monitoring that must be applied.

Business relationships and occasional transactions which, when considered in a holistic manner, are not considered to represent an increased ML/FT risk must be designated as "Standard Risk".

Business relationships and occasional transactions which, when considered in a holistic manner, represent an increased ML/FT risk must be designated as "Medium Risk", "High Risk" or "Very High Risk" depending on the number and nature of the risk factors that are present.

23 The calibration of the risk categories may not by unduly influenced by economic (incl. staffing) or profit considerations and must take into account regulatory or supervisory requirements, guidance as well as AXA Group and industry practices.

4.3.2.3 Monitoring and review

24 Individual risk assessments of business relationships and with respect to occasional transactions must be kept up-to-date and under review. To this end individual risk assessments must be reperformed each time relevant changes to the information collected as part of the initial and ongoing due diligence are identified or any other relevant information becomes known by AXA Bank Belgium. In addition, a mandatory review of individual risk assessments must be carried out as part of the periodic review of business relationships required by section 4.3.5. of this Policy.

4.3.3. Consequences of the categorisation of a business relationship and occasional transaction into a risk category

4.3.3.1 Possibility to establish or maintain a business relationship or carry out an occasional transaction

25 With a view of complying with the risk appetite and risk tolerances defined in section 4.2.3. of this Policy, a business relationship may not be established or maintained and an occasional transaction may not be carried out when:

- the risk-based initial or ongoing due diligence measures prescribed by the present Policy and the procedures and manuals implementing have not been or could not be successfully applied it due to a lack of cooperation of the persons involved, other external factors or internal factors;
- there are clear indications that the business relationship or occasional transaction is intended to be used or is being used for the purpose of ML/FT. Notwithstanding the aforementioned, an existing business relationship may not be terminated automatically following a notification to the Financial Intelligence Unit ("CFI-CTIF") in accordance with section 4.5. of this Policy or when such termination would directly or indirectly lead to the persons becoming aware that such a notification has been made. In such as a situation, alternative measures to limit the risk must be taken;
- it is not possible to develop and implement the initial or ongoing due diligence measures that are necessary to obtain reasonable assurance that the (potential) customer involved will not use or is not using the products and services of AXA Bank Belgium to engage in ML/FT. The combination of risk factors for which this is deemed to be the case must be set out in the procedures and manuals implementing the present Policy. This will amongst others be the case in the following situations:
    - the business relationship is or would be established with or an occasional transaction would be carried out for:
        - an undertaking that is active in the diamond sector or trade;
        - a person with a managerial function at such an undertaking;
    - the business relationship is or would be established with or an occasional transaction would be carried out for a trust or similar legal structure.
- it is not possible to assess the ML/FT risk associated with the business relationship or occasional transaction in accordance with section 4.3.2. of this Policy.

For the purpose of the above, alternative restrictive measures must be applied if a termination of an existing business relationship is not possible.

The above is without prejudice to the possibility to refuse the establishment of or terminate a business relation or refuse the carrying out of an occasional transaction based on the definition of the target audience of AXA Bank Belgium.

4.3.3.2 Authorization required for the establishment or maintenance of a business relationship or the carrying out of an occasional transaction

26 A business relationship may only be established (or maintained) and an occasional transaction may only be carried out after being authorized at an hierarchical level that is commensurate with the ML/FT risk associated with the business relationship or occasional transaction. This entails that the hierarchical level at which the establishment of the business relationship or the carrying out of an occasional transaction can be authorized must be higher when the ML/FT risk associated with the business relationship or occasional transaction is higher.

The allocation of the power to authorize the establishment of a business relationship or the carrying out of an occasional transaction to a hierarchical level and individuals at such level must be adhere to the following principles:

- the power to authorize the establishment of the business relationship or the carrying out of an occasional transaction must be assigned to persons:
    - whose hierarchical level provides them with a degree of seniority that is appropriate given the impact their decision will have on the overall risk exposure of AXA Bank Belgium in the area of ML/FT;
    - that have the knowledge and expertise that is required to understand the consequence of their decision.
- the authorization of the establishment of the business relationship or the carrying out of an occasional transaction can only be performed in a decentralised manner for business relationships and occasional transactions which have a standard ML/FT risk;
- business relationships and occasional transactions involving a politically exposed person, a family member of a politically exposed person or a person known to be a close associate of a politically exposed person or with “Very High Risk” classification may only be authorized after the advice from the Anti-Money Laundering Compliance Officer has been obtained;
- business relationships and occasional transactions with a “Very High Risk” classification or that involve a politically exposed person, a family member of a politically exposed person or a person known to be a close associate of a politically exposed person (excluding business relationships and occasional transactions involving, a politically exposed person, a family member of a politically exposed person or a person known to be a close associate of a politically exposed person with a “Very High Risk” classification) may only be authorized with the approval of the Customer Acceptance and Review Committee; and
- business relationships and occasional transactions involving a politically exposed person, a family member of a politically exposed person or a person known to be a close associate of a politically exposed person with a “Very High Risk” classification may only be authorized with the approval of the Management Board of AXA Bank Belgium.

27 An existing business relationship must be re-authorized in accordance with this Policy and procedures or manuals implementing it each time there is an increase of the risk classification of a business relationship. This re-authorization must be performed in the same manner as the initial authorization using the updated individual risk assessment of the business relationship.

28 A decision not to authorize the establishment or maintenance of a business relationship or not to accept the carrying out of an occasional transaction can only be appealed in case there is new factual information that has not yet been taking into account for the performance of the individual risk assessment.

The authorization of the establishment or maintenance of a business relationship or the carrying out of an occasional transaction by another hierarchical level than the ones defined in the Policy and the procedures and manuals implementing is not allowed.

It is strictly prohibited to authorize the establishment or maintenance of a business relationship or the carrying out a business relationship that does not comply with the conditions set out in section 4.3.1. of the Policy (for example because of commercial reasons).

29 The procedures or manuals implementing the present Policy must:

- set out various hierarchical levels to which the power to authorize the establishment of business relationships or the carrying out of occasional transactions has been allocated, the criteria for determining the relevant hierarchical levels for a particular business relationship or occasional transaction and the decision flows that must followed;
- define the situations in which existing business relationships must be re-authorized; and
- the process to appeal decisions not to (re)authorize the establishment or maintenance of a business relationship or not to authorize the carrying out of an occasional transaction.

The procedures or manuals must take into account relevant regulatory or supervisory requirements and guidance as well as AXA Group and industry practices.

4.3.3.3. Extent of the initial and ongoing due diligence and monitoring that must be applied

30 The initial and ongoing due diligence described in sections 4.3.4. and 4.3.5. of this Policy must be commensurate to the ML/FT risk associated with business relationships. The same must be the case of the initial due diligence and monitoring that is performed with regard to envisaged occasional transactions.

31 (Envisaged) business relationships with a “Standard Risk” must be subjected to a basic initial and ongoing due diligence in accordance with regulatory or supervisory requirements and guidance as well as AXA Group and industry practices.

Envisaged occasional transactions with a “Standard Risk” must be subjected to a basic initial due diligence and monitoring in accordance with regulatory or supervisory requirements and guidance as well as AXA Group and industry practices.

32 (Envisaged) business relationships and occasional transactions with a “Medium Risk”, “High Risk” or “Very High Risk” classification must be subjected to an enhanced initial and ongoing due diligence in accordance with regulatory or supervisory requirements and guidance as well as AXA Group and industry practices.

Envisaged occasional transactions with a “Medium Risk”, “High Risk” or “Very High Risk” classification must be subjected to an enhanced initial due diligence and monitoring in

accordance with regulatory or supervisory requirements and guidance as well as AXA Group and industry practices.

Depending on the risk factors that have been identified, the enhanced initial and ongoing due diligence must at least include the following measures:

- verifying the customer's, authorized representative's and the beneficial owner's identity on the basis of more than one reliable and independent source and using a higher standard with regard to degree of certainty that must be obtained with regard to the identity of the persons involved;
- obtaining more information about the customer and the nature and purpose of the business relationship to build a more complete customer profile;
- increasing the frequency of transaction monitoring; and
- reviewing and, where necessary, updating information and documentation held more frequently.

4.3.4. Performance of the initial due diligence of envisaged business relationships and with regard to envisaged occasional transactions

33 AXA Bank Belgium can only effectively contribute to AML/CFT and comply with sanctions measures when it has an accurate view on who its (envisaged) customers are and for what purpose and how the customers are intending to use the products and services of the bank. To this end, an initial diligence of envisaged business relationships and with regard to envisaged occasional transactions must be carried out.

The above initial due diligence must consist of the following components:

- A risk-based identification of the customer, his authorized representative(s) (if applicable) and his beneficial owner(s) (if applicable) and verification of their identity; and
- A risk-based assessment of the characteristics of the customer and the purpose and intended nature of the business relationship or occasional transaction.

4.3.4.1. Risk-based identification of the customer, his authorized representative(s) (if applicable) and his beneficial owner(s) (if applicable) and verification of their identity

34 The identification of the customer, his authorized representative(s) (if applicable) and his beneficial owner(s) (if applicable) and the verification of their identity must consist of the following measures:

- identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
- identifying the authorised representatives of the customer that will represent him in the context of the business relationship or occasional transaction and verifying their identity on the basis of documents, data or information obtained from a reliable and independent source;
- identifying the beneficial owner and taking reasonable measures to verify that person's identity so AXA Bank Belgium is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and

similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer.

35 The extent of the above measures must be aligned with the ML/FT risk associated with the business relationship or the occasional transaction as determined by the individual risk assessment described in section 4.3.2. of this Policy.

36 The risk-based identification of the customer, his authorized representative(s) (if applicable) and his beneficial owner(s) (if applicable) and verification of their identity can only be considered as successfully completed when:

- the collected identification information is sufficient to distinguish them from any other person with reasonable certainty. The degree of certainty that must be achieved depends on the ML/FT risk associated with the business relationship or occasional transaction as determined by the individual risk assessment described in section 4.3.2. of this Policy;
- the veracity of the identification information has been confirmed using one or more reliable documents and/or information sources that are reliable and independent from the persons being identified. The degree of certainty about the veracity that must be obtained and the identification information to be verified depends on the ML/FT risk associated with the business relationship or occasional transaction as determined by the individual risk assessment described in section 4.3.2 of this Policy.

37 The procedures or manuals implementing the present Policy must define how the above risk-based identification of the customer, his authorized representative(s) (if applicable) and his beneficial owner(s) (if applicable) and verification of their identity must be carried out (incl. measures to determine, in exhaustive manner, the persons that need to be identified and the modalities for identification and identity verification).

The procedures or manuals must take into account relevant regulatory or supervisory requirements and guidance as well as AXA Group and industry practices.

4.3.4.2. Risk-based assessment of the characteristics of the customer and the purpose and intended nature of the business relationship or occasional transaction

38 The collection and verification of the identification information with regard to customers must be supplemented with the collection of information about the characteristics of customers and the purpose and intended nature of a business relationship or occasional transaction that is necessary:

- for the performance of the individual risk assessment described in section 4.3.2. of this Policy and the application of the customer acceptance policy.
- for the performance of the ongoing due diligence described in section 4.3.5 of this Policy and, in particular, for the development of a customer transaction profile.

In the context of the above, a two-pronged approach must be used to detect that a customer, an authorized representative of a customer and/or a beneficial owner of a customer is a politically exposed person, a family member of a politically exposed person or a person known to be a close associate of a politically exposed person:

- Potential customers, authorized representatives and beneficial owners must be requested to indicate whether they are a politically exposed person, a family member of a politically exposed person or a person known to be a close associate of a politically exposed person; and
- The veracity of the above declaration must be checked using a reliable and independent information source or sources.

In case there is discrepancy between the information collected from the potential customers, authorized representatives and beneficial owners and the independent information source, an assessment must be carried out to ascertain the correct status of the person involved.

39 The extent of the above measures must be aligned with the ML/FT associated with the business relationship or occasional transaction as determined by the individual risk assessment described in Section 4.3.2. of this Policy.

40 The risk-based collection of information about the characteristics of customers and the purpose and intended nature of a business relationship or occasional transaction can only be considered as successfully completed when:

- the collected information provides AXA Bank Belgium with adequate insight in the characteristics of the customer involved and the (envisaged) business relationship or occasional transaction to accurately assess the ML/FT risk involved and to be able to assess whether a transaction is atypical and/or suspicious; and
- the collected information can be deemed as reliable.

41 The procedures or manuals implementing the present Policy must define how the above risk-based collection of information about the characteristics of customers and the purpose and intended nature of a business relationship or occasional transaction must be performed (incl. which information needs be collected, from which sources this information can be obtained and when the information can be deemed to be reliable).

The procedures or manuals must take into account relevant regulatory or supervisory requirements and guidance as well as AXA Group and industry practices.

4.3.5. Performance of the ongoing due diligence of business relationships and monitoring with regard to occasional transactions

42 After the establishment of a business relationship with a customer or after the execution of an occasional transaction has been authorized, the following measures must be taken:

- risk-based ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted and his behaviour are consistent with AXA Bank Belgium's knowledge of the customer, the business and risk profile and/or not otherwise suspicious;
- risk-based periodic review and updating of due diligence collected in the context of the initial or ongoing due diligence;
- review of the individual risk assessment in case information that is relevant for the assessment has changed and re-application of the customer acceptance policy based on the outcome of the review.

In the context of the above, a two-pronged approach must be used to detect that a customer, an authorized representative of a customer and/or a beneficial owner of a customer has become politically exposed person, a family member of a politically exposed person or a person known to be a close associate of a politically exposed person:

- Customers, authorized representatives and beneficial owners must be required to notify AXA Bank Belgium when they become a politically exposed person, a family member of a politically exposed person or a person known to be a close associate of a politically exposed person after the establishment of the business relationship; and
- The compliance with the above requirement and veracity of the above information must be checked using a reliable and independent information source or sources. The customer base must be screened periodically using this information source(s).

In case:

- there is discrepancy between the information collected from the potential customers, authorized representatives and beneficial owners and the independent information source, an assessment must be carried out to ascertain the correct status of the person involved;
- it is detected that a customer, authorized representative or beneficial owner has become a politically exposed person, a family member of a politically exposed person or a person known to be a close associate of a politically exposed person after the establishment of the business relationship and this was not notified to AXA Bank Belgium, the person involved must notified thereof and his/her assumed status.

With regard to occasional transactions, the following measures must be taken:

- Inclusion of the occasional transactions in the scope of the risk-based (ongoing) monitoring of transactions and behaviour that is foreseen for business relationships while taking into account the occasional nature of the transactions;
- If a customer wishes to carry out an occasional transactions and he has already been subjected to an initial due diligence in past, this initial due diligence must be reperformed in accordance with section 4.3.4. of the Policy. The same applies for individual risk assessment.

43 The extent of the above measures must be aligned with the ML/FT risk associated with the business relationship or occasional transaction as determined by the individual risk assessment described in section 4.3.2. of this Policy.

44 The risk-based (ongoing) monitoring of business relationships and with regard to occasional transactions must consist of the following two elements:

1. a priori monitoring of business relationships and occasional transactions by the persons that are in direct contact with customers, their authorized representatives and/or, where relevant, beneficial owners or that have been tasked with the carrying out of customer transactions. To be able to effectively carry-out their monitoring duties, the aforementioned persons must be provided with adequate training and guidance.
2. a posteriori monitoring of transactions carried out on behalf of customers and of the accounts of customer held by AXA Bank Belgium.

45 The a posteriori monitoring of transactions carried out on behalf of customers and accounts of customer held by AXA Bank Belgium must at all times meet the following conditions:

- the monitoring arrangements must cover all agreements concluded by customers with or by means of the intermediation of AXA Bank Belgium, all accounts of customers held by AXA Bank Belgium and all customer transactions executed with the cooperation of AXA Bank Belgium;
- the monitoring that is performed must be based on accurate, effective and relevant scenarios for the detection of transactions and behaviour that are not consistent with AXA Bank Belgium's knowledge of the customer involved, the business and risk profile and/or otherwise suspicious ("atypical behaviour and transactions"). The detection scenarios must be based on the characteristics of the customers involved, the products and services being offered, the jurisdictions or geographical areas in which AXA Bank Belgium is active or to whom customers or transactions are linked and the channel through with services and product are provided. They must take into account the outcome of the Business-Wide Risk Assessment described in section 4.2.2. of this Policy.
- the monitoring arrangements must be able to quickly detect atypical transactions and must be automated; and
- the monitoring arrangements and their parameterisation must be subject to a formal validation and periodical review process to ensure they remain effective, accurate, relevant and appropriate for the ML/FT risk to which AXA Bank Belgium is exposed.

46 The procedures or manuals implementing the present Policy must define how the above risk-based ongoing monitoring of business relationships and occasional transactions must be performed.

The procedures or manuals must take into account relevant regulatory or supervisory requirements and guidance as well as AXA Group and industry practices.

4.3.6. Use of agents, sub-contractors and third party introducers for the performance of the initial and ongoing due diligence

47 When AXA Bank Belgium uses agents or sub-contractors for the establishment and/or for maintaining business relationships, such persons must be provided with written instructions and guidance on how to perform their assigned duties

48 AXA Bank Belgium may use third party introducers for the performance of the initial due diligence and for keeping customer due diligence information up-to-date if the following conditions are met:

- the third party introducer is an obliged entity:
  - in the sense of Law of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash; or
  - within the meaning of Article 2 of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and subject to national law transposing this Directive or third country legislation and supervision that is equivalent to the requirements under this Directive.
- the third party introducer is not established in a high-risk third country;
- the third party introducer must be contractually required to immediately submit the information on the identity of the customer and, where appropriate, of his authorized representatives and beneficial owners, as well as on the customer's characteristics and on the purpose and intended nature of the business relationship, that is necessary for the fulfilment of the due diligence requirements that have been conferred upon the third party introducer; and
- appropriate measures must be in place to enable the third party introducer to, immediately and at first request send AXA Bank Belgium a copy of the supporting documents or of the reliable sources of information it used to verify the identity of the customer and, where appropriate, of his agents and beneficial owners. The obligation to provide the aforementioned documents must be contractually agreed.

4.4. Reporting and analysis of atypical behaviour and transactions and the reporting to the Financial Intelligence Unit

4.4.1 Internal reporting of identified atypical behaviour and transactions

49 Atypical behaviour and transactions that is identified as part of the a priori monitoring of business relationship and occasional transactions or in any other context must be reported to the Anti-Money Laundering Compliance Officer without delay.

The Anti-Money Laundering Compliance Officer must also be notified when it is not possible to successfully apply the required initial and ongoing due diligence measures with regard to a business relationship or an occasional transaction.

50 The procedures or manuals implementing the present Policy must define the modalities for the above internal reporting.

4.4.2. Analysis of atypical behaviour and transactions and the reporting to the Financial Intelligence Unit

51 All atypical behaviour and transactions that have been identified and reported as part of the a priori monitoring of business relationship and occasional transactions and the ex-post monitoring of transactions or reported by any other means must be analysed in order to determine whether the behaviour or transactions can be suspected of being linked to ML/FT. This analysis must be performed under the responsibility of the Anti-Money Laundering Compliance Officer.

The outcome of the above analysis must be adequately documented in a written report.

52 All instances where it is not possible to successfully complete the required initial and ongoing due diligence due to a lack of cooperation or due to external interference must be investigated to determine whether the causes of the inability to fulfil the due diligence requirements could raise suspicions with regard to ML/FT. This analysis must be performed under the responsibility of the Anti-Money Laundering Compliance Officer.

The outcome of the above analysis must be adequately documented in a written report.

53 The Financial Intelligence Unit ("CTIF-CFI") must be informed by the Anti-Money Laundering Compliance Officer (or his delegates) immediately when AXA Bank Belgium:

- knows, suspects or has reasonable grounds to suspect that:
  - funds, regardless of the amount, are related to ML/FT;
  - transactions or attempted transactions are related to ML/FT;
- becomes aware of a fact of which it knows, is related to ML/FT.

In case of transactions, the Financial Intelligence Unit ("CTIF-CFI") must be informed before an atypical transaction is carried out unless it is not possible to inform the Unit prior to the 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. In case of the aforementioned exceptions, the Financial Intelligence Unit ("CTIF-CFI") must be informed immediately after carrying out the transaction.

If it not possible to notify Financial Intelligence Unit ("CTIF-CFI") by means of the normal procedures as set out procedures or manuals implementing the present Policy or the normal procedure is not followed, every director, employee or representative of AXA Bank Belgium that is aware of the behaviour or transaction must be notify the Financial Intelligence Unit ("CTIF-CFI").

The above reporting must be performed in accordance with the modalities determined by the Financial Intelligence Unit ("CTIF-CFI") and prescribed by the applicable legislation.

54 The procedures or manuals implementing the present Policy must define how reported atypical or suspicious behaviour and transactions must be analysed and set out the modalities for the reporting to the Financial Intelligence Unit ("CTIF-CFI").

The procedures or manuals must take into account relevant regulatory or supervisory requirements and guidance as well as AXA Group and industry practices.

4.5. Cooperation with the Financial Intelligence Unit ("CTIF-CFI"), the National Bank of Belgium and judicial authorities

55 In matters regarding ML/FT, AXA Bank Belgium must:

- cooperate with the Financial Intelligence Unit ("CTIF-CFI"), the National Bank of Belgium and judicial authorities to the extent required by the applicable legislation;
- be able to respond to valid information request from the Financial Intelligence Unit ("CTIF-CFI"), the National Bank of Belgium and judicial authorities within timeframe and via secure and confidential channels.

5. STANDARDS TO BE ADHERED TO WITH REGARD TO SANCTION COMPLIANCE

5.1. Prohibitions

56 It is prohibited to:

- engage in and/or participate in, commit, aid, abet, facilitate or counsel the carrying out of actions that constituted breaches of sanction measures ("prohibited activities"). This includes but is not limited to facilitating the provision of economic resources to persons, entities or group listed on sanction lists or facilitating the carrying out of transactions by such persons.
- carry out any activity on behalf of AXA involving the countries and regions listed in Appendix 1 of the AXA Group Sanctions Policy ("Sanctioned Countries") unless pre-approval from AXA Group Compliance was been obtained.

Breaches of the above prohibitions can result in:

- criminal and/or administrative sanctions for AXA Bank Belgium and/or the individual(s) committing the breach; and/or
- internal disciplinary and/or legal actions in accordance with the applicable contractual framework and labour regulations.

5.2. Measures to manage sanction risk

57 Adequate measures must be implemented to ensure compliance with sanctions with which AXA Bank Belgium is required to comply. These measures must at minimum include the following:

- performance and maintenance of a Business-Wide Sanction Risk Assessment;
- determination of a sanction risk appetite;
- integration of sanction risk into the customer acceptance policy; and
- integration of sanction screening and awareness into the initial and ongoing due diligence of business relationships and occasional transactions.

5.2.1. Performance and maintenance of a Business-Wide Sanction Risk Assessment

58 The objective of the Business-Wide Sanction Risk assessment to develop a thorough understanding of exposure to sanctions risk presented by the products, services and customer base of AXA Bank Belgium.

59 To achieve the above objective, the following assessment must be performed:

1. assessment of the inherent sanction risk;
2. assessment of the internal control environment (both the design and operating effectiveness);
3. determination of the residual sanction risk based on the outcome of the above assessments.

The Business-Wide Sanction Risk Assessment can be performed on a standalone basis or integrated in the Business-Wide Risk Assessment in the area of ML/FT risk described in section 4.2.2.

60 The procedures or manuals implementing the present Policy must define how the above Business-Wide Sanction Risk Assessment must be performed. These procedures or manuals must adhere to the standards and requirements set out in the below sections.

5.2.1.1 Standards with regard to the risk assessment methodology to be used for the performance of a Business-Wide Sanction Risk Assessment

61 In order to identify and assess the inherent sanction risk exposure, the assessment must at least cover the following categories:

1. risks associated with the customer base;
2. risks associated the products and services offered by AXA Bank Belgium;
3. risks associated with the countries and geographical areas within which AXA Bank Belgium or its customers do business.

The above categories must be further sub-divided into quantitative and qualitative risk factors that are derived from regulatory or supervisory requirements, guidance and supra-national and national risk assessment as well as AXA Group and industry practices. These risk factors should reflect causes or circumstances that, either on their own or in combination, may increase or decrease the sanction risk to which the AXA Bank Belgium is exposed.

62 For the purpose of the above assessment, categories and risk factors must be assigned an weight which reflects the degree to which they contribute to the sanction risk.

63 Notwithstanding the above-mentioned specificities, the assessment of the inherent sanction risk, the assessment of the internal control environment and determination of the residual sanction risk must be performed in accordance with the methodology defined for the assessment of compliance risk.

65 The Business-Wide Sanction Risk Assessment must be performed in holistic manner and cover all the activities of AXA Bank Belgium.

5.2.1.2. Monitoring and review

66 The Business-Wide Sanction Risk Assessment must at all times provide an accurate, up-to-date and relevant view of the sanction risk to which AXA Bank Belgium is exposed. To this end, the assessment as well as the underlying risk factors must be reviewed (after being performed for the first time) each year or when situations or circumstances occur which have a significant impact on the risk exposure of AXA Bank Belgium.

The above situations or circumstances include but are not limited to the following:

- significant strategy and operational changes effecting the inherent risk to which AXA Bank Belgium is exposed such as the introduction of a major new product or service, a merger or acquisition, opening a branch or subsidiary in a new location or closing a branch or subsidiary in a location, decisions to significantly grow the number of customers or accounts and changes to delivery channels;

- the imposition of sanctions with regard to jurisdictions that were not subject to sanctions before or the lifting of sanctions;
- significant internal control changes or issues affecting the residual risk to which AXA Bank Belgium is exposed such as the identification of internal control deficiencies during external/internal audits and changes in legal and regulatory requirements, supervisory expectations and/or industry practices.

5.2.1.3. Reporting and communication of the outcome of the Business-Wide Risk Assessment

67 The outcome of the Business-Wide Sanction Risk Assessment and any revision thereof must be communicated to the management of AXA Bank Belgium, business stakeholders and AXA Group. It must be approved by the Management Board.

5.2.1.4. Response to the outcome of the Business-Wide Sanction Risk Assessment

68 Appropriate remedial action must be taken when during the Business-Wide Sanction Risk Assessment:

- gaps or deficiencies in the internal control environment are identified; and/or
- when the residual sanction risk exceeds to defined risk appetite limits with regard to sanction risk.

5.2.2. Risk appetite and risk tolerances with regard to sanction risk

69 AXA Bank Belgium has a very low risk appetite related to sanctions. This entails the bank is unwilling take any action that may put in at risk of being considered to engage in and/or participate in, commit, aid, abet, facilitate or counsel the carrying out of actions that constituted breaches of sanction measures ("prohibited activities").

Based holistic and broad view on the management of the risks associated with sanctions, the following two risk tolerance must be adhered to ensure that the above risk appetite is met:

1. The sanction risk associated with the customer base

Sanction risk is the risk that customers may use the products and services of AXA Bank Belgium for the carrying out of prohibited activities.

The sanction risk associated with the customer basis in terms of aggregated residual sanction risk may not exceed:

All segments
Very Low Risk

Taking into account the nature of the sanction measures, the fact that the applicable legislation does not allow for a risk-based approach to sanction compliance and the impact of breaches of sanction measures, the residual sanction risk must be the same for all segments.

The above risk tolerance must be measured using the methodology of the Business-Wide Risk Sanction Assessment described in section 5.2.1. of this Policy. Consequently, compliance with the risk tolerance must also be monitored by means of the Business-Wide Risk Assessment.

The classification of ML/FT risk foresee in the following 5 (residual) risk levels: 1) Very Low Risk, 2) Low Risk, 3) Medium Risk, 4) High Risk and 5) Very High Risk.

2. Compliance risk in the area of sanctions

Compliance risk is the risk that a legal, administrative or regulatory sanction is imposed on an institution and/or on its staff member(s) because of the non-compliance with the legal and regulatory integrity rules and rules of conduct, resulting in a loss of reputation and a possible financial damage.

Compliance risk in the area of sanctions may not exceed Low Risk on an aggregated basis.

The above statement acknowledges that it is not possible to assert with absolute assurance that financial sanction measures will be complied with in all circumstances. This is due to the inherent limitations with regard to the effectiveness of its compliance program (such the possibility of human error) and the subject matter of "proliferation financing".

The above risk tolerance must be measured using the methodology of the Compliance Risk Assessment. Consequently, compliance with the risk tolerance must also be monitored by means of the Compliance Risk Assessment.

The classification of Compliance Risk foresee in the following 5 (residual) risk levels: 1) Low Risk, 2) Medium Risk, 3) High Risk, 4) Very High Risk and 5) Extremely High Risk.

5.2.3. Integration of sanction risk into the customer acceptance policy

70 No business relationship may be established or maintained and no occasional transaction may carried when this is prohibited by sanctions or when it is not possible to reduce the sanction risk associated with the business relationship or occasional transaction to within the risk appetite and risk tolerances with regard to sanction risk defined in section 5.2.2 of this Policy.

5.2.3. Integration of sanction screening and awareness into the initial and ongoing due diligence of business relationships and occasional transactions

5.2.3.1. Integration of sanction screening and awareness into the initial due diligence of business relationships and occasional transactions

71 Based on the information collected as part of the initial due diligence described in section 4.3.4 of this Policy and before the establishment of a business relationship or the carrying out of an occasional transaction:

- all customers, the authorized representatives of customers and the beneficial owners of customers must be screened against sanction lists related to financial sanctions in an automated manner ("Onboarding WLM Screening"); and
- it must be assessed whether the business relationship or the occasional transaction involved entails a high-risk in terms of proliferation financing and other prohibited

activities taking into account the parties involved, the activities of the customer and the geographical scope of these activities. If such high risk is present, additional information must be collected to determine whether prohibited activities might be carried out.

5.2.3.2. Integration of sanction screening and awareness into the ongoing due diligence of business relationships and occasional transactions

72 After the establishment of a business relationship and as part of the ongoing due diligence of business relationships and occasional transactions described in section 4.3.5. of this Policy, business relationships and occasional transactions must be subjected to an ongoing monitoring with a view of detecting:

- when a business relationship comes subject to financial sanctions; and
- activities prohibited by financial sanctions or that constitute proliferation financing.

73 The above ongoing monitoring of business relationships and occasional transactions must consist of the following elements:

1. a priori monitoring of business relationship and occasional transactions by the persons that are in direct contact with customers or their authorized representatives or that have been tasked with the carrying out of customer transactions with a view of identifying prohibited activities being envisaged by customers or their authorized representatives. To be able to effectively carry-out their monitoring duties, the aforementioned persons must be provided with adequate training and guidance;
2. periodic screening of customer base to verify that no customers, the authorized representatives of customers or the beneficial owners of customers have become subject to financial sanctions. This screening must at minimum be performed when a relevant sanction list is updated ("Periodic WLM Screening");
3. pre-transactional screening of the counterparties of incoming or outgoing customer transactions against financial sanction lists (insofar information about the counterparty is known) ("Transactional WLM Screening");
4. pre-transactional screening of incoming or outgoing customer transactions against financial sanction lists to verify that financial sanctions applicable to customers are being applied with ("Transactional WLM Screening"); and
5. a posteriori monitoring of the account activity of customers to detect possible proliferation financing.

In case the performance of transactional WLM Screening is not possible before the carrying of transaction due to technical reasons and the sanction risk associated with the transactions is low, the pre-transactional screening may be replaced by a post-transaction screening.

5.2.3.3. Standards to be adhered to with regard to the sanction screening and the a posteriori monitoring of transactions and business relationships

74 The a posteriori monitoring of business relationships and transactions aimed at the detection of possible proliferation financing and other prohibited activities must meet the following standards:

- it must cover the entire customer base;

- it must cover all agreements concluded by customers with or by means of the intermediation of AXA Bank Belgium, all accounts of customers held by AXA Bank Belgium and all incoming and outcoming customer transactions (incl. fund transactions and transactions in financial instruments) executed with the cooperation of AXA Bank Belgium;
- it must be performed based on accurate, effective and relevant scenarios for the detection of customer agreements and transactions and behaviour that may be indicative of proliferation financing;
- it must be able to quickly detect (possible) prohibited activities and generate alerts; and
- the parameterisation and set-up of the a posteriori monitoring must be subject to a formal validation and periodical review process to ensure they remain effective, accurate, relevant and appropriate given the sanction risk to which AXA Bank Belgium is exposed.

75 The sanction screening (a priori Onboarding WLM Screening, Periodic WLM Screening and a priori Transactional WLM Screening) must meet the following standards:

- it must cover the entire customer base (customers, their authorized representatives and their beneficial owners);
- it must be automated;
- it must cover all agreements concluded by customers with or by means of the intermediation of AXA Bank Belgium, all accounts of customers held by AXA Bank Belgium and all incoming and outcoming customer transactions (incl. fund transactions and transactions in financial instruments) executed with the cooperation of AXA Bank Belgium;
- it must be able to:
    - quickly check whether the identification information of customers, the authorized representatives of customers and the beneficial owners of customers matches with the identification information (incl. aliases) of persons, groups or entities on a relevant sanction list;
    - quickly check whether the identification information of counterparties of transactions matches with the identification information (incl. aliases) of persons, groups or entities on a relevant sanction list;
    - quickly detect assets and economic resources which are:
        - owned by persons, groups or entities on a relevant sanction list;
        - in the possession or under the control of persons, groups or entities on a relevant sanction list;
        - which are directly or indirectly being made available to persons, groups or entities on a relevant sanction list by means of transactions or otherwise.
    - generate alerts based on the above checks.
- the screening must be performed against:
    - The EU consolidated financial sanction list;

- The Belgian consolidated financial sanction list;
- The US/OFAC financial sanction lists;
- The French MINEFI Sanctions List (MINEFI List); and
- Any another list mandated by AXA Group Compliance.

- the set-up of the sanction screening must be subject to a formal validation and periodical review process to ensure they remain effective, accurate and relevant.

The above matching must be performed using the principle of "fuzzy matching". The threshold for the "fuzzy matching" must be set in accordance with relevant regulatory or supervisory requirements and guidance as well as AXA Group and industry practices.

76 The procedures or manuals implementing the present Policy must define:

- the process for the analysis, validation and periodical review of the functioning and the parameterisation of the automated sanction screening and a posteriori monitoring of business relationships and transactions; and
- the process for keeping the sanction lists used for automated sanction screening up-to-date.

The procedures or manuals must take into account relevant regulatory or supervisory requirements and guidance as well as AXA Group and industry practices.

5.3. Reporting and analysis of alerts and detected prohibited activities, the implementation of sanctions and the reporting to competent authorities.

5.3.1 Internal reporting of identified prohibited activities

77 Possible prohibited activities (in particular proliferation financing) that are identified as part of the a priori monitoring of business relationship and occasional transactions or in any other context must be reported to the Anti-Money Laundering Compliance Officer without delay.

78 The procedures or manuals implementing the present Policy must define the modalities for the above internal reporting.

5.3.2. Analysis of alerts and detected prohibited activities and the reporting to the competent authority

79 Under the responsibility of the Anti-Money Laundering Compliance Officer, an analysis must be performed of:

- all prohibited activities and transactions involving possible breaches of sanction measures identified and reported as part of the a priori monitoring of business relationship and occasional transactions and the ex-post monitoring of transactions or reported by any other means. The purpose of the analysis must be to determine whether the activities involved constitute a breach of sanctions.
- all alerts generated by the sanction screening. This analysis must determine whether the person or entity involved is indeed the person or entity subject to financial sanctions.

The outcome of the above analyses must be adequately documented in a written report.

80 In case of alerts generated in the context of pre-transactional sanction screening, the transactions or agreements involved may not be executed as long as no approval for execution has been granted by the Anti-Money Laundering Compliance Officer.

81 When it is determined that a business relationship, occasional transaction or transaction that is carried out in the context of a business relationship is subject to sanctions:

- the applicable sanction measures must be immediately applied;
- the Treasury Department of the FPS Finance (in case of financial sanctions) must be immediately informed by the Anti-Money Laundering Compliance Officer (or his delegates) and provided with all information prescribed by the applicable legal and supervisory requirements;
- AXA Group Compliance must be informed;
- review of the individual risk assessment and performance of an in-depth analysis of the relationship (including the transaction and business history) between AXA Bank and the persons involved must be performed to identify instances where funds, financial instruments and economic resources may have been made available to persons, groups or entities subject to financial sanctions or may be linked to ML/FT or proliferation financing.

When it is suspected or there are reasons to subject that a (envisaged) transaction is being linked to proliferation financing or the financing of terrorism, the Financial Intelligence Unit ("CFI-CTIF") must be immediately informed.

82 The procedures or manuals implementing the present Policy must:

- define how alerts and detected prohibited activities must be analysed;
- set out the modalities for the reporting to Treasury Department of the FPS Finance and the Financial Intelligence Unit ("CFI-CTIF"); and
- define the process for the application of sanction measures, the release of assets or transactions (incl. the use of waivers granted by Treasury Department of the FPS Finance) and the use of exceptions (such as interest payments).

The procedures or manuals must take into account relevant regulatory or supervisory requirements and guidance as well as AXA Group and industry practices.

5.4. Cooperation with the Financial Intelligence Unit ("CTIF-CFI") and the Treasury Department of the FPS Finance

83 In matters regarding sanction compliance, AXA Bank Belgium must:

- cooperate with the Financial Intelligence Unit ("CTIF-CFI") and the Treasury Department of the FPS Finance to the extent required by the applicable legislation;
- be able to respond to valid information request from the Financial Intelligence Unit ("CTIF-CFI") and the Treasury Department of the FPS Finance within the set timeframe and via secure and confidential channels.

6. STANDARDS TO BE ADHERED TO WITH REGARD TO COMPLIANCE WITH REGULATION (EU) 2015/847 OF 20 MAY 2015 ON INFORMATION ACCOMPANYING TRANSFERS OF FUNDS

6.1. Scope of application

84 The requirements set out in Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds (hereinafter "Regulation (EU) 2015/847") and the standards in this Chapter must be complied with at all times. They apply to transfers of funds, in any currency, which are sent or received by AXA Bank Belgium unless legally defined exemptions apply.

The procedures implementing the present Policy must set out which payment services and instruments offered by AXA Bank Belgium fall under the scope of requirements set out in Regulation (EU) 2015/847 and the present Standards and which are exempted from the scope.

6.2. Standards with regard to outgoing transfers of funds

6.2.1. Information that must accompany outgoing transfers of funds within the European Economic Area

85 Outgoing transfers of funds where the payment service provider of the payee is established in the European Economic Area must as a minimum contain the following information:

Information on the payer	**Information on the payee**
The account number of the payment account of the payer being debited in the IBAN format or, in the case of a transfer of funds is not made from payment account, a unique transaction identifier.	The account number of the payment account of the payee being credited in the IBAN format or, in the case of a transfer of funds is not made to a payment account, a unique transaction identifier.

86 Arrangements must be in place to make available to the payment service provider of the payee or any intervening intermediary payment service provider the below information within three working days of receiving a request to provide the information (unless the information has already been provided):

Information on the payer	**Information on the payee**
1) The full legal name of the payer 2) The payer's address, customer identification number or date and place of birth. 3) The account number of the payment account of the payer being debited in the IBAN format or, in the case of a transfer of funds is not made from payment account, a unique transaction identifier.	1) The name of the payee 2) The account number of the payment account of the payee being credited in the IBAN format or, in the case of a transfer of funds is not made to a payment account, a unique transaction identifier.

6.2.2. Information that must accompany outgoing transfers of funds to outside the European Economic Area

87 Outgoing transfers of funds where the payment service provider of the payee is established outside of the European Economic Area must always contain the following information:

Information on the payer	Information on the payee
1) The full legal name of the payer 2) The payer's address 3) The account number of the payment account of the payer being debited in the IBAN format or, in the case of a transfer of funds is not made from payment account, a unique transaction identifier.	1) The name of the payee 2) The account number of the payment account of the payee being credited in the IBAN format or, in the case of a transfer of funds is not made to a payment account, a unique transaction identifier.

88 In case of a batch file transfer from a single payer, the above standard can be complied with by including the required information in the batch file and ensuring that individual transfers carry the payment account number of the payer or the unique transaction identifier.

6.2.3. Verification of the identity information of the payer

89 With a view of complying with the standards set out in sections 6.2.1 and 6.2.2. of this Policy, the following identification information of the payer may only be included in transfers of funds or made available to the payment service provider of the payee or any intervening intermediary payment service if it has been verified in accordance with the section 4.3.4. or 4.3.5. of this Policy:

- the full legal name of the payer;
- the payer's address;
- the date and place of birth.

As the payment services and instruments offered by AXA Bank Belgium are only accessible to persons that have been accepted as customers in accordance with the customer acceptance policy referred to in section 4.3. of this Policy, the above requirement will in principle always be met.

6.2.4. Organizational requirements

90 The procedures or manuals implementing the present Policy must ensure that:

- the required information on the payee is accompanying each transfer of funds and this information is not meaningless; and
- the fields relating to the information on the payer and the payee have been filled in using characters or inputs admissible in accordance with the conventions of the messaging or payment and settlement system used to effect transfers of funds.

For the application of the above, arrangements must be in place to determine what information has to accompany outcoming transfers of funds based on their destination and the amount concerned and the type of transfer of funds involved. Derogations and exemptions may only be used when the conditions for their use are met.

91 Any staff member that detect a transfer of funds are missing the required information must immediately contact the responsible operational department and, when possible, suspend the carrying out of the transfer of funds involved.

6.3. Standards with regard to incoming transfers of funds

6.3.1. Detection of missing or incomplete information accompanying incoming transfers of funds

92 Effective monitoring arrangements must be in place to detect missing or incomplete information accompanying incoming transfers of funds. These monitoring arrangements must meet the following requirements:

- The monitoring must cover all in scope incoming transfers of funds;
- The arrangements allow for a quick detection of breaches of Regulation (EU) 2015/847 and foresee in the generation of alerts in case such breaches are detected. In particular, the arrangements must be able to detect:
    - Instances where fields relating to the information on the payer and the payee have been filled in using characters or inputs admissible that do not comply the conventions of the messaging or payment and settlement system used to effect transfers of funds ("Admissible character or inputs checks").
    - Missing and meaningless information (such a strings of random characters and designations that do not make sense) ("Missing information checks"); and
    - Incomplete information ("Incomplete information checks")
- The monitoring must be automated unless manual monitoring can be justified taking into account the nature and volume of transfers of funds. In this regard a distinction can be made between different payment flows.

For the application of the above, arrangements must be in place to determine what information has to accompany incoming transfers of funds based on their origin and the amount concerned and the type of transfer of funds involved. This determination must take into account any derogations and exemptions for which the conditions are met (incl. the detection of transfers of funds that appear to be linked and together exceed € 1.000 for incoming transfer of funds from outside the European Economic Area).

93 In addition to the above, any staff member that detects a transfer of funds are missing the required information must immediately contact the responsible operational department and, when possible, suspend the carrying out of the transfer of funds involved.

6.3.1.1. Performance of admissible character or inputs checks

94 The admissible character or inputs checks described in section 6.3.1. of this Policy must be performed before funds are credited to the account of the payee or before they are made available to the payee (if the payee does not have payment account with AXA Bank Belgium)

95 The admissible character or inputs checks must not be in place when the following conditions are met:

- AXA Bank Belgium is satisfied and can demonstrate that it understands the validations rules of the messaging or payment and settlement system being used; and
- the conventions and arrangements of the messaging or payment and settlement system being used:
    - require the completion of all of the fields necessary to obtain the information required by Regulation (EU) 2015/847;
    - automatically prevents the sending or receiving of transfers of funds where inadmissible characters or inputs are detected;
    - flags rejected transfers of funds for manual review and processing.

6.3.1.2. Performance of missing and incomplete information checks

96 The missing and incomplete information checks referred to in section 6.3.1. of this Policy must be risk-based. This entails that the manner in which the checks are performed must be commensurate with the ML/FT risk associated with the transfers of funds involved and, where relevant, the ML/FT risk associated with the business relationship with payees and the type of (occasional) transaction involved.

In application of the above, the missing and incomplete information checks must adhere to the following minimum standards:

- the checks must be performed in an ex-post or ex-ante manner. Whether an ex-post or ex-ante check needs to be performed will depend on the nature and number of risk factor that are present; and
- ex-ante checks must at a minimum be carried out when the information that must be checked is limited to the payment account number of the payer and payee and when there are specific concerns.

The above checks must be supplemented by the performance of regular sample-based ex-post checks of all processed transfers of funds.

The ML/FT risk associated with transfers of funds must be assessed based on the following risk factors:

- the ML/FT risk associated with the business relationship with the payee involved and the type of (occasional) transaction involved.
- the value of the transfer of funds and in particular whether the value is unusually large considering the average value of transfers of funds that are normally processed;
- the country or jurisdiction in which the payment service provider of the payer is based and in particular whether this is a country or jurisdiction with a high ML/FT risk.

- the AML/CFT compliance record of the intermediary payment service provider or payment service provider of the payer (whoever is the prior payment service provider in the payment chain)
- the record of compliance with Regulation (EU) 2015/847 of the intermediary payment service provider or payment service provider of the payer (whoever is the prior payment service provider in the payment chain) and in particular whether the transfer of funds is being carried out by a intermediary payment service provider or payment service provider of the payer that has been identified as repeatedly failing to provide required information on the payer without good reason or by intermediary payment service provider or payment service provider of the payer that has been previously been known to fail to provide required information on the payer or the payee on a number of occasions without good reason, even if it did not repeatedly fail to do so.
- the degree with which a transfer of funds complies with Regulation (EU) 2015/847 and in particular whether the name of the payee or payer is missing (if this information must be provided).

6.3.2. Management of transfers of funds with missing or incomplete information or inadmissible characters or inputs

6.3.2.1. Review of alerts related to missing or incomplete information or inadmissible characters or inputs

97 All alerts related to missing or incomplete information or inadmissible characters or inputs generated by the monitoring arrangements described in section 6.3.1. of this Policy must be manually reviewed to determine whether the alert is correct. This analyse must be performed under the responsibility of the Anti-Money Laundering Compliance Officer.

If based on the above review it cannot be concluded that the alert is a false positive, the alert must be reported to the Anti-Money Laundering Compliance Officer as a confirmed alert. The outcome of the review must be adequately documented in a written report.

No manual review is required when it is immediately clear that an alert is correct and this can be determined in an automated manner.

98 In case of ex-ante checks, transfers of funds which generated an alert must be suspended during the time that the alert is under review and until the Anti-Money Laundering Compliance Officer has determined which course of action to take.

99 The above review may be carried out by operational departments under the condition that any conflicts of interests that may arise are adequately managed and the persons performing the review report functionally to the Anti-Money Laundering Compliance Officer for the performance of this task.

6.3.2.2. Determination of the response to confirmed alerts

100 Situation 1: Response to confirmed alerts stemming from ex-ante checks

The Anti-Money Laundering Compliance Officer must determine whether to execute, reject or suspend a transfer of funds where ex-ante checks have detected that the required information on the payer or the payee is missing or incomplete or provided using inadmissible characters or inputs. This decision must be risk-based and at least take into account whether or not:

- the type of information missing (incl. meaningless information) or incomplete gives rise to ML/FT suspicions when taking a holistic view of ML/FT risk associated with the transfer of funds (incl. the payment service provider involved) and the occasional transaction or business relationship involved. Missing or inadmissible information may not, by itself, give rise to suspicion of ML/FT.
- the ML/FT risk associated with the transfer of funds (incl. the payment service provider involved) and the occasional transaction or business relationship involved taking into account the risk factors mentioned in section 6.3.1.2. of this Policy and the outcome of the individual risk assessment mentioned in section 4.3.2. of this Policy.

In the context of the above and for specific situations only, the Anti-Money Laundering Compliance Officer may decide to implement a pre-determined response. The implementation of such pre-determined response does not provide an derogation from the requirement to generate alerts in case of missing or incomplete information or inadmissible characters or inputs and determine whether the type of information missing (incl. meaningless information) or incomplete gives rise to ML/FT concerns.

In case a transfer of funds is rejected, the reason for the rejection must be communicated to with the prior payment service provider in the payment chain.

Compliance with Regulation (EU) 2015/84 and the AML/CFT legislation takes precedence over compliance with the national legislation transposing Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (and in particular the requirements with regard to the timeframe within which funds must credited to payee's payment account).

Situation 2: Response to confirmed alerts stemming from ex-post checks

The Anti-Money Laundering Compliance Officer must analyse whether or not the type of information missing (incl. meaningless information) or incomplete gives rise to ML/FT suspicions when taking a holistic view of ML/FT risk associated with the transfer of funds (incl. the payment service provider involved) and the occasional transaction or business relationship involved. Missing or inadmissible information may not, by itself, give rise to suspicion of ML/FT.

101 In both of the above situations 2, the prior payment service provider in the payment chain must be requested to provide the missing or complete information or provide the required information using admissible characters or input within a reasonable deadline (unless the transfer of funds is rejected). Unless in exceptional circumstances and in case of complex payment chains, the deadline may not exceed three working days for transfers of funds

taking place within the EEA and five working days for transfers of funds received from outside the EEA.

102 When requested information is not provided by the set deadline, the Anti-Money Laundering Compliance Officer must:

- decide whether to reject or execute the transfer of funds (if relevant);
- consider whether the failure of the prior payment service provider in the payment chain to supply the required information gives rise to ML/FT suspicions; and
- consider the future treatment of the prior payment service provider in the payment chain for AML/CFT compliance purposes.

103 All decisions and actions taken (incl. the reasons behind them) with regard to the above must be adequately documented and recorded in a written report.

104 In case of the type of information missing (incl. meaningless information) or incomplete information (or any other elements detected during the analysis) gives rise to ML/FT suspicions, section 4.4. of this Policy applies.

6.3.3. Identification and response to payment service providers that repeatedly fail to comply with Regulation (EU) 2015/847

6.3.3.1. Identification of payment service providers that repeatedly failing to comply with Regulation (EU) 2015/847

105 Arrangements must be implemented to identity payment service providers that repeatedly fail to comply with Regulation (EU) 2015/847 using a combination of the following quantitative and qualitative criteria:

Quantitative criteria:	**Qualitative criteria:**
a) The percentage of transfers of funds that did not include the required information sent by a specific payment service provider over a defined observation period. The length of this observation period should be defined in function of the number and frequency of transfers of funds that are received from the payment service provider involved b) the percentage of follow-up requests that were left unanswered or were not adequately answered within by a certain deadline.	a) The level of cooperation of the payment service provider involved relating to previous requests to provide the required information; b) The type information that is missing.

6.3.3.2. Response to a payment service provider being identified as repeatedly failing to comply with Regulation (EU) 2015/847

106 Once a payment service provider has been identified as repeatedly failing to comply with Regulation (EU) 2015/847, the following steps must be taken:

- the National Bank of Belgium must notified thereof without undue delay and no later than three months after identifying the repeatedly failing payment service provider;
- implementation of appropriate measures to limit the ML/FT generated by the repeatedly failing payment service provider by the Anti-Money Laundering Compliance Officer. If the implementation of such measures is not possible, any future transfer of funds from the payment service provider involved must be rejected and any business relationship with them terminated.

6.3.4. Organizational requirements

107 The procedures or manuals implementing the present Policy must define:

- the process that must be followed in terms of analysis, decision making, management and reporting with regard to transfers of funds with missing or incomplete information or inadmissible characters or inputs
- the process for the detection of payment service providers that repeatedly failing to comply with Regulation (EU) 2015/847 and decision making process for the determining the response to payment service provider being identified as repeatedly failing to comply with Regulation (EU) 2015/847.

For the application of the above, arrangements must be in place to determine what information has to accompany outcoming transfers of funds based on their destination and the amount concerned and the type of transfer of funds involved. Derogations and exemptions may only be used when the conditions for their use are met.

7. ORGANISATIONAL REQUIREMENTS

7.1. Governance

108 To be able to effectively contribute to AML/CFT and ensure compliance with sanctions, appropriate and effective governance arrangements for the application and implementation of the present Policy must be in place. These arrangements must adhere to standards set out in the present section

7.1.1. Appointment of a member of senior management that is responsible for AML/CFT and an Anti-Money laundering Compliance Officer

7.1.1.1. Appointment of a member of senior management that is responsible for AML/CFT

109 A member of the Management Board of AXA Bank Belgium must be designated as being responsible for ("the member of senior management that is responsible for AML/CFT")

- ensuring the internal control measures (incl. policies and procedures) in the area of AML/CFT and sanction compliance are adequate and proportionate, taking into the ML/FT risk and sanction risk to which AXA Bank Belgium is exposed;
- ensuring that the Anti-Money laundering Compliance Officer 1) has access to all the necessary information for the carrying out of his duties, 2) has the necessary tools and resources to carry out his duties in an effective manner and 3) is adequately informed of any gaps or deficiencies that are found with regard to compliance with regulatory and supervisory requirements with regard to the prevention of the use of the financial system for money laundering and financing of terrorism.

The above member must meet the following conditions:

- he or she must be fit & proper and have the necessary knowledge in the area of AML/CFT and sanction compliance to be able to assess and challenge the measures being taken by the Anti-Money Laundering Compliance Officer and the operational departments;
- he or she does not have any other responsibilities which could conflict with the responsibility for ensuring compliance with the AML/CFT legislation.

Taking into account the above, AXA Bank Belgium has designated the Chief Risk Officer as the member of senior management that is responsible for AML/CFT.

7.1.1.2. Appointment of an Anti-Money laundering Compliance Officer

110 There must be a permanent and independent Anti-Money laundering Compliance Function consisting of one or more Anti-Money laundering Compliance Officers.

To be able to be appointed as Anti-Money laundering Compliance Officers, a person must meet the following conditions:

- he must be fit & proper and have the necessary knowledge in the area of AML/CFT and sanction compliance to be able to carry out the function of Anti-Money laundering Compliance Officer;

- he must be part of the Compliance Function;
- he must be able to allocate sufficient time to the carrying out of the duties of Anti-Money laundering Compliance Officer.

The Anti-Money laundering Compliance Officer is responsible for:

- the development and implementation of policies, procedures and internal control measures to ensure compliance with the AM/CFT legislation, the legislation on information accompanying transfers of funds, sanctions and AXA Group Standards (insofar they are compatible with the applicable legal requirements);
- the analysis of atypical transactions and behaviour, instances where the required initial and ongoing due diligence cannot be successfully completed, alerts generated by the automated sanction screening and alerts with regard to breaches of Regulation (EU) 2015/847;
- ensuring the application of sanction measures and notifying the Treasury Department of the FPS Finance thereof;
- the identification and measurement of the ML/FT risk (and sanctions risk) to which the AXA Bank Belgium is exposed;
- deciding whether to notify behaviour or transactions to the Financial Intelligence Unit ("CFI-CTIF");
- deciding action that will be taken:
    - in case checks have detected that the required information on the payer or the payee is missing or incomplete or provided using inadmissible characters or inputs;
    - in case of a payment service provider has been identified as repeatedly failing to comply with Regulation (EU) 2015/847;
- awareness creation and the provision of tailored AML/CFT training and sanction compliance;
- the development and execution of an annual compliance monitoring plan to verify compliance with the applicable policies and procedures in the area of AML/CFT, the information accompanying transfers of funds and sanction compliance at the level of staff members and tied agents of AXA Bank Belgium;
- management and supervisory reporting (incl. the drafting and submission of an annual Anti-Money Laundering Report);
- serving the point of contact for the Financial Intelligence Unit ("CFI-CTIF") and the Treasury Department of the FPS Finance thereof.

111 The Anti-Money laundering Compliance Officer:

- must have the necessary tools and resources to carry out his/her duties in an effective manner; and
- must have the authority to propose to the Board of Directors and the Management Board of AXA Bank Belgium, at his or her own initiative, all measures which are necessary or useful for ensuring that the internal control measures in the area of AML/CFT and the financing of terrorism and sanction compliance are effective.

7.1.2. Responsibilities of the Board of Directors of AXA Bank Belgium

112 In the area of AML/CFT and sanction compliance, the Board of Director of AXA Bank Belgium has the following responsibilities:

- determination of the general strategy of AXA Bank Belgium with regard to the management of ML/FT risk and sanction risk (incl. the risk appetite limits);
- approval of amendments of the present Policy;
- approval of the annual activity report of Anti-Money Laundering Reporting Officer; and
- annual assessment of the effectiveness of the Compliance Function (incl. its activities in the area of AML/CFT and sanction compliance and whether the Anti-Money Laundering Reporting Officer is fit and proper)

7.1.3. Responsibilities of the Management Board of AXA Bank Belgium

113 In the area of AML/CFT and sanction compliance, the Management Board of AXA Bank Belgium has the following responsibilities:

- development and implementation, under the direction of the member of senior management that is responsible for AML/CFT, of the necessary organisation and operational measures (incl. internal control measures) to:
  - comply the AML/CFT legislation, the legislation on information accompanying transfers of funds, sanctions and AXA Group Standards (insofar they are compatible with the applicable legal requirements); and
  - implement the general strategy of AXA Bank Belgium with regard to the management of ML/FT risk and sanction risk.
- approval of procedures and manuals implementing the present Policy. Minor changes of the procedures and manuals can be approved by the member of senior management that is responsible for AML/CFT.
- approval of the annual activity report of Anti-Money Laundering Reporting Officer;
- annual assessment of the effectiveness of the governance and internal control measures (incl. the present Policy) as part of the annual general assessment of the effectiveness of the internal control measures;
- ensuring adequate reporting to Board of Director, AXA Group and the National Bank of Belgium.

7.1.4. Responsibilities of the management of the operational departments, staff members and tied agents

114 Under the responsibility and at the direction of the Management Board and with the support of the Anti-Money laundering Compliance Officer, the management of the operational departments must develop and implement the necessary procedures and internal control measures:

- to comply with the AML/CFT legislation, the legislation on information accompanying transfers of funds, sanctions and AXA Group Standards (insofar they are compatible with the applicable legal requirements); and

- to implement the present Policy in accordance with the standard set out therein.

The above procedures and internal control measures must be proportionate to the size, the nature of the activities and the ML/FT and sanction risk to which AXA Bank Belgium is exposed.

115 Staff members (incl. contractors), tied agents and employees of tied agents of AXA Bank Belgium are required to comply with the present Policy and the above internal control measures to the extent that they are relevant for the carrying out of their assigned duties.

7.2. Training and awareness

116 Mandatory ongoing training programmes must be implemented to ensure that staff members and tied agents are at all times:

- adequately trained to implement the present Policy and the procedures and manuals implementing it taking into account their assigned responsibilities;
- have an appropriate knowledge of Belgian AML/CFT legislation and sanction legislation.

The above mentioned training programmes must meet the following conditions:

- the training programmes must cover all staff members and tied agents that are involved in the management of ML/FT risk and sanction risk;
- the trainings and materials must be tailored to specific responsibilities and tasks of the staff members and tied agents that will be receiving them;
- the training programme must foresee in mandatory training for new staff members and tied agents;
- the training programmes must be periodically reviewed and remain up-to-date. Such a review must at least be carried out in case of changes to internal process and controls and changes in legal and regulatory requirements, supervisory expectations, guidance (incl. typologies and/or industry practices.
- the training programmes must foresee in mandatory refresher training to ensure that staff members and tied agents are reminded of their obligations and their knowledge and expertise are kept up to date. The scope and frequency of such training must be tailored to the risk factors to which staff members and tied agents are exposed due to their responsibilities and the level and nature of risk present at the level of AXA Bank Belgium.

117 Mandatory ongoing training programmes must be supplemented by measures to create general and ongoing awareness about ML/FT and the need for sanction compliance and ML/FT risk and sanction risks to which AXA Bank Belgium is exposed.

7.3. Internal whistleblowing

118 Arrangements must be implemented that allow staff members and tied agents to report breaches of the AML/CFT legislation and sanction legislation and/or the present Policy and the procedures and manuals implementing it through a specific, independent and anonymous channel to the Anti-Money Laundering Compliance Officer and the member of senior management that is responsible for AML/CFT.

119 Staff members and tied agents making use of the above reporting channel or otherwise report breaches of the AML/CFT legislation and sanction legislation and/or the present Policy and the procedures and manuals implementing it must protected from being exposed to threats or hostile action, and in particular from adverse or discriminatory employment actions.

7.4. External whistleblowing

120 Members of the management , staff members (incl. contractors), tied agents and employees of tied agents of AXA Bank Belgium have the possibility to report **b**reaches of the Law of 18 September 2017 on the prevention of money laundering and the financing of terrorism and on the limitation of the use of cash **(and its implementation legislation)**, EU Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds implementation legislation **(and its implementation legislation)** and **sanction measures by AXA Bank Belgium to the National Bank of Belgium**.

Breaches can be reported via the following website: **https://www.nbb.be/nl/financieel-toezicht/algemeen/een-inbreuk-melden, https://www.nbb.be/fr/supervision-financiere/generalites/signaler-une-infraction or https://www.nbb.be/en/financial-oversight/general/report-breach.**

7.5. Fit & proper in the area of ML/FT and sanctions

121 No relationship may be established and maintained with (potential) members of the management , staff members (incl. contractors), tied agents and employees of tied agents and vendors that are suspected of ML/TF and/or subject to financial sanctions.

To this end, the following standards must be adhered to:

- performance of an appropriate ML/FT and sanction due diligence before the establishment of the relationship by means of adverse information and sanction checks. The extent of this due diligence must take into account the tasks and duties that will be assigned to the persons involved or the services or products that will be provided.
- in case of ongoing relationships members of the management , staff members (incl. contractors), tied agents and employees of tied agents and vendors must be periodical screened against sanction list and periodical adverse information checks must be performed. Any hits must immediately be reported to the Anti-Money Laundering Compliance Officer;
- decisions with regard to termination of a relationship based on adverse ML/FT-related information and the applicability of sanction are to be taken at an appropriate hierarchical level in accordance with assigned business responsibilities following the provision of an advice by the Anti-Money Laundering Compliance Officer.

.

8. STANDARDS TO BE ADHERED TO WITH REGARD TO RECORDKEEPING

122 Arrangements must be implemented that ensure the appropriate records of the information and documents collected, obtained or generated in the context of business relationships, the execution of (occasional) transactions (incl. transfers of funds), the analysis of atypical transactions or behaviour and alerts generated automated monitoring and screening systems, any decisions taken based on this analysis, and the setup of automated monitoring and screening systems is retained for the period and in the manner required by legal and regulatory requirements in the area of AML/CFT and sanction legislation.

The above information and direction must be delete the end of the legally required retention period unless any other any other applicable legislation requires that document to be held for a longer period.

123 The procedures or manuals implementing the present Policy must set out:

- the list of information and documents that must be retained and the required retention period (incl. the starting date of this period);
- the rules that must be adhered to safeguard the confidentiality of the information;
- the modalities for deleting information and documents at the end of the retention period.

9. STANDARDS TO BE ADHERED TO WITH REGARD TO REPORTING TO NATIONAL BANK OF BELGIUM AND THE AXA GROUP

124 The requirements for reporting to the National Bank of Belgium in the area of AML/CFT must be complied with.

125 The requirements for reporting to AXA Group in the area of AML/CFT and sanction compliance must be complied with.