



***Politiques Générales sur la Gestion du Risque de
Blanchiment de Capitaux et de Financement du
Terrorisme***

Février 2021

GROUPE NOVO BANCO

TABLE DES MATIÈRES :

1. OBJECTIFS	4
2. ACRONYMES.....	4
3. CADRE JURIDIQUE ET RÉGLEMENTAIRE.....	5
3.1. INFORMATION INSTITUTIONNELLE.....	5
3.2. NORMES ET RECOMMANDATIONS INTERNATIONALES.....	6
3.3. LÉGISLATION ET RÉGLEMENTATION PORTUGAISES.....	7
3.4. NORMES RÉGLEMENTAIRES DES AUTORITÉS SECTORIELLES.....	9
4. MODÈLE DE RISQUE.....	12
4.1. ÉVALUATION DES RISQUES DE COMPLIANCE – RISK ASSESSMENT	13
5. POLITIQUE D'ACCEPTATION DES CLIENTS.....	13
6. PROCESSUS ET CONTRÔLES QUI ATTÉNUENT LES FACTEURS DE RISQUE (BCFT).....	14
6.1. KNOW YOUR CUSTOMER (KYC) – ANALYSE DES CONTREPARTIES (OUVERTURE DE COMPTE, GESTION DES PARTICIPATIONS, ÉVALUATION DES CONTREPARTIES ET RMA'S).....	14
6.1.1. FACTEURS ET TYPES DE RISQUES POTENTIELLEMENT PLUS ÉLEVÉS.....	15
6.2. FINANCEMENT DU TERRORISME	15
6.3. RELATIONS DE CORRESPONDANT BANCAIRE.....	16
6.4. PROPRES TRANSACTIONS	17
6.5. PERSONNES POLITIQUEMENT EXPOSÉES (PEP'S), MEMBRES DE LA FAMILLE ET ASSOCIÉS DE PEP'S, ET AUTRES TITULAIRES DE FONCTIONS POLITIQUES OU PUBLIQUES (OTCPP)	18
6.6. ÉVALUATION DU RISQUE CLIENT ET MODÈLES DE SCORING.....	19
6.7. MISE À JOUR DES INFORMATIONS	20
6.8. KNOW YOUR TRANSACTION (KYT) – MONITORING	20
6.9. SIGNALEMENT DES TRANSACTIONS SUSPECTES (SAR'S)	21
6.10. COOPÉRATION AVEC LES AUTORITÉS	21
6.11. KNOW YOUR PROCESS (KYP)	22
6.11.1. GESTION DU MODÈLE DE RISQUE.....	22
6.11.2. HIGH RISK CUSTOMERS	22
6.11.3. EXAMEN DU RISQUE DE COMPLIANCE	22
6.11.4. FERMETURE DE COMPTES À LA DEMANDE DU SERVICE DE LA COMPLIANCE.....	22
6.12. APPROBATION DE NOUVEAUX PRODUITS ET SERVICES - PROCESSUS DE SIGN-OFF	23
6.13. JURIDICTIONS À RISQUE ÉLEVÉ	23
7. SYSTÈME DE SANCTIONS ET DE MESURES RESTRICTIVES - FILTERING	24
7.1. WOLFSBERG AML QUESTIONNAIRE	24
7.2. USA PATRIOT ACT CERTIFICATE	25
8. FORMATION.....	25
9. CODE DE CONDUITE, POLITIQUE EN MATIÈRE DE CONFLITS D'INTÉRÊTS, DE PARTIES LIÉES ET DE LUTTE CONTRE LA CORRUPTION - POLITIQUE DE WHISTLEBLOWING,	26
10. SUIVI DES SUCCURSALES ET DES FILIALES	26
10.1. APPLICATION AUX ENTITÉS DU GROUPE NOVO BANCO	27
10.2. MODÈLES D'ARTICULATION.	27
11. CONSERVATION D'INFORMATIONS.....	27
12. PROTECTION DE DONNÉES.....	27
13. CONTRÔLE INTERNE ET AUDITS (INTERNES ET EXTERNES)	28
14. PARTICIPATION À DES GROUPES DE TRAVAIL SECTORIELS.....	28

15. PROJETS STRATÉGIQUES DU GNB	28
15.1. PROJET DE LA BANQUE DIGITALE.....	28
15.2. PROJET TALENT AND MERIT 2018-2021	29
15.3. PROJET APIC	29
16. ANALYSE CRITIQUE DU MODÈLE BC/FT MIS EN ŒUVRE – OBJECTIFS POUR L'AVENIR	30
17. RISQUES GÉNÉRAUX LIÉS AUX MOUVEMENTS DE TRÉSORERIE.....	30
18. DEVOIRS PRÉVENTIFS DU BCFT – BANQUE ET COLLABORATEURS	31
18.1. DEVOIR DE CONTRÔLE.....	31
18.2. DEVOIR D'IDENTIFICATION ET DE VIGILANCE.....	31
18.3. DEVOIR DE COMMUNICATION.....	31
18.4. DEVOIR D'ABSTENTION.....	31
18.5. DEVOIR DE REFUS.....	32
18.6. DEVOIR DE CONSERVATION.....	32
18.7. DEVOIR D'EXAMEN.....	32
18.8. DEVOIR DE COLLABORATION.....	33
18.9. DEVOIR DE NON-DIVULGATION.....	33
18.10. DEVOIR DE FORMATION.....	33
19. GESTION DU DOCUMENT	33
19.1. PROPRIÉTÉ, INTERPRÉTATION, VALIDITÉ ET RÉVISION PÉRIODIQUE.....	33
19.2. GESTION DES DOCUMENTS CONNEXES.....	33

ANNEXES

A. LISTE DES PAYS NON-COOPÉRANTS PUBLIÉE PAR LE FATF/GAF.....	35
B. PAYS TIERS PRÉSENTANT DES DÉFICIENCES STRATÉGIQUES EN DANS LE CADRE DE BC/FT, JURIDICTIONS FISCALES NON COOPÉRATIVES ET ORDRES JURIDIQUES OFFSHORE.....	36
C. LISTE DES PERSONNES POLITIQUEMENT EXPOSÉES (PEP'S) ET LISTE DES TITULAIRES D'AUTRES FONCTIONS POLITIQUES ET PUBLIQUES	40
D. ANNEXE III DE LA LOI N° 83/2017, DU 18 AOÛT - LISTE NON EXHAUSTIVE DES FACTEURS ET TYPES INDICATIFS DE RISQUE POTENTIELLEMENT PLUS ÉLEVÉ, EN COMPLÉMENT DES SITUATIONS SPÉCIFIQUEMENT PRÉVUES PAR LA LOI	42

1. OBJECTIFS

Le présent document vise :

- Présenter une vision intégrée des Politiques Générales sur la Gestion des Risques de Blanchiment de Capitaux et de Financement du Terrorisme ;
- Établir les principes directeurs, les paramètres d'action et de diligence à adopter par les entités du Groupe NOVO BANCO (GNB) en matière de prévention, de détection, de gestion et d'atténuation des risques de blanchiment de capitaux et de financement du terrorisme, ainsi que pour le respect effectif des mesures restrictives et des sanctions internationales ;
- Garantir le respect des exigences légales et réglementaires applicables dans le cadre de la Prévention du Blanchiment de Capitaux et du Financement du Terrorisme ;
- Protéger NOVO BANCO (NB) et le groupe NOVO BANCO (GNB) de l'exposition à des situations comportant un risque potentiel de constituer un délit de Blanchiment de Capitaux et/ou de Financement du Terrorisme ;
- Définir les vecteurs d'action du modèle de Gestion du risque adopté dans ce domaine, en fonction des exercices spécifiques d'Évaluation du Risque (*Risk Assessment*) sur la prévention du Blanchiment de Capitaux et du Financement du Terrorisme.

Ce document s'applique à NOVO BANCO S.A. - Succursale de Luxembourg

2. ACRONYMES

Acronyme	Définition
AML	Anti-Money Laundering
BCFT	Blanchiment de Capitaux et Financement du Terrorisme
BdP	Banque du Portugal
CDD	Customer Due Diligence
CSSF	Commission de Surveillance du Secteur Financier
CRF	Cellule de Renseignement Financier
DCIAP	Departamento Central de Investigação e Ação Penal, da Procuradoria-Geral da República
DOF	Déclaration d'Origine des Fonds
EDD	Enhanced Due Diligence

FATF/GAFI	Financial Action Task Force / Grupo de Ação Financeira Internacional
GNB	Groupe Novo Banco
HRC	High Risk Customers
KYC	Know Your Customer
KYP	Know Your Process
KYT	Know Your Transaction
NB	NOVO BANCO
NBL	NOVO BANCO – Succursale de Luxembourg
OTCPP	Autres Titulaires d’Autres Fonctions Politiques ou Publiques
PBCFT	Prévention du Blanchiment de Capitaux et de Financement du Terrorisme
PEP	Personne Politiquement Exposée
RCBE	Registre Central des Bénéficiaires Effectifs
RBA	Risk Based Approach
SLA	Service Level Agreement
UBO	Ultimate Beneficial Owner
UIF	Unité d’Intelligence Financière de la Police Judiciaire
RMA	Relationship Management Application de la SWIFT

3. CADRE JURIDIQUE ET RÉGLEMENTAIRE

3.1. INFORMATION INSTITUTIONNELLE

- **Dénomination** : NOVO BANCO, S.A.
- **Adresse** : Avenida da Liberdade, nº 195, 1250-142 Lisbonne, Portugal
- **Code SWIFT** : BESCPTPL
- **Nature juridique** : Société anonyme
- **Nº de Personne Morale et Registre au C.R.C. de Lisbonne** : 513 204 016
- **Adresse électronique** : www.novobanco.pt
- **Organes de la société** : www.novobanco.pt (Homepage Institucional> NOVO BANCO> Governance> Órgãos Sociais)

- **Présence internationale** : www.novobanco.pt (*Home> Para si> Informação útil> Contactos> Rede de Agências> Balcões> Presença Internacional*)
- **Capital social** : € 5.900.000.000,00
- **Actionnaires** : Nani Holdings, SGPS, S.A. (75%) e Fundo de Resolução (Pessoa Coletiva de Direito Público (25%)
- <http://www.fundoderesolucao.pt/pt-PT/ofundo/Paginas/OFundo.aspx>)
- **Entités de Surveillance Sectorielle** : Banque Centrale Européenne (www.ecbc.europa.eu), Banque du Portugal (www.bportugal.pt), Commission des Opérations de Bourse (www.cmvm.pt), et Autorité de Surveillance des Assurances et des Fonds de Pension (www.asf.com.pt).
- **Auditeurs Externes** : EY – Ernst & Young Audit & Associados – SROC, S.A.
- **Contact** : *Chief Compliance Officer* – Département de Compliance
- **Adresse** : Avenida da Liberdade, n° 195, 1250-142 Lisbonne, Portugal
- **Tel.**: (+351) 213 804 536 / **Fax**: (+351) 213 804 581
- **E-mail**: compliance@novobanco.pt

SUCCURSALE DU LUXEMBOURG

- **Dénomination** : NOVO BANCO, S.A. - *Succursale Luxembourg*
- **Adresse** : 1, rue Schiller L - 2519 Luxembourg
- **Code SWIFT** : BESCLULL
- **Nature juridique** : Société anonyme
- **N° de Personne morale** : **B190974**
- **Adresse électronique** : www.novobancoluxembourg.lu
- **Entités de Surveillance Sectorielle** : CSSF
- **Contact** : Compliance Officer – Département de Compliance
- **Tel.**: (+352) 27 36 25 16 / **Fax**: (+352) 27 36 25 12
- **E-mail**: compliance@novobancoluxembourg.lu

3.2. NORMES ET RECOMMANDATIONS INTERNATIONALES

GNB respecte et se conforme aux cadres législatifs et réglementaires européens et aux normes nationales sur les PBC/FT, en mettant en œuvre et en opérationnalisant les exigences légales et réglementaires correspondantes.

- **Directive (UE) 2015/849 du Parlement Européen et du Conseil du 20 mai 2015**, relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme.
- **Directive (UE) 2018/843 du Parlement Européen et du Conseil, du 30 mai**, modifiant la directive (UE) 2015/849 du 20 mai relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, et modifiant les directives 2009/138/CE et 2013/36/UE.

- **Directive (UE) 2018/1673 du Parlement Européen et du Conseil, du 23 octobre** relative à la lutte contre le Blanchiment de Capitaux au moyen du Droit Pénal les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive au plus tard le 3 décembre 2020.
- **Directive (UE) 2016/2258 du Conseil, du 6 décembre 2016**, modifiant la directive 2011/16/UE concernant l'accès des autorités fiscales aux informations relatives à la lutte contre le blanchiment de capitaux.
- **Règlement (UE) 2015/847 du Parlement Européen et du Conseil, du 20 mai 2015**, établissant des règles relatives aux informations sur le donneur d'ordre et le bénéficiaire devant accompagner les virements de fonds, dans quelque monnaie que ce soit, à des fins de prévention et de détection et d'enquête en matière de blanchiment de capitaux et de financement du terrorisme..
- **Règlement (UE) 2018/1672 du Parlement Européen et du Conseil, du 23 octobre 2018**, relatif aux contrôles de l'argent liquide entrant ou sortant de l'Union européenne.
- **Règlement Délégué (UE) 2016/1675 de la Commission du 14 juillet 2016**, complétant la directive (UE) 2015/849 du Parlement européen et du Conseil en identifiant les pays tiers à haut risque présentant des déficiences stratégiques.
- **Règlement Délégué (EU) 2019/758 de la Commission du 31 janvier 2019**, complétant la directive (UE) 2015/849 du Parlement européen et du Conseil en ce qui concerne les normes techniques régissant les mesures minimales et le type de mesures supplémentaires que les établissements de crédit et les institutions financières doivent prendre pour atténuer le risque de blanchiment de capitaux et de financement du terrorisme dans certains pays tiers.
- **40 Recommandations du FATF/GAFI**, sur le blanchiment de capitaux et le financement du terrorisme, datant de 1990, révisée en 1996, 2003, 2004 et 2012, intégrant dans la dernière révision les 9 recommandations sur le financement du terrorisme, considérées comme des normes internationales en la matière, dans l'évaluation mutuelle du degré de respect de ces normes par les membres respectifs, ainsi que dans l'identification de nouveaux risques et de nouvelles méthodologies de lutte contre les activités criminelles¹.
- **Principes AML (Anti-Money Laundering) du Groupe Wolfsberg²**

3.3. LÉGISLATION ET RÉGLEMENTATION PORTUGAISES

¹ Le Portugal et le Luxembourg sont membres du GAFI depuis 1990

² Le Groupe *Wolfsberg* est composé de quelques-unes des principales institutions financières internationales : Banco Santander, Bank of America, Bank of Tokyo – Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale, Standard Chartered Bank e UBS.

- **Loi n° 58/2020, du 31 août, transpose la Directive (UE) n° 2018/843, relative à la prévention du Système Financier aux fins du blanchiment de capitaux et du financement du terrorisme et la Directive UE n.° 2018/1673, relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme par le biais du Droit Pénal.** Il introduit plusieurs modifications pour se conformer aux diplômes juridiques en la matière, à savoir la **loi n° 83/2017 et la loi n° 89/2017**, révisant également la **loi n° 97/2017** et le cadre pénal prévu à **l'article 368-A du Code Pénal -Décret-loi 400/82**, tous énumérés ci-dessous.
- **Loi n° 83/2017, du 18 août**, qui établit des mesures de nature préventive et répressive pour lutter contre le blanchiment de capitaux et le financement du terrorisme. Transpose partiellement la Directive 2015/849/UE, du Parlement européen et du Conseil, du 20 mai 2015, et la Directive 2016/2258/UE, du Conseil, du 6 décembre 2016, modifie le Code Pénal et le Code de la Propriété Industrielle et abroge la loi n° 25/2018, du 5 juin, et le décret-loi n° 125/2008, du 21 juillet.
- **Loi n° 89/2017, du 21 août**, qui approuve le Cadre Juridique pour le Registre Central des Bénéficiaires Effectifs - RCBE. Transpose le chapitre III de la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 et modifie les codes et autres actes juridiques.
- **Loi n° 97/2017, du 23 août**, sur la mise en œuvre et l'application des mesures restrictives adoptées par les Nations unies ou l'Union européenne et sur les sanctions applicables en cas de violation de ces mesures.
- **Loi n° 92/2017, du 22 août**, sur l'obligation d'utiliser un moyen de paiement spécifique dans les transactions portant sur des montants égaux ou supérieurs à 3 000,00 euros, modifiant la loi fiscale générale et la loi générale sur les infractions fiscales.
- **Loi n° 52/2003, du 22 août**, qui approuve la loi sur la lutte contre le terrorisme, modifiée par les lois n° 59/2007 du 4 septembre, n° 25/2008 du 5 juin, n° 17/2011 du 3 mai, n° 60/2015 du 24 juin et n° 16/2019 du 14 février.
- **Loi n° 52/2019, du 31 juillet**, qui approuve le régime d'exercice des fonctions des titulaires de mandats politiques et des hauts fonctionnaires.
- **Loi n° 5/2002, du 11 janvier, et ses modifications ultérieures et ses modifications ultérieures** établissent des mesures de lutte contre la criminalité organisée et la criminalité économique-financière. Elle prévoit un système spécial de collecte de preuves, de violation du secret professionnel et de confiscation des biens au profit de l'État en ce qui concerne divers types de délits, notamment le blanchiment de capitaux et la contrefaçon de monnaie et de titres équivalents à la monnaie.
- **Loi n° 15/2017, du 3 mai** - Interdit l'émission de titres au porteur.
- **Code Pénal – article 368. - A – Blanchiment** - sur la définition du crime de blanchiment de capitaux.
- **Décret-loi n° 61/2007, du 14 mars**, approuvant le cadre juridique applicable au contrôle de l'argent liquide transporté par les personnes physiques entrant ou sortant de l'UE par le territoire national et au contrôle des mouvements d'argent liquide avec les autres États membres de l'UE.

- **Décret-loi n° 123/2017, du 25 septembre**, établissant le régime de conversion des valeurs mobilières au porteur en valeurs nominatives, en application de la loi n° 15/2017, du 3 mai.
- **Arrêté n° 233/2018, du 21 août**, qui régit le régime juridique du Registre central des bénéficiaires effectifs (RCBE), conformément aux articles 22 et 23 de la loi n° 89/2017, du 21 août. Le régime juridique de la RCBE est prévu à l'article 34 de la loi 83/2017, du 18 août. "**Déclaration de rectification n° 33/2018 " respective. (D.R., 1^{ère} série - n° 194 - 9 octobre 2018)**", qui publie les modifications apportées à l'arrêté n° 233/2018, du 21 août, en ce qui concerne l'article 14, paragraphe 1, et l'article 17, paragraphe 1.
- **Arrêté n° 200/2019, du 28 juin**, fixant les délais de déclaration initiale du RCBE, et abrogeant les articles 13 à 17 de l'arrêté n° 233/2018 du 21 août.
Arrêté n° 310/2018, du 4 décembre, qui définit les types d'opérations, comportant des risques, à communiquer systématiquement au DCIAP (Département Central d'Investigation et d'Action Pénale du Bureau du Procureur Général) et à la UIF (Unité d'Intelligence Financière de la Police Judiciaire), et régleme la forme et les termes de ces communications.
- **Arrêté n° 150/2004, du 13 février** - Approuve la liste des pays, territoires et régions ayant des régimes fiscaux privilégiés nettement plus favorables (diplôme repris par l'article 290 de la loi n° 114/2017, du 29 décembre).
- **Arrêté n° 345-A/2016, du 30 décembre**, modifiant l'arrêté ministériel n°150/2004 établissant la liste des pays, territoires et régions à régime fiscal préférentiel.
- **Résolution du Conseil des ministres n° 88/2015, du 1^{er} octobre**, qui crée la Commission de coordination des politiques de PCBCFT.

3.4. NORMES RÉGLEMENTAIRES DES AUTORITÉS SECTORIELLES

- **Notification de la Banque du Portugal n° 2/2018, du 26 septembre**, qui régleme l'application des textes suivants : i) loi n° 83/2017 du 18 août ; ii) loi n° 97/2017 du 23 août. Abroge la notification de la Banque du Portugal n° 5/2013, du 18 décembre, qui comprenait des modifications introduites par la notification de la Banque du Portugal n° 1/2014, du 28 février.

La présente Notification régit :

- i) les conditions d'exercice, les procédures, les instruments, les mécanismes, les formalités d'application, les devoirs de déclaration et les autres aspects nécessaires pour assurer le respect des devoirs de prévention du blanchiment de capitaux et du financement du terrorisme, dans le cadre de l'activité des entités financières soumises à la surveillance de la Banque du Portugal ;
- ii) les moyens et les mécanismes nécessaires pour qu'ils puissent se conformer aux

devoirs énoncés dans la loi n° 97/2017 ;

- iii) les mesures que les prestataires de services de paiement doivent prendre pour détecter les virements de fonds lorsque les informations sur le donneur d'ordre ou le bénéficiaire sont manquantes ou incomplètes, et les procédures qu'ils doivent adopter pour gérer les virements de fonds qui ne sont pas accompagnés des informations requises en vertu du règlement (UE) 2015/847 du Parlement européen et du Conseil du 20 mai 2015 relatif aux informations accompagnant les virements ("règlement (UE) 2015/847") ;
- **Notification de la Banque du Portugal n° 8/2016, du 30 septembre**, qui régit les obligations d'enregistrement et de communication à la Banque du Portugal prévues à l'article 118-A n°3 et 5 du RGICSF et à l'article 9-A du RJSPME, ainsi que les conditions, mécanismes et procédures nécessaires à leur respect effectif;
- **Notification de la Banque du Portugal n° 7/2009, du 16 septembre**, qui interdit les prêts à des entités basées dans une juridiction *offshore* considérée comme non coopérative ou dont le bénéficiaire final est inconnu, définit la juridiction *offshore* et la juridiction *offshore* non coopérative et exige une déclaration des autorités de surveillance prudentielle dans les juridictions *offshore* où elles ont l'intention d'effectuer des opérations de crédit afin de s'assurer qu'il n'existe aucun obstacle à la communication.
- **Notification de la Banque du Portugal n° 5/2008, du 18 décembre**, qui prévoit que les établissements de crédit, les sociétés financières et les succursales ayant leur siège dans des pays tiers doivent disposer d'un système de contrôle interne permettant d'assurer l'exercice efficace et rentable de l'activité, l'existence d'information financière et de gestion complète, fiable, et pertinente en temps utile, ainsi que le respect des dispositions légales et réglementaires applicables. Abroge la notification n° 3/2006, du 9 mai.
- **Instruction de la Banque du Portugal n° 5/2019, du 30 janvier 2019** - établissant le modèle unique de déclaration annuelle et définissant les exigences en matière d'informations devant être périodiquement communiquées à la Banque du Portugal par les entités soumises à sa surveillance dans le domaine des PBCFT.
- **Instruction de la Banque du Portugal n° 6/2020, 06 du mars 2020** – qui modifie l'instruction n° 5/2019 pour inclure dans le Rapport sur la Prévention du Blanchiment du Financement du Terrorisme des informations concernant les procédures spécifiques pour se conformer au règlement (UE) 2015/8.
- **Règlement de la CMVM n° 2/2020, du 05 mars 2020**, établissant les mesures à caractère préventif de lutte contre le blanchiment de capitaux et le financement du terrorisme à mettre en œuvre par les entités obligées de nature financière soumises à la surveillance de la CMVM et des auditeurs dans le cadre des pouvoirs conférés par la loi n° 83/2017, du 18 août (la " LBCFT ") et la loi n° 97/2017, du 23 août (la " loi n° 97/2017 "), et établit également les obligations d'information périodique à fournir par les entités obligées.
- **Règlement n° 276/2019, du 26 mars 2019, de l'Instituto dos Mercados Públicos, do Imobiliário e da Construção, I. P. (IMPIC, IP)** - Règlement sur la prévention et la lutte contre le blanchiment de capitaux et le financement du terrorisme dans le secteur immobilier ;

- **Règlement n° 686/2019, du 2 septembre 2019 de l’Autorité de Sécurité Alimentaire et Économique**, qui régit les fonctions spécifiques de prévention et de lutte contre le blanchiment de capitaux et le financement du terrorisme des entités gestionnaires des plateformes de financement collaboratif par don ou avec récompense.
- **Lettre circulaire de la BdP n° CC/2020/0000062, du 27 novembre 2020**, sur l’application de mesures renforcées - Utilisation de structures complexes de participation ou de domination pour les pratiques de blanchiment de capitaux.
- **Lettre circulaire de la BdP n° CC/2020/0000063, du 27 novembre 2020**, sur l’application de mesures renforcées - Utilisation de sociétés créées par des moyens expéditifs pour la création de sociétés de blanchiment de capitaux.
- **Lettre circulaire de la BdP n° CC/2020/0000074, du 31 décembre 2020**, sur les juridictions à risque et le renforcement de la liste GAFI/FATF.

LÉGISLATION ET RÉGLEMENTATION LUXEMBOURGEOISES

- **Loi modifiée du 12 novembre 2004** relative à la lutte contre le blanchiment d’argent et le financement du terrorisme (« LBC/FT »).
- **Loi du 13 février 2018**, portant des dispositions ayant trait aux obligations professionnelles et aux pouvoirs des autorités de contrôle en matière de lutte contre le blanchiment et contre le financement du terrorisme.
- **Loi du 25 mars 2020, portant modification de la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme.**
- **Règlement grand-ducal du 14/08/2020** portant précisions de certaines dispositions de la loi modifiée du 12 novembre 2004.
- **Règlement grand-ducal du 29/10/2010** portant exécution de la loi du 27 octobre 2010 relative à la mise en œuvre des résolutions du Conseil de Sécurité des Nations Unies et d’actes adoptés par l’Union européenne comportant des interdictions et des mesures restrictives en matière financière à l’encontre de certaines personnes, entités et groupes dans le cadre de la lutte contre le financement du terrorisme.
- **Règlement CSSF N° 12-02 du 14 décembre 2012** visant à préciser et à compléter les dispositions luxembourgeoises en matière de LBC/FT.
- **Règlement (UE) 2015/847** du Parlement européen et du Conseil du 20 mai 2015 sur les informations accompagnant les transferts de fonds et abrogeant le règlement (CE) n. 1781/2006.
- **Règlement CSSF n° 20-05** portant modification du Règlement CSSF n° 12-02 du 14 décembre 2012 relatif à la lutte contre le blanchiment et contre le financement du terrorisme
- **Circulaire CSSF 13/556** relative à l’entrée en vigueur du règlement CSSF N° 12-02 et à l’abrogation des circulaires CSSF 08/387 et 10/476;
- **Circulaire CSSF 11/528** sur la suppression de la transmission à la CSSF des déclarations d’opérations suspectes relatives à un éventuel blanchiment ou financement du terrorisme;
- **Circulaire CSSF 11/519** relative à l’analyse des risques dans le cadre de la LBC/FT;

- **Circulaire CRF 22/10** relative à l'application de l'article 5 (« devoir de coopération avec les autorités ») de la loi modifiée du 12 novembre 2004.
- **Circulaire 19/732** – *Prevention of money laundering and terrorist financing: clarifications on the identification and verification of the identity of the ultimate beneficial owners.*
- *Circulaire CSSF 17/650 (telle que modifiée par la circulaire CSSF 20/744)*

4. MODÈLE DE RISQUE (BCFT)

La définition d'un modèle efficace de gestion des risques de blanchiment de capitaux et de financement du terrorisme (Modèle de Risque), avec des pratiques adéquates pour l'identification, l'évaluation, la gestion, le contrôle et la communication des risques auxquels GNB est, ou pourrait être, soumis dans ce domaine, a été considérée comme une priorité aux fins du respect des objectifs stratégiques dûment alignés sur le modèle d'entreprise du Groupe, des engagements assumés avec les *stakeholders* et des exigences réglementaires en vigueur..

L'organe de direction est chargé d'établir et de mettre à jour annuellement le niveau de tolérance au risque de l'institution, de surveiller le profil de risque effectif et de veiller à la conformité entre les deux.

La structure organique du département de *compliance*, ses attributions et ses compétences ont été approuvées par l'organe administratif.

En garantissant l'indépendance de la fonction de contrôle, définie dans le "*Règlement de la fonction de compliance*", le niveau de tolérance au risque du GNB et de ses principales unités commerciales est basé sur le respect des principes déterminants instillés dans les "*Compliance Policies and Guidelines for NB Group Financial Entities*", conformément à une méthodologie adaptée aux circonstances et à la réalité juridique de chaque unité/marché, basée sur le principe/axiome **Risk Based Approach (RBA)**, le niveau de risque perçu et le degré d'exposition du Groupe.

Conformément à la définition figurant dans les "*Compliance Policies and Guidelines for NB Group Financial Entities*", le Conseil d'Administration Exécutif a approuvé le document "Modèle de gestion des risques en matière de blanchiment de capitaux et de financement du terrorisme". Ce modèle est mis à jour périodiquement, ou lorsque des situations pertinentes le justifient, dûment encadrées et publiées.

Dans ce contexte, le Modèle de Risque adopté est basé sur un environnement de contrôle qui garantit le maintien du profil de risque dans les limites établies par le degré de tolérance au risque défini, ainsi que par les limites établies en fonction du type de risques répertoriés comme acceptables pour chaque activité concernée, compte tenu également des recommandations des organes de surveillance et de réglementation et des meilleures pratiques du marché national et international.

Le modèle de risque établit donc, comme principaux vecteurs d'atténuation, des programmes Know Your Customer (KYC), Know Your Transactions (KYT) et Know Your Process (KYP), mis en œuvre et définis dans des manuels de procédures spécifiques et des règlements internes, ainsi que dans son propre document, garantissant non seulement la conformité légale et réglementaire établie, mais aussi la liste des raisons et des mécanismes sous-jacents aux politiques assumées par l'institution pour la gestion de ces risques en particulier.

En ce qui concerne les **juridictions à risque**, le GNB considère 3 scénarios AML différents, changeants et dynamiques de risque de blanchiment de capitaux, soutenus par des listes internationales et la législation nationale, qui déterminent différentes approches d'action, de considération et d'analyse, avec 3 gradations de risque différentes - Risque élevé, Risque moyen, et Risque faible.

4.1 ÉVALUATION DES RISQUES DE COMPLIANCE – RISK ASSESSMENT

L'évaluation du risque, communément appelée *Risk Assessment*, est effectuée par le GNB dans le cadre et le contexte de chaque processus opérationnel, par le biais de procédures et de mécanismes établis : i) qui intègrent les processus opérationnels eux-mêmes ; ii) qui sont appliqués à la suite des processus opérationnels et des relations d'affaires sous-jacentes ; iii) ou, dans certaines situations, après l'occurrence de ces processus opérationnels ou après la fin/l'exécution des opérations liées aux relations d'affaires établies.

Le GNB considère et incorpore dans ses fonctions de prévention et de détection du blanchiment de capitaux et du financement du terrorisme, les pratiques de marché les plus actuelles et les normes juridiques récentes en vigueur, soutenues par le Modèle de risque pour la prévention du blanchiment de capitaux et du financement du terrorisme, récemment révisé et mis à jour.

Cette question est traitée spécifiquement dans un document connexe.

5 POLITIQUE D'ACCEPTATION DES CLIENTS ³

L'établissement de toute relation d'affaires est encadré par le respect des exigences légales et réglementaires en vigueur et, dans ce contexte, doit faire l'objet d'une non-acceptation lorsqu'elle implique :

- Des contreparties dont la réputation, selon des sources crédibles, semble associée à des activités criminelles ou dont l'activité rend impossible, ou difficile à prouver, la connaissance de l'origine des actifs insuffisamment justifiés ;
- Des contreparties qui, au cours du processus d'ouverture de compte, refusent de fournir des informations ou des documents jugés nécessaires pour se conformer aux obligations légales et réglementaires de la banque ;

³ La notion de "Client" doit être comprise dans un sens large, incluant les clients en relation d'affaires, les clients en transaction occasionnelle, les représentants du client et les personnes autorisées à agir au nom du client.

- Des banques fictives, entités exerçant une activité propre ou équivalente à celle d'une entité financière, qui sont constituées dans un pays ou une juridiction dans lequel elles n'ont pas de présence physique impliquant une gestion et une direction effectives, la simple existence d'un agent local ou d'employés subordonnés ne faisant pas partie d'un groupe financier réglementé ne constituant pas une présence physique ;
- Des comptes de "passage" (*payable through accounts*)⁴ - "Comptes assurés par des correspondants qui, soit directement, soit par l'intermédiaire d'un sous-compte, permettent l'exécution de transactions, pour leur propre compte, par les clients du répondant ou d'autres tiers" ;
- Des comptes anonymes, numérotés ou fictifs⁵ : le GNB ne fournit pas à ses clients de comptes anonymes ou numérotés ;
- Des entités sanctionnées, à savoir celles intégrant des listes de référence internationales obligatoires dans le circuit bancaire ;
- Des entités présentant un profil de risque spécifique, au moyen d'indicateurs considérés comme pertinents dans le cadre de la prévention du blanchiment de capitaux et du financement du terrorisme en relation avec certains segments d'activité (par exemple, la gestion ou la commercialisation de devises numériques, les jeux de hasard et les casinos en ligne / *gambling*) ou certaines juridictions à risque (par exemple, les centres *off-shore* et non coopératifs).

Suite à l'analyse des risques de blanchiment de capitaux qui motivent l'adoption de mesures renforcées⁶, à savoir les situations légalement indiquées comme potentiellement plus risquées⁷, les relations d'affaires nouvelles ou existantes qui relèvent de ces situations ou d'autres définies en interne en fonction de leur degré de risque, seront soumises à une **acceptation conditionnelle** (sous réserve d'un examen par le Département de Compliance).

6 PROCESSUS ET CONTRÔLES QUI ATTÉNUENT LES FACTEURS DE RISQUE (BCFT)

6.1 KNOW YOUR CUSTOMER (KYC) - ANALYSE DES CONTREPARTIES (OUVERTURE DE COMPTE, GESTION DES PARTICIPATIONS, ÉVALUATION DES CONTREPARTIES ET RMA'S)

Dans le cadre de l'établissement et du suivi des relations d'affaires avec les clients (ouverture de comptes, inclusion de nouveaux titulaires de comptes dans les contrats existants, évaluation des

⁴ Conformément à l'article 2, paragraphe m) de la loi n° 83/2017 du 18 août.

⁵ Conformément à l'article 64, de la loi n° 83/2017 du 18 août.

⁶ Conformément à l'article 36 de la loi n° 83/2017 du 18 août, qui établit des mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme, transpose partiellement les directives 2015/849/UE, du Parlement européen et du Conseil, du 20 mai 2015, et 2016/2258/UE, du Conseil, du 6 décembre 2016, modifie le code pénal et le code de la propriété industrielle et abroge la loi n° 25/2008, du 5 juin, et le décret-loi n° 125/2008, du 21 juillet.

⁷ Inscrits à l'annexe III de la loi n° 83/2017, du 18 août et de la notification 2/2018 de la BdP.

contreparties dans les opérations (*Due Diligence*), et établissement de *RMA* avec les institutions financières (*Swift's Relationship Management Application*) et conformément aux obligations réglementaires générales imposées, à savoir la vérification de l'identité et la diligence applicable⁸, des processus et des procédures ont été mis en œuvre à l'aide d'outils informatiques, qui sont appliqués de manière transversale aux risques identifiés, permettant de classer les clients en fonction de leur profil de risque (*Scoring*).

Dans ce contexte, la fonction Prévention du blanchiment de capitaux et du financement du terrorisme rattachée au Département Compliance peut être sollicitée, par la demande de documentation et d'informations complémentaires, de clarifications techniques et/ou ciblées, de collaboration dans la compréhension des structures de propriété et de contrôle, et de collaboration dans l'identification des UBO's (*Ultimate Beneficial Owners*), et le début de la relation d'affaires peut même être refusé si les éléments considérés comme satisfaisants ne sont pas obtenus.

6.1.1. FACTEURS ET TYPES DE RISQUES POTENTIELLEMENT PLUS ÉLEVÉS

Outre les processus et procédures génériques adoptés, fondés sur les exigences légales et réglementaires définies et tenant compte d'une gestion plus efficace des risques inhérents au BCFT, des processus et procédures spécifiques sont adoptés pour les facteurs et types de risques potentiellement plus élevés, notamment en ce qui concerne: i) **Relations de correspondant** (hors de l'Union européenne); ii) **Personnes politiquement exposées** (résidents et non-résidents); iii) **Titulaires d'autres fonctions politiques ou publiques**; iv) et **Bénéficiaires effectifs**.

6.2 FINANCEMENT DU TERRORISME

Le financement du terrorisme est un phénomène mondial qui a de graves répercussions sur la réputation des institutions financières et auquel nous devons tous être particulièrement attentifs.

Le crime de financement du terrorisme est considéré comme tel lorsque quelqu'un, par quelque moyen que ce soit, fournit, collecte ou détient, directement ou indirectement, des fonds, des biens, des produits ou des droits susceptibles d'être transformés en fonds, dans le but d'être utilisés dans la planification ou la pratique d'actes terroristes, ces actes et incrimination étant juridiquement reconnus par la loi⁹.

Conformément aux obligations de prévention du financement du terrorisme et par le biais d'alertes et de communications internes, les principaux indicateurs de suspicion ont été divulgués par les secteurs commerciaux afin qu'ils puissent, sur la base de leur connaissance du client (KYC) et de

⁸ Conformément aux dispositions de l'article 23 de la loi n° 83/2017 du 18 août - Devoir d'identification et de diligence.

⁹ Selon la loi n° 83/2017, du 18 août, article 2 - Définitions, paragraphe s), " *Financement du terrorisme* " les comportements prévus et sanctionnés par l'article 5 - A de la loi n° 52/2003, du 22 août, loi sur la lutte contre le terrorisme, modifiée par les lois n° 59/2007, du 4 septembre, 25/2008, du 5 juin, 17/2011, du 3 mai, et 60/2015, du 24 juin.

leur profil transactionnel (KYT), identifier les comportements et/ou opérations potentiellement suspects.

6.3 RELATIONS DE CORRESPONDANT BANCAIRE

L'ouverture de relations de correspondant bancaire (y compris les comptes et les RMA) est soumise à un processus de calcul de notation, dans lequel la domiciliation dans des pays tiers à risque élevé, des pays non membres de l'UE ou des juridictions identifiées par la Commission européenne comme ayant des régimes nationaux de lutte contre le blanchiment de capitaux et le financement du terrorisme présentant des déficiences stratégiques qui constituent une menace significative pour le système financier de l'Union européenne, est évaluée, ce qui donne lieu à une notation de risque pertinente.

L'évaluation des risques réalisée cherche à comprendre la nature de l'activité développée par la contrepartie et à savoir si elle est dûment autorisée, à déterminer si ses politiques et procédures sont conformes aux meilleures pratiques internationales, la composition de son actionnariat, les membres de son *Executive Board*, les bénéficiaires effectifs et la consultation de sources ouvertes, ainsi qu'à effectuer les procédures d'identification supplémentaires requises par la loi¹⁰.

Les réponses aux demandes de *Due Diligence* (KYC/KYT) de correspondants bancaires sont également produites dans le cadre du PBCFT.

Il existe certaines opérations pour compte propre, dans le cadre des contrats de garde de titres, dans lesquelles les banques dépositaires sont sélectionnées par NB (*service providers*) pour fournir des services de règlement et de garde de titres sur les marchés internationaux, et il existe une relation de correspondance avec chacune de ces entités, qui font l'objet d'une identification et de diligences.

Les opérations sur titres en question peuvent être effectuées pour le compte de clients ou de la banque, et il existe une obligation légale de les conserver dans des comptes de dépôt séparés.

Dans ce type d'opération, NB s'occupe de l'ouverture, du maintien des conditions ou de la fermeture des comptes supportant ce service dans d'autres banques. Les comptes de dépôt ouverts auprès des banques dépendent et sont directement liés aux comptes techniques typés *Nostro*.

En ce qui concerne les opérations de Paiement, c'est-à-dire les transferts émis ou reçus par ou depuis des banques correspondantes, *Clearing Houses* ou d'autres contreparties, pour le compte de clients, ou pour le compte de la Banque elle-même, NB peut également intervenir dans l'ouverture, le maintien des conditions ou la fermeture des comptes *Nostro* associés.

¹⁰ Conformément aux dispositions de l'article 27 de la loi n° 83/2017, du 18 août - " L'obtention de l'objet et de la nature de la relation d'affaires, l'origine et la destination des fonds de la relation d'affaires ou de la transaction occasionnelle et le suivi continu de la relation d'affaires en fonction du profil de risque du client".

6.4 PROPRES TRANSACTIONS

Dans le cadre des propres transactions, la Banque considère :

- i) Les transactions pures de portefeuille pour compte propre (titres, disponibilités financières et parts sociales) dans lesquelles NB assume le rôle de contrepartie d'achat ou de vente vis-à-vis des *Clearing Houses*, Courtiers (*Brokers*), des dépositaires sélectionnés et d'autres entités ;
- ii) Opérations de salle des marchés contractées et exécutées à des fins de gestion de trésorerie (*cash*) avec des banques et des courtiers ;
- iii) Les opérations effectuées pour le compte de tiers qui n'ont pas la qualité de clients (Dépositaires, Correspondants, Intermédiaires financiers, Agents, gestion et maintenance de RMA, opérations hors bilan, etc...) ;
- iv) Les transactions pour son propre compte ou autrement entre NB et toute autre entité appartenant au même groupe, en dehors d'une relation avec un client, c'est-à-dire les transactions intragroupe (NB avec d'autres entités du GNB et NB avec des succursales étrangères).

Les transactions négociées, compensées et réglées sur les instructions des clients, pour lesquelles un recours est exercé auprès d'entités tierces, *trading* (négociation), de dépositaires, de liquidateurs, d'agents de compensation, d'agents payeurs, entre autres, ne sont pas considérées comme faisant partie de ce champ d'application.

Cette dimension est dûment encadrée dans la législation en vigueur, à savoir à l'article 63 de la loi 83/2017, du 18 août, et à l'article 44 de la Notification de la BDP n° 02/2018, du 26 septembre, et l'activité elle-même est réglementée par des mécanismes de marché.

Les relations avec les contreparties commerciales utilisées obéissent à l'établissement de contrats et à la signature SLA (*Service Level Agreements*), qui tendent à suivre une standardisation internationale des conditions et des clauses, et atténuent ainsi les risques actuels et inhérents aux circuits financiers.

En règle générale, NB fait appel à des entités de marché central dont les pratiques sont reconnues comme la norme de l'activité (Interbolsa, LCH Clearnet), à des courtiers nationaux (Haitong et autres) ou internationaux (Pershing LLC et autres) soumis aux règles en vigueur et dûment réglementés et supervisés par les superviseurs respectifs, ainsi qu'à des dépositaires mondiaux, réputés et également soumis à des cadres réglementaires stricts (Euroclear, JPMorgan, Intesa SanPaolo, KAS Bank, Pershing LLC), en appliquant des mesures de diligence simplifiées pour les situations de continuité d'exploitation découlant de relations contractuelles établies et de mesures à faible risque potentiel.

Si un risque se matérialise du point de vue du PBCFT, il incombera au DCOMPL d'intervenir et de chercher à évaluer le niveau d'atténuation et de correction requis.

6.5 PERSONNES POLITIQUEMENT EXPOSÉES (PEP'S), MEMBRES DE LA FAMILLE ET ASSOCIÉS DE PEP'S, ET AUTRES TITULAIRES DE FONCTIONS POLITIQUES OU PUBLIQUES (OTCPP)

Lors de l'établissement de relations d'affaires, au début ou au cours de l'activité (insertion de la participation dans les contrats), avec des clients résidents ou non-résidents PEP¹¹ (Politically Exposed Person) et catégories équivalentes¹², la Banque recueille des informations déclaratives concernant l'exercice de fonctions politiques/publiques, et autorise l'établissement de relations d'affaires avec ces clients, exigeant l'intervention de niveaux hiérarchiques supérieurs.

La loi 83/2017 du 18 août, dans son article 39, a introduit un concept large de PEP, en augmentant l'éventail des personnes physiques à caractériser, elle implique également l'adoption de mesures de diligence accrue, notamment en ce qui concerne l'obligation de présenter des preuves de patrimoine (avant l'établissement de la relation d'affaires ou de la transaction occasionnelle, au cours de la relation d'affaires lorsqu'il y a une acquisition ultérieure des entités susmentionnées, au cours des actions d'actualité d'information).

Compte tenu des nouvelles exigences réglementaires et du nouveau modèle de rapport sur la prévention, le blanchiment de capitaux et le financement du terrorisme, la Banque a procédé aux adaptations et développements informatiques nécessaires pour : i) ventiler les informations entre les PEP et les OTCPP et ii) considérer individuellement les positions exercées et les juridictions dans lesquelles les PEP exercent ou ont exercé des positions.

La Banque enregistre désormais des informations sur les entités suivantes :

- **Personnes Politiquement Exposées**- les personnes physiques qui exercent, ou ont exercé au cours des 12 derniers mois, dans tout pays ou toute juridiction, les fonctions publiques importantes suivantes de haut niveau (liste ci-jointe) ;
- **Membres de la Famille Proche** – i) Les ascendants et descendants en ligne directe d'une personne politiquement exposée ; ii) Les conjoints ou partenaires non mariés d'une personne politiquement exposée et des personnes visées à l'alinéa précédent ;

¹¹ Conformément à l'article 2 Définitions - alinéas cc), dd), i), ii) et iii) de la loi no. 83/2017, du 18 août, cc) " Personnes politiquement exposées ", les personnes physiques qui exercent ou ont exercé au cours des 12 derniers mois, dans tout pays ou juridiction, des fonctions publiques éminentes de niveau supérieur ; (...) dd) " Personnes reconnues comme étroitement associées " ; i) " Toute personne physique connue pour être copropriétaire d'une personne politiquement exposée (...) ".)" ; (ii) "Toute personne physique qui est propriétaire du capital social ou détient les droits de vote d'une personne morale (...) dont on sait qu'elle a pour bénéficiaire effectif une personne politiquement exposée" ; (iii) "Toute personne physique, dont on sait qu'elle a une relation d'entreprise, commerciale ou professionnelle avec une personne politiquement exposée".

¹² Conformément à l'article 2 - Définitions de la loi n° 83/2017, du 18 août, alinéa gg) " Titulaires d'autres fonctions politiques publiques", les personnes physiques qui, sans être qualifiées de personnes politiquement exposées, occupent ou ont occupé, au cours des 12 derniers mois et sur le territoire national, l'une des fonctions suivantes : i) les fonctions énumérées au paragraphe 3 de la loi n° 4/83, du 2 avril, Contrôle public des titulaires de fonctions politiques, modifiée par les lois n° 38/83 du 25 octobre, 25/95 du 18 août, 19/2008 du 21 avril, 30/2008, du 10 juillet, et 38/2010, du 2 septembre, lorsqu'elles ne déterminent pas la qualification du titulaire comme "personne politiquement exposée" ; ii) Membres de l'organe représentatif ou exécutif d'une zone métropolitaine ou d'autres formes d'association municipale.

- **Personnes Reconnues comme Étroitement Associées** - i) toute personne physique, dite copropriétaire, avec une personne politiquement exposée, d'une personne morale ou d'un groupement juridique ; ii) toute personne physique qui est propriétaire du capital social ou des droits de vote d'une personne morale, ou des biens d'un groupement juridique connu comme bénéficiaire effectif d'une personne politiquement exposée ; iii) toute personne physique connue pour avoir une relation d'entreprise, commerciale ou professionnelle avec une personne politiquement exposée ;
- **Titulaires d'autres Fonctions Politiques ou Publiques** - les personnes physiques qui, sans être qualifiées de personnes politiquement exposées, exercent ou ont exercé, au cours des 12 derniers mois et sur le territoire national (liste ci-jointe).

La Banque garantit l'enregistrement des informations pendant la période de transition/mise en œuvre du nouveau modèle, et procède au recouvrement de l'historique correspondant.

6.6 ÉVALUATION DU RISQUE CLIENT ET MODÈLES DE SCORING

Lors de l'établissement de relations d'affaires, et afin d'assurer la connaissance de la structure de propriété et de contrôle des personnes morales ou des groupements juridiques, la banque doit identifier et recueillir des informations auprès du ou des bénéficiaires effectifs, conformément à l'obligation d'identification.

Le risque attribué aux contreparties, à leurs représentants et aux bénéficiaires effectifs est mesuré de deux manières différentes :

- 1) Initialement, en combinant les différents indicateurs de risque présents dans le modèle de risque défini par la Banque, qui forment le " *scoring* PBC/FT" :

Le résultat du " *scoring* PBC/FT" pourra être :

- i) Maintenance (risque faible) ;
- ii) Surveillance (risque moyen) ;
- iii) Enquête (risque élevé) ;

Seuls les processus ayant un résultat de *scoring* enquête (risque élevé - enquête) nécessitent une intervention du DCOMPL.

Les processus qui obtiennent un résultat de *scoring* DMO (risque moyen et faible - suivi et maintenance) sont transmis et traités directement par le DMO - Département des ressources opérationnelles.

- 2) Au cours de sa relation d'affaires avec la banque, au moyen d'un ensemble de pondérations préalablement identifiées et régulièrement réévaluées, de nature diversifiée :

Le résultat du "Risque AML" pourra être :

- i) Élevé ;
- ii) Moyen ;

iii) Faible.

Dans le cadre de l'analyse et de l'approbation des contreparties et sur la base du risque, des mesures sont prises pour prouver la qualité des bénéficiaires effectifs, notamment en recueillant les preuves documentaires jugées nécessaires pour comprendre pleinement la structure de l'actionnariat de ces contreparties, afin de les identifier correctement et, d'autre part, de permettre la relation entre les bénéficiaires effectifs identifiés et le client.

Conformément aux dispositions légales, la Banque consultera et, si nécessaire, notifiera au service compétent du Registre central des bénéficiaires effectifs (RCBE) toute omission, inexactitude, non-conformité ou information périmée sur le statut du bénéficiaire effectif.

La Banque recueille également l'identité des organes de direction, des autres encadrements supérieurs concernés et des détenteurs de participations au capital et aux droits de vote supérieures ou égales à 5% du capital social.

6.7 MISE À JOUR DES INFORMATIONS

Considérant que la connaissance du Client et la collecte des informations qui permettent de recueillir cette connaissance ne s'arrêtent pas au moment de l'établissement de la relation d'affaires, mais doivent être approfondies et mises à jour régulièrement, en fonction du degré de risque attribué ou à chaque fois qu'un événement justifiable se produit, des procédures ont été développées pour respecter l'obligation de mise à jour des informations¹³. Les diligences de mise à jour des informations ont priorité et fréquence différentes et varient en fonction du degré de risque associé au client.

6.8. KNOW YOUR TRANSACTIONS (KYT) - MONITORING

Afin de surveiller en permanence le comportement de ses clients, une analyse est faite de leur profil transactionnel, qui est évalué et comparé en fonction de la connaissance historique du client, de la logique économique de sa fonction professionnelle et/ou de son secteur d'activité et de son potentiel d'implication dans des contextes de risque de blanchiment de capitaux et de financement du terrorisme, tout en tenant compte des zones géographiques concernées.

La compréhension des circuits potentiels d'origine et de destination des fonds dans les contrats est obtenue au moment de l'établissement de la relation d'affaires, et à un moment ultérieur, l'information de l'encadrement pour le mouvement des fonds est évaluée chaque fois que nécessaire, et en plus, les transactions enregistrées dans chaque contrat doivent impérativement contenir l'identification du donneur d'ordre et du bénéficiaire.

Dans le cadre des contrôles établis pour le suivi des transactions (Monitoring), la Banque effectue une évaluation basée sur l'analyse comparative des alertes générées par un outil automatique de

¹³ Conformément aux dispositions de l'article 40 de la loi n° 83/2017, du 18 août - Procédures de mise à jour.

suivi des contrats, en fonction de paramètres spécifiques, en adoptant des mesures de diligence renforcée (EDD) (*Enhanced Due Diligence*) chaque fois que cela est justifié, dans le cadre de la prévention du blanchiment de capitaux et du financement du terrorisme.

Au cours du processus de *Monitoring*, une attention particulière est accordée à la *Due Diligence* relative aux transactions internationales (banques correspondantes et pré-validation sur demande des opérations de *Trade Finance*), au suivi et à la surveillance des comptes (alertes AML), ainsi qu'aux alertes liées aux mouvements de risque (qui obéissent à des limites et définitions préalables et adaptables).

Les diligences mises en œuvre peuvent, par exemple, conduire à l'exigence d'un encadrement supplémentaire et à la présentation de pièces justificatives, à savoir l'obtention d'une DOF (Déclaration d'Origine des Fonds), ou autres.

6.9 SIGNALEMENT DES TRANSACTIONS SUSPECTES (SAR'S)

La Banque a mis en place des politiques et procédures internes en matière de déclaration de transactions suspectes aux autorités compétentes, conformément aux dispositions légales et réglementaires en vigueur¹⁴ :

- i) DCIAP (Departamento Central de Investigação e Ação Penal) - Procuradoria-Geral da República;
- ii) UIF (Unidade de Informação Financeira) – Polícia Judiciária.

Les communications sont encadrées par le devoir de refus (art. 50), le devoir de communication (art. 43) et le devoir d'abstention (art. 47), consacrées par la loi n° 83/2017, du 18 août.

En ce qui concerne les rapports de transactions suspectes, la succursale du Luxembourg rapporte à l'autorité compétente de ce pays - *Cellule de Renseignement Financier* (CRF).

6.10 COOPÉRATION AVEC LES AUTORITÉS

En raison des différents processus d'analyse et de suivi et de la diligence opérationnelle dans le domaine de la prévention du BCFT, et dans l'exercice des devoirs de communication (Section IV - Article 43), d'abstention (Section V - Article 47) et de collaboration (Section VI - Autres Devoirs - Article 53), de la Loi 83/2017, du 18 août, les réponses aux demandes des autorités compétentes et sectorielles sont mises à disposition de manière complète et perceptible, dans les délais établis par celles-ci¹⁵.

¹⁴ Considérant les dispositions de l'article 43 de la loi n° 83/2017, du 18 août - Déclaration de transactions suspectes.

¹⁵ Reproduit dans les articles 43, 53 et 47 de la loi n° 83/2017, du 18 août

Dans ce domaine, les types de processus, entre autres, sont principalement liés aux processus d'enquête du PBCFT, dans le cadre de procédures pénales, et avec diverses demandes de la Banque du Portugal. L'accomplissement en temps voulu de cette obligation par la Banque implique un exercice très exigeant en termes de compilation et de disponibilité des informations en rapport.

En ce qui concerne la coopération avec les autorités luxembourgeoises, la *Loi du 12 novembre 2004 (art.5)* et les autres législations applicables en vigueur s'appliquent dans le cadre de la rédaction du présent point 6.10 Collaboration avec les Autorités, notamment en ce qui concerne les interactions à maintenir avec la *Cellule de Renseignement Financier*.

6.11 KNOW YOUR PROCESS (KYP)

6.11.1 GESTION DU MODÈLE DE RISQUE

Aux fins de la gestion du modèle de risque, divers processus transversaux ont été mis en œuvre en vue d'identifier les vulnérabilités, les probabilités d'occurrence, les impacts potentiels et les facteurs d'atténuation des risques liés, entre autres, à l'ouverture de comptes, à la mise à jour des informations et aux processus opérationnels pour la réalisation des transactions bancaires.

6.11.2 HIGH-RISK CUSTOMERS

Dans la perspective de la gestion du risque PBCFT, des équipes pluridisciplinaires ont été créées au sein du Département de *Compliance* afin de suivre en permanence les clients et les opérations classés à haut risque en termes de KYC/KYT, avec la création d'un plan stratégique spécialement conçu pour contrôler et surveiller ce type de clients et les opérations dont font partie : i) le filtrage en ligne ; ii) et des scénarios spécifiques de risque, conçus sur mesure et soutenus par une application logicielle (*AML Manager*). Les géographies et les Groupes de risques, présents sur les différents continents, ont également été segmentés.

Suivant une Matrice RBA (***Risk Based Approach***), le GNB surveille les clients à haut risque dans 2 dimensions différentes :

- 1) Projet de récidive - qui intègre une analyse des clients basée sur les interactions avec les autorités compétentes (rapports, lettres) ;
- 2) Projet de clients à haut risque - qui intègre plusieurs dimensions de risque AML, notamment :
 - i) les Clients nécessitant une surveillance étroite ;
 - ii) juridictions considérées comme étant à risque
 - iii) certains secteurs d'activité (par exemple, *Money Remitters*, Monnaies virtuelles, *Gambling*) et
 - iv) certains Groupes et structures commerciales.

6.11.3 EXAMEN DU RISQUE DE COMPLIANCE

L'aspect KYP (*Know Your Process*), outre la prise en compte de l'évaluation des risques de conformité (*Risk Assessment*) déjà mentionnée ci-dessus, intègre des procédures de surveillance continue et périodique (*backtesting*), la révision des contenus établis et l'adaptation aux nouvelles exigences légales et réglementaires, ainsi que la gestion des risques généraux dans le contexte du PBCFT.

6.11.4 FERMETURE DE COMPTES À LA DEMANDE DU SERVICE DE LA COMPLIANCE

Dans l'exécution de ses fonctions de contrôle, de suivi et de surveillance, et de prévention des risques généraux de BCFT, le département de la compliance peut, dans certaines circonstances, demander la fermeture de comptes clients comme mesure ultime d'atténuation des risques.

Ces demandes sont régulièrement suivies et analysées par les Comités de risque en présence du DCOMPL et du Conseil d'administration de la Banque, et font l'objet d'un règlement interne.

Cette pratique est encadrée par la loi 83/2017, du 18 août (article 50 - 3b) - Devoir de refus), et par la notification de la BdP n° 02/2018, du 26 septembre (article 39 - Devoir de refus), justifiant la rupture de la relation d'affaires avec un client dès lors qu'est identifié un risque BCFT potentiel qui ne peut être géré par la Banque d'une autre manière.

La clôture des contrats à la demande de DCOMPL peut se faire de deux manières différentes :

- i) Résultant d'un processus d'ouverture de compte où il est décidé de refuser le contrat ;
- ii) Résultant des diligences effectuées dans le domaine des transactions.

Les demandes de clôture par instruction bancaire et/ou décision de compliance sont exécutées et enregistrées au moyen d'outils informatiques qui assurent la traçabilité nécessaire, et sont exclusivement exécutées par les employés ayant la responsabilité définie à cet effet. Le suivi des commandes est strictement contrôlé et surveillé jusqu'à ce que la clôture du compte soit garantie.

6.12 APPROBATION DE NOUVEAUX PRODUITS ET SERVICES - PROCESSUS DE SIGN-OFF

La Banque dispose d'un processus de *sign-off* préalable à la mise à disposition de nouveaux produits et services qu'elle commercialise auprès des clients dans le cadre de son activité, qui est étendu au GNB et géré par un secteur spécifique du Département de *Compliance*.

Ce processus établit un ensemble de règles et de procédures internes qui doivent être respectées en ce qui concerne la conception et/ou la distribution de produits et de services, en vue d'identifier, d'évaluer et d'atténuer les différents risques associés d'un point de vue préventif, y compris, du point de vue du blanchiment de capitaux et du financement du terrorisme.

6.13 JURIDICTIONS À RISQUE ÉLEVÉ

Compte tenu des indicateurs de risque associés aux juridictions ou pays à risque, tels que diffusés dans des documents publiés par des organismes internationaux ou des entités de référence appropriées, le GNB n'a pas l'intention d'établir ou de maintenir des relations avec des clients ou des contreparties, privés ou collectifs, situés dans des juridictions qui ne disposent pas de systèmes efficaces de prévention et de lutte contre le blanchiment de capitaux et le financement du terrorisme.

Il convient d'accorder une attention particulière à l'analyse et à l'examen, généralement étayés par des mesures de vigilance renforcées, des actions de vigilance supplémentaires et la collecte de documents justificatifs concluants, des qualités de risque inhérentes au type d'opérations impliquant

des transactions dans des centres considérés comme offshore ou dont les participants ont une qualité spécifique qui implique des exigences plus strictes en matière d'information, comme par exemple les PEP et les personnes liées, d'autres titulaires de fonctions publiques, conformément à la loi, ou même les EB (UBO), notamment lorsqu'ils sont associés à des structures d'entreprise complexes.

7 SYSTÈME DE SANCTIONS ET DE MESURES RESTRICTIVES - FILTERING

Les mesures restrictives, également appelées sanctions, sont un instrument multilatéral de nature politique, diplomatique ou économique utilisé par les institutions internationales pour exercer une influence sur des questions telles que la prévention et la répression du terrorisme, la promotion et la défense des droits de l'homme et des libertés publiques, la dissuasion d'un éventuel conflit armé ou l'interdiction du développement d'armes de destruction massive.

Au Portugal, la loi n° 11/2002 du 16 février définit le régime pénal applicable au non-respect des sanctions financières ou commerciales imposées par les résolutions du Conseil de sécurité des Nations unies ou les règlements de l'Union européenne, qui déterminent des restrictions à l'établissement ou au maintien de relations financières ou commerciales avec des États, d'autres entités ou des individus expressément identifiés.

Au Luxembourg la *Loi du 19 décembre 2020 relative à la mise en œuvre de mesures restrictives en matière financière*, fait référence à cette question.

La publication des lois n° 83/2017¹⁶, du 18 août, et n° 97/2017, du 23 août, et les dispositions du nouveau Rapport BCFT ont renforcé et intensifié le cadre juridique et réglementaire national en cette matière.

Par conséquent, le GNB est soumis aux régimes de sanctions nationaux et internationaux, à savoir ceux émanant de l'Union européenne (règlements et directives), du Conseil de sécurité des Nations unies et de l'**OFAC** - *Office of Foreign Assets Control (US Treasury Lists)*, des *US President Executive Acts* concernant les opérations en dollars américains, ainsi qu'au champ d'application des sanctions secondaires (extraterritoriales), le cas échéant.

Les processus AML prennent également en considération les listes du GAFI (OCDE), la législation portugaise et luxembourgeoise.

Les systèmes de filtrage établis (*Database Filtering*) intègrent des processus qui prévoient la mise à jour permanente et le croisement des noms des personnes et des entités figurant sur les listes de sanctions et de mesures restrictives approuvées par les Organisations internationales compétentes, et des systèmes de filtrage en ligne pour les transactions, les paiements et les virements - SWIFT, SEPA et TARGET sont en place.

¹⁶ Article 21 - Mesures restrictives ; Article 18 - Procédures et systèmes d'information en général ; Article 169 - Délits et Annexe III - Liste non exhaustive des facteurs de risque et des types de risque potentiellement plus élevés, paragraphe 3 - Facteurs de risque liés à la localisation géographique, paragraphe c) *Pays ou juridictions faisant l'objet de sanctions, d'embargos ou d'autres mesures restrictives ou contre-mesures supplémentaires imposées notamment par les Nations unies et l'Union européenne et (d) Pays ou juridictions apportant un financement ou un soutien à des actes ou activités terroristes, ou sur le territoire desquels opèrent des organisations terroristes.*

Compte tenu également du changement de registre et du régime de sanctions internationales, des consultations sont organisées avec les autorités nationales compétentes¹⁷ chaque fois que cela est utile à des fins de clarification et de sécurité opérationnelle du PBCF, en intégrant les recommandations interprétatives respectives en la matière. Le cas échéant, et afin de mieux définir les standards de l'action commerciale, ces recommandations sont également diffusées par les fonctions de première ligne de défense (Zones commerciales), par le biais d'une publication sur l'intranet de la Banque.

En raison de la préoccupation croissante pour le contrôle et la surveillance, et de la prolifération de listes et d'éléments liés au processus de filtrage, un nombre croissant de résultats positifs ont été générés, dont le cadre et les hypothèses de génération sont examinés, dans un effort continu pour réduire la génération de faux positifs et se concentrer sur les résultats positifs pertinents.

7.1 WOLFSBERG AML QUESTIONNAIRE

La Banque suit les principes contenus dans le Wolfsberg AML Questionnaire concernant le PBCFT. Ce document, qui est mis à jour périodiquement, est publié sur le site web de la Banque : www.novobanco.pt.

7.2 USA PATRIOT ACT CERTIFICATE

Conformément au "*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001*" (*USA Patriot Act*), NB peut être amené à fournir, le cas échéant, le *Certification Regarding Accounts for Foreign Banks*.

L'*USA Patriot Act* est publié sur le site web de la Banque : www.novobanco.pt.

8 FORMATION

L'intervention auprès de la première ligne de défense (Zones Commerciales) est supposée être une matrice stratégique pour l'action contre les phénomènes de blanchiment de capitaux et de financement du terrorisme. Dans ce contexte, des cycles de formation annuels sont établis, sous réserve d'une certification finale, par le biais de la plateforme d'apprentissage en ligne, pour tous les employés de la Banque.

En outre, des sessions de formation sur site sont organisées dans les zones de la Banque les plus exposées au risque BCFT, comme les Centres d'affaires et les structures similaires.

Le Département Compliance assure également la promotion régulière de la mise à jour des connaissances spécifiques et des formations spécifiques pour les employés et le personnel technique impliqués dans la prévention et la détection du blanchiment de capitaux et du financement du terrorisme.

¹⁷ Ministère des affaires étrangères et ministère des finances.
Ministère des finances (Luxembourg)

9 CODE DE CONDUITE, POLITIQUE EN MATIÈRE DE CONFLITS D'INTÉRÊTS, DE PARTIES LIÉES ET DE LUTTE CONTRE LA CORRUPTION¹⁸ - POLITIQUE DE *WHISTLEBLOWING*

Le Département de Compliance du GNB assure la promotion de la conformité de toutes ses entités et collaborateurs avec les exigences légales, réglementaires, statutaires, opérationnelles, de supervision, éthiques et de conduite applicables, dans le cadre de l'environnement institutionnel de contrôle et de supervision défini par les organismes de régulation compétents et par les réglementations légales auxquelles ils sont soumis, en guidant ses actions par un maximum d'intégrité, d'honnêteté, de diligence, de compétence, de transparence et de neutralité.

À cette fin, il a encouragé la divulgation, auprès du GNB et de ses collaborateurs, du Code de conduite, de la Politique en matière de conflits d'intérêts, de la Politique relative aux parties liées et du Règlement sur le signalement d'irrégularités (*Whistleblowing*).

Le Code de conduite comporte un chapitre spécifique sur les obligations en matière de prévention et de détection du blanchiment de capitaux et du financement du terrorisme, qui met l'accent sur les procédures instituées pour l'identification des clients et le suivi de la relation d'affaires, l'analyse des opérations effectuées au cours de la relation et la vérification de leur conformité avec les informations obtenues précédemment et la connaissance du client, en tenant compte, entre autres, des changements significatifs dans les schémas d'activité du compte et de la cohérence entre les opérations effectuées et le profil du client.

De plus, dans le but de suivre en permanence le comportement de ses clients, une analyse est également faite de leur profil transactionnel du point de vue du risque de marché, afin de détecter des situations potentielles d'*inside trading* et opérations d'initiés, de conflits d'intérêts, de corruption, d'incitations reçues ("*Gift Policy*"), d'éthique et de conduite.

10 SUIVI DES SUCCURSALES ET DES FILIALES

Dans le cadre de la prévention du blanchiment de capitaux et du financement du terrorisme, des politiques et des procédures ont été définies ("*Compliance Policies and Guidelines for NB Group Financial Entities*") qui garantissent le respect de la législation nationale matricielle, en appliquant les mêmes principes de définition, paramètres d'action et diligence de la fonction de *compliance*.

¹⁸ Le Code de conduite, la Politique sur les Conflits d'intérêts et la Politique sur les parties liées sont disponibles sur le site web de NB. <https://www.novobanco.pt/site/cms.aspx?plg=3AE91E8E-AAFB-4BD0-8C6A-07823384AEE3>. Sur le site web de NBL, les informations sont disponibles à l'adresse suivante: <http://www.novobancoluxembourg.lu/site/cms.aspx?labelid=HPPT>.

10.1 APPLICATION AUX ENTITÉS DU GROUPE NOVO BANCO

NOVO BANCO encourage l'adoption par ses Filiales des principes directeurs, paramètres d'action et de diligence établis par ces politiques, avec l'approbation des organes de gestion respectifs.

10.2 MODÈLES D'ARTICULATION

De plus, afin de définir clairement les responsabilités et le mode de fonctionnement entre les secteurs de *Compliance* des différentes structures (Succursales et Filiales) du GNB, des Modèles d'articulation bilatéraux ont été définis, qui sont soumis à une révision et à un contrôle périodique par une unité spécifique au sein du Département de *Compliance*.

11 CONSERVATION D'INFORMATIONS

Les documents originaux, copies, références ou tout autre support durable, mis à disposition par les clients ou les contreparties liées dans le cadre du processus d'identification et de diligence, ainsi que tous les documents, enregistrements de transactions ou analyses de support prouvant le respect des dispositions légales et réglementaires applicables, sont conservés dans le respect des délais légaux, après le processus d'identification, l'exécution de la transaction et également après la fin de la relation commerciale.

12 PROTECTION DE DONNÉES

La prévention et la lutte contre le blanchiment de capitaux et le financement du terrorisme sont expressément reconnues comme un domaine de protection d'intérêt public, y compris en ce qui concerne le traitement des données à caractère personnel effectué sur la base de la Loi n°. n° 83/2017, du 18 août¹⁹, ainsi que référencée dans le Règlement général sur la protection des données (RGPD), approuvé au Parlement européen le 27 avril 2016 et avec application obligatoire le 25 mai 2018 dans tous les États membres de l'Union européenne, remplaçant au Portugal la loi n° 67/98²⁰ du 26 octobre (transposition de la directive n° 95/46/CE).

Au Luxembourg, la *Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données* est applicable.

¹⁹ Comme prévu à l'article 57 - Objet et but de ladite loi.

²⁰ Loi sur la protection des données personnelles.

13 CONTRÔLE INTERNE ET AUDITS (INTERNES ET EXTERNES)

En complément de la fonction de contrôle exercée par la troisième ligne de défense - l'audit interne - et dans le cadre de l'évaluation systématique de l'efficacité du système de contrôle interne du GNB, des tests d'efficacité sont effectués chaque année sur le processus de prévention et de détection du blanchiment de capitaux et du financement du terrorisme²¹.

Le respect des dispositions légales et réglementaires en vigueur, dans le cadre des fonctions de contrôle du Département de *Compliance*, est également évalué, dans les termes et la périodicité prévus, par des Auditeurs Externes - Audit Externe - faisant l'objet d'un avis spécifique et d'une information à l'autorité de contrôle, y compris dans les rapports annuels d'activité dans la fonction de prévention du blanchiment de capitaux et du financement du terrorisme correspondants²².

14 PARTICIPATION À DES GROUPES DE TRAVAIL SECTORIELS

La participation à des réunions et à des groupes de travail sectoriels (Association bancaire portugaise (APB), Association des Banques et Banquiers, Luxembourg (ABBL), Unité de renseignement financier (UIF) et *International Chamber of Commerce* (ICC) est également une matrice du GNB que nous avons l'intention d'encourager et de continuer à remplir en tant que génératrice de connaissances et de partage de bonnes pratiques dans le contexte du PBCFT.

15 PROJETS STRATÉGIQUES DU GNB

Le GNB a entrepris des projets stratégiques qui, de par leur nature, leur incidence et leurs objectifs, ont un impact direct sur les questions BCFT, en particulier sur les Politiques générales de gestion du risque de blanchiment de capitaux et de financement du terrorisme.

Parmi ceux-ci, le Projet de la Banque Numérique, le Projet *Talent and Merit* 2018-2021, et le Projet APIC se distinguent.

15.1 PROJET DE LA BANQUE DIGITALE

Son principal objectif est de fournir à la banque les outils nécessaires aux services bancaires numériques modernes, en se tenant au courant des marchés et des tendances nationales et internationales sur tous les canaux et processus opérationnels.

²¹ La méthodologie utilisée par la DAI est basée sur les tests d'efficacité requis par l'article 44(d) de la Notification de la BdP n° 5/2013, définis pour l'application des mesures préventives et répressives de lutte contre le blanchiment de capitaux et le financement du terrorisme prévues par la loi n° 83/2017 du 18 août.

²² Conformément à la Notification de la BdP n° 9/2012, du 17 mai, qui approuve le Rapport sur la prévention du blanchiment de capitaux et du financement du terrorisme (RPB), établissant son élaboration annuelle et sa soumission à la BdP par le biais du système BPnet

NOVO BANCO a également nommé un *Chief Digital Officer* (CDO), dont le rôle est de diriger les mises en œuvre nécessaires et de fournir une vision transversale interdépartementale.

L'objectif est de faire de NOVO BANCO une banque à l'avant-garde du numérique, notamment grâce aux projets suivants :

- *Marketplace*, un nouveau concept permettant d'aller "au marché" grâce à un marché virtuel.
- *Homebuying*, réinventer l'expérience de l'achat d'une maison
- *Small Business Finance* (SFB), créant une meilleure expérience de financement pour le segment des entreprises.
- *Onboarding*, amélioration de l'expérience lors du premier contact du client avec la banque.

15.2 PROJET TALENT AND MERIT 2018-2021

Son objectif principal est d'indiquer la future voie stratégique du GNB, basée sur plusieurs piliers de transformation des processus et des technologies, où les piliers "IT" et "*Risk Adjustment*" sont d'une importance particulière. Le programme vise à atteindre la différenciation, la numérisation et l'optimisation.

Cette analyse comprend la remise en question des outils IT destinés à soutenir les processus AML. Soit par des améliorations fonctionnelles, soit par des solutions complémentaires et/ou alternatives permettant une gestion intégrée de l'information (*Filtering* - opérations et bases de données, *Monitoring*, *Risk Case Analysis*, *Reporting and Data Management*), une communication intra-applicative de l'information, et une vision unique et intégrée du client. Les éléments essentiels pour faire face à la complexité croissante des circuits et des scénarios de risque.

15.3 PROJET APIC

Ce projet multi départemental porte sur la mise à jour permanente des informations relatives aux Clients NB, afin de se conformer aux obligations réglementaires en vigueur.

En tant que projet transversal pour l'ensemble de la zone opérationnelle et technologique de la banque, la solution a été conçue dans le but de maximiser l'utilisation des canaux numériques, tout en maintenant les fonctionnalités de support analogique lorsque cela était justifié.

La solution vise à intégrer les obligations légales de collecte et de mise à jour des informations dans la relation commerciale normale entre NB et ses clients, en les transformant en opportunités.

Il comporte plusieurs objectifs segmentés, dont les suivants : i) Définition d'une solution automatique, favorisant les supports numériques en vue de la mise en œuvre du processus ; ii) Conception d'une solution polyvalente qui combine les différents systèmes et domaines documentaires de la banque ;

iii) Conception d'une solution flexible qui permette le traitement des données de contrôle des résultats permanents ; iv) Conception de la structure du processus en respectant une logique d'efficacité et d'impact minimum pour les zones commerciales ; v) Conception d'une solution qui permette de réduire les coûts d'exploitation, d'atténuer les risques d'exploitation et d'améliorer la relation avec le client.

Les principales mises en œuvre sont orientées vers la relation de NB avec le *customer onboarding* qui sera développé par NOVO BANCO Digital Project, et vers les mises en œuvre KYC découlant de la loi 83/2017 du 18 août.

NBL bénéficiera des développements techniques qui doivent encore être mis en œuvre dans NB et, compte tenu de sa dimension et de sa complexité moindres, applique déjà, de manière manuelle, les principes et procédures nécessaires qui permettent de collecter et de conserver une documentation adéquate sur ses clients.

16 ANALYSE CRITIQUE DU MODÈLE BC/FT MIS EN ŒUVRE – OBJECTIFS POUR L'AVENIR

Le GNB procède à une analyse critique continue du modèle BC/FT mis en œuvre, en tenant compte des multiples facteurs contextuels, de l'actualité nationale et internationale, de l'évolution du cadre juridique, des pratiques et des tendances du marché, de l'évolution de la composante technologique et des nouveaux projets stratégiques, entre autres facteurs.

En ce sens, et en orientant la vision de l'exigence et de l'importance croissante du PBC/FT vers les objectifs des programmes stratégiques en cours, il appartient au DCOMPL, en assumant sa fonction de contrôle indépendant, de concentrer son attention sur l'aspect KYP (*Know Your Process*), compte tenu des exigences du marché, et du cadre juridique complexe, sans négliger évidemment les aspects complémentaires KYC (*Know Your Customer*) et KYT (*Know Your Transaction*).

Le principal objectif stratégique pour l'avenir est la mise en œuvre de la gestion d'une vision unique et intégrée du client à tout moment, ainsi que de l'information produite par les différents processus de base du PBCFT (*Analyse des contreparties, Filtering - Opérations et Bases de données, Monitoring e Risk Case Analysis, Reporting e Data Management*). L'orientation vers les processus implique une attention particulière aux mécanismes, aux circuits, à la production et à la validation des données statistiques, à la qualité globale des résultats obtenus, au contrôle des procédures et à la rigueur de l'analyse des risques.

Le GNB vise à investir dans les développements IT et les solutions AML interdépendantes, avec des outils de *Audit Trail*, l'incorporation de nouveaux scénarios de risque et des modules statistiques auxiliaires à l'analyse PBCFT et aux décisions de gestion.

17 RISQUES GÉNÉRAUX LIÉS AUX MOUVEMENTS DE TRÉSORERIE

Cette question présente un intérêt particulier pour les circuits de PBCFT, où une approche renforcée du contrôle, de l'identification des déposants et des personnes impliquées dans les opérations de trésorerie en général est pertinente en fonction des circonstances spécifiques de l'opération. Cela inclut l'utilisation du mécanisme de demande de Déclaration de Provenance et de Justification des Fonds (DOF) pour certaines typologies d'opérations, en plus des obligations actuelles d'identification des déposants. Les mêmes règles s'appliquent aux opérations d'échange de billets et de pièces, classées comme des transactions occasionnelles.

18 DEVOIRS PRÉVENTIFS DU BCFT – BANQUE ET COLLABORATEURS

La loi 83/2017, du 18 août, établit des mesures préventives et répressives pour lutter contre le BCFT, et étend le champ d'application et renforce le respect des 10 Devoirs préventifs du BCFT que les institutions financières (GNB) et leurs collaborateurs doivent observer.

Ces devoirs sont également abordés dans le nouveau Rapport annuel de BCFT.

18.1. DEVOIR DE CONTRÔLE

Impose aux Institutions Financières l'application effective de politiques, procédures et contrôles adaptés à la gestion efficace des risques de Blanchiment de Capitaux et de Financement du Terrorisme et le respect des normes légales et réglementaires en la matière.

18.2. DEVOIR D'IDENTIFICATION ET DE VIGILANCE

Oblige à respecter les procédures dans ce domaine chaque fois que l'une de ces situations se produit :

- Établissement d'une relation d'affaires ;
- Réalisation de transactions occasionnelles d'un montant égal ou supérieur à 15 000,00 euros (que la transaction soit effectuée en une seule opération ou en plusieurs opérations apparemment liées entre elles) ou d'un transfert de fonds d'un montant supérieur à 1.000,00 euros ;
- S'il existe un soupçon que les transactions peuvent être liées au BC ou FT ;
- S'il existe des doutes sur la véracité ou l'adéquation des données d'identification des clients obtenues précédemment.

Ce devoir est étendu à d'autres entités, à savoir : i) les Entités Tierces ; ii) les Intermédiaires de Crédit ; iii) les Promoteurs et les relations d'intermédiation ; iv) l'*outsourcing*.

18.3. DEVOIR DE COMMUNICATION

Cela implique le devoir de signaler les cas où l'on sait, soupçonne ou à des motifs raisonnables de

soupçonner que des fonds ou des biens proviennent d'une activité criminelle ou sont liés au financement du terrorisme, couvrant toutes les opérations proposées, tentées, en cours ou exécutées.

18.4. DEVOIR D'ABSTENTION

Impose de n'effectuer aucune transaction dont on sait ou dont on soupçonne qu'elle est associée à des fonds ou à d'autres biens provenant de la perpétration d'activités criminelles ou du financement du terrorisme.

18.5. DEVOIR DE REFUS

Cela implique de ne pas entrer dans une relation d'affaires, d'exécuter une transaction occasionnelle ou d'autres opérations, lorsque l'une des circonstances suivantes s'applique :

- Défaut d'obtention des éléments identifiés et des moyens de preuve respectifs nécessaires auprès du client, du représentant ou du bénéficiaire effectif, y compris les informations nécessaires pour établir le statut du Bénéficiaire Effectif et la Structure de propriété du client ;
- Informations sur la nature, l'objet et la finalité de la relation d'affaires ;
- Impossibilité d'effectuer les procédures d'identification et de diligence, y compris les procédures de mise à jour des données.

18.6. DEVOIR DE CONSERVATION

Oblige l'archivage pendant 7 ans après le moment de l'identification du client ou, dans le cas de relations d'affaires, après leur cessation.

18.7. DEVOIR D'EXAMEN

Impose l'obligation d'examiner avec un soin et une attention particuliers, en intensifiant le degré et la nature de sa surveillance, les comportements, activités ou opérations dont les caractéristiques les rendent susceptibles d'être liées à des fonds ou autres biens provenant d'une activité criminelle, ou d'être liées au financement du terrorisme.

Sont notamment à prendre en compte les éléments de caractérisation suivants :

- a) La nature, la finalité, la fréquence, la complexité, le caractère inhabituel et atypique de la conduite, des activités ou des opérations ;
- b) L'absence apparente d'un objectif économique ou d'un but légitime associé à la conduite, à l'activité ou aux opérations ;
- c) Les montants, l'origine et la destination des transactions ;
- d) Le lieu d'origine et de destination des transactions ;
- e) Les moyens de paiement utilisés ;
- f) La nature, l'activité, le mode de fonctionnement, la situation économique et financière et le profil des personnes impliquées ;

- g) Le type de transaction, de produit, de structure d'entreprise ou de construction juridique qui pourrait favoriser l'anonymat en particulier.

18.8. DEVOIR DE COLLABORATION

Oblige à coopérer promptement et pleinement à toute demande des autorités compétentes (DCIAP-PGR / UIF-PJ), des Autorités judiciaires et policières, de l'Administration fiscale et douanière, et des Autorités sectorielles.

18.9. DEVOIR DE NON-DIVULGATION

Détermine qu'aucune information ne peut être divulguée aux clients ou à des tiers, à savoir des informations relatives à des communications faites, en cours ou sur le point d'être faites aux autorités compétentes, ou concernant des demandes d'information de leur part, ou se trouvant en cours d'enquête, de recherche, d'investigation, d'analyse ou de procédure judiciaire par les autorités susmentionnées. Le devoir impose la prudence nécessaire à l'égard des clients dans le cadre de l'exécution d'opérations particulièrement suspectes, en évitant toute diligence qui, pour quelque raison que ce soit, pourrait laisser soupçonner que des procédures visant à vérifier des pratiques suspectes en matière de BC/FT sont en cours.

Le non-respect de cette obligation par les collaborateurs et l'institution financière peut entraîner des infractions pénales, passibles d'une peine de prison et d'une amende.

18.10. DEVOIR DE FORMATION

Oblige la réalisation d'actions de formation spécifiques et régulières permettant aux collaborateurs de reconnaître les opérations pouvant être liées au BC/FT et d'agir conformément à la loi et aux normes réglementaires qui la mettent en œuvre.

19 GESTION DE DOCUMENTS

19.1 PROPRIÉTÉ, INTERPRÉTATION, VALIDITÉ ET RÉVISION PÉRIODIQUE

L'approbation de ce document est assignée à l'organe de direction de NOVO BANCO, S.A..

L'interprétation et l'adéquation de leur contenu relèvent de la responsabilité du Comité de Compliance.

Son contenu et son adéquation sont revus périodiquement, en même temps que la révision et la mise à jour du modèle de risque de NOVO BANCO, ou chaque fois que des changements juridiques et réglementaires sont apportés ou que d'autres éléments sont considérés comme pertinents par la fonction de contrôle du risque BCFT.

Pour tout éclaircissement sur les présentes Politiques, contactez l'UPBCFT - Unité de Prévention et de Détection du Blanchiment de Capitaux du Département de Compliance.

19.2 GESTION DES DOCUMENTS CONNEXES

Dans le cadre global des compétences et du champ d'intervention de l'UPDBCFT - Unité de Prévention et de Détection du Blanchiment de Capitaux et du Financement du Terrorisme (UPDBCFT) du Département de *Compliance*, en plus des Politiques Générales de Gestion des Risques BCFT, abordées dans ce document, il existe une prise en compte effective et intégrée dans la portée et le contexte de chaque processus opérationnel, de l'évaluation du Risque de *compliance*, communément appelée *Risk Assessment*, suivant les pratiques les plus actuelles du marché et les normes légales récentes en vigueur, qui est traitée dans un autre document séparé, défini comme connexe - le Modèle de Gestion des Risques de Blanchiment de Capitaux et de Financement du Terrorisme.

Le Modèle de Gestion des Risques a été développé avec l'objectif principal de créer un modèle conforme à la législation et à la réglementation en vigueur et en même temps adapté à la réalité de la Banque, basé sur:

- L'identification et l'évaluation des facteurs de risque applicables à la Banque, en tenant compte de la législation et de la réglementation, ainsi que des bonnes pratiques du secteur ;
- L'évaluation du système de contrôle interne de PBC/FT et les Sanctions de la Banque, en cartographiant les risques et les contrôles, afin d'identifier les domaines où le système de contrôle interne doit être renforcé ;
- Cartographie et solution des recommandations des audits internes et externes réalisés sur le système de contrôle interne.

ANNEXES

A. LISTE DES PAYS NON-COOPÉRANTS PUBLIÉE PAR LE FATF/GAFI²⁵

Le Groupe d'action financière (GAFI) agit pour identifier les juridictions qui présentent des lacunes stratégiques en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme et qui n'ont pas fait de progrès suffisants pour y remédier et/ou qui n'ont pas convenu d'un plan d'action avec le GAFI à cette fin.

Dans ce contexte, le GAFI publie trois fois par an des "Communiqués" identifiant les juridictions considérées comme "à risque élevé" et "non coopératives"²⁶.

Selon le dernier communiqué, publié à la suite de la réunion plénière du 23 octobre 2020 (Paris), les juridictions suivantes ont été mises à jour et identifiées :

FATF PUBLIC STATEMENT		IMPROVING GLOBAL AML/CTF COMPLIANCE	
Juridictions soumises à l'application de contre-mesures		Juridictions soumises à un examen particulier des risques qui leur sont associés	
SESSION PLÉNIÈRE 23 OCTOBRE 2020 (Paris)	République Populaire Démocratique de Corée (Corée du Nord)	-	Barbade, Commonwealth des Bahamas, Jamaïque, Myanmar, Royaume du Cambodge République d'Albanie, République Arabe Syrienne République du Botswana, République du Ghana République du Yémen, République Islamique du Pakistan, République de Maurice, République du Nicaragua République du Panama République de l'Ouganda, République du Zimbabwe
	République Islamique d'Iran		

Les informations figurant dans ce tableau doivent être confirmées à l'adresse électronique indiquée dans la note 23, compte tenu des mises à jour périodiques des communiqués émis par le FATF/GAFI.

²⁵ Divulgué par la Lettre circulaire de la Banque du Portugal.

²⁶ Notifications disponibles pour consultation à l'adresse "[http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc\(fatf_releasedate\)](http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate))", qui contient l'historique des "juridictions à risque élevé et non coopératives" qui ont été identifiées tout au long des années.

B. PAYS TIERS PRÉSENTANT DES DÉFICIENCES STRATÉGIQUES EN DANS LE CADRE DE BC/FT, JURIDICTIONS FISCALES NON COOPÉRATIVES ET ORDRES JURIDIQUES OFFSHORE

Liste des pays tiers présentant des déficiences stratégiques dans leur cadre de lutte contre le blanchiment de capitaux et le financement du terrorisme, publiée par la Commission européenne le 13 février 2019.

- Afghanistan
- Samoa Américaine
- Bahamas
- Botswana
- République Populaire Démocratique de Corée
- Éthiopie
- Ghana
- Guam
- Iran
- Iraq
- Libbie
- Nigéria
- Pakistan
- Panamá
- Porto Rico
- Samoa
- Arabie Saudia
- Sri Lanka
- Syrie
- Trinidad et Tobago
- Tunisie
- Îles Vierges des États-Unis
- Yémen

Liste des juridictions fiscales non coopératives, également publiée par la Commission européenne (dernière mise à jour le 06 octobre 2020) :

- Samoa Américaine
- Anguilla
- Barbade
- Îles Fiji
- Guam
- Palau

- Panamá
- Samoa
- Trinidad et Tobago
- Îles Vierges Américaines
- Vanuatu
- Seychelles

Liste des entités juridiques offshore, publiée à l'Annexe III de la notification n° 8/2016 de la Banque du Portugal.

- Anguilla
- Antigua et Barbuda
- Antilles néerlandaises
- Aruba
- Bahamas
- Bahreïn
- Barbade
- Belize
- Bermudes
- Bolivie
- Brunei
- Cap-Vert
- Îles du Canal
- Îles Cayman
- Îles Cocos (Keeling)
- Chypre
- Îles Cook
- Costa Rica
- Delaware
- Dominique
- Égypte
- Émirats Arabes Unis
- Îles Falkland ou Malouines
- Fiji
- Philippines
- Gambie
- Grenade
- Gibraltar
- Île de Guam
- Guatemala
- Guyane

- Honduras
- Hong-Kong
- Yémen
- Indonésie
- Iran
- Jamaïque
- Djibouti
- Jordanie
- Kiribati
- Koweït
- Liban
- Libéria
- Liechtenstein
- Région Administrative Spécial de Macao
- Malaisie
- Maldives
- Île de Man
- Îles Mariannes du Nord
- Îles Marshall
- Mauricie
- Îles Mineures (EUA)
- Myanmar
- Monaco
- Montserrat
- Nauru
- Îles de Noël
- Nevada
- Nigéria
- Île de Niue
- Île Norfolk
- Oklahoma
- Oman
- États fédérés de Micronésie
- Îles Palau
- Panamá
- Pakistan
- Île de Pitcairn
- Polynésie Française
- Porto Rico
- Qatar
- Îles Salomon

- Samoa Américaine
- Samoa Occidentale
- Sainte Lucie
- Sainte-Hélène, Ascension et Tristan da Cunha
- Saint-Christophe-et-Niévès
- Saint Marin
- São Tomé e Príncipe
- Île de Saint Pierre et Miquelon
- Saint Vincent et les Grenadines
- Îles Sandwich du Sud
- Seychelles
- Singapour
- Swaziland
- Suisse
- Îles Svalbard
- Tokelau
- Tonga
- Trinidad et Tobago
- Îles Turks et Caicos
- Turkménistan
- Tuvalu
- Ukraine
- Uruguay
- Ouzbékistan
- Vanuatu
- Îles Vierges Britanniques
- Îles Vierges des États-Unis d'Amérique
- Wyoming

C. LISTE DES PERSONNES POLITIQUEMENT EXPOSÉES (PEP'S) ET LISTE DES TITULAIRES D'AUTRES FONCTIONS POLITIQUES ET PUBLIQUES.

. LISTE DES PERSONNES POLITIQUEMENT EXPOSÉES (PEP's)

- i) Chefs d'État, chefs de gouvernement et membres du gouvernement, à savoir ministres, secrétaires et sous-secrétaires d'État ou équivalent ;
- ii) Députés ;
- iii) Juges de la Cour Constitutionnelle, de la Cour Suprême de Justice, de la Cour Administrative Suprême, de la Cour des Comptes, ainsi que les membres des cours suprêmes, des cours constitutionnelles et des autres instances judiciaires de haut niveau d'autres Etats et d'organisations internationales ;
- iv) Représentants de la République et membres des organes de gouvernement des régions autonomes ;
- v) Médiateur, Conseillers d'État et membres de la Commission Nationale de Protection des Données, du Conseil Supérieur de la Magistrature, du Conseil Supérieur des Tribunaux Administratifs et Fiscaux, du Bureau du Procureur Général, du Conseil Supérieur du Ministère Public, du Conseil Supérieur de la Défense Nationale, du Conseil Économique et Social et de l'Autorité de Régulation des Médias ;
- vi) Chefs de missions diplomatiques et de postes consulaires ;
- vii) Officiers Généraux des Forces Armées en service actif ;
- viii) Présidents et conseillers exerçant des fonctions exécutives des conseils municipaux ;
- ix) Membres des organes d'administration et de surveillance des banques centrales, y compris la Banque centrale européenne ;
- x) Membres des organes d'administration et de surveillance des instituts publics, des fondations publiques, des établissements publics et des entités administratives indépendantes, quel que soit leur mode de désignation ;
- xi) Membres des organes de gestion et de surveillance des entités appartenant au secteur des entreprises publiques, y compris les secteurs des entreprises, régional et local ;
- xii) Membres des organes exécutifs de direction des partis politiques au niveau national ou régional ;
- xiii) Directeurs, directeurs adjoints et membres du conseil d'administration ou les personnes exerçant des fonctions équivalentes dans une organisation internationale.

.. LISTE DES TITULAIRES D'AUTRES FONCTIONS POLITIQUES OU PUBLIQUES

Les fonctions énumérées au point 3 de l'article 4 de la loi 4/83, du 2 avril, sur le contrôle public du patrimoine des titulaires de fonctions politiques, modifiée par les lois 38/83, du 25 octobre, 25/95, du 18 août, 19/2008, du 21 avril, 30/2008, du 10 juillet, et 38/2010, du 2 septembre, lorsqu'ils ne déterminent pas la qualification du titulaire respectif en tant que « personne politiquement exposée » ;

- a. Titulaires d'un organe de direction d'une société dans laquelle l'État détient une participation, lorsqu'ils sont désignés par cette dernière ;
 - b. Membres des entités publiques indépendantes prévues par la Constitution ou par la loi ;
 - c. Membres des organes directeurs des instituts publics ;
 - d. Gestionnaires publics ;
 - e. Membres des organes exécutifs des entreprises appartenant au secteur des entreprises local ;
 - f. Titulaires d'une fonction de direction de niveau supérieur de 1^o degré ou équivalent.
- ii) Membres de l'organe représentatif ou exécutif d'une zone métropolitaine ou d'autres formes d'association municipale ;

D. ANNEXE III DE LA LOI N° 83/2017, DU 18 AOÛT - LISTE NON EXHAUSTIVE DES FACTEURS ET TYPES INDICATIFS DE RISQUE POTENTIELLEMENT PLUS ÉLEVÉ, EN COMPLÉMENT DES SITUATIONS SPÉCIFIQUEMENT PRÉVUES PAR LA LOI.

1 – Facteurs de risque inhérents au client :

- a) Relations d'affaires qui se déroulent dans des circonstances inhabituelles ;
- b) Clients résidant ou opérant dans des zones à risque géographique élevé, déterminées conformément au paragraphe 3 de la présente annexe ;
- c) Personnes morales ou constructions juridiques qui seraient des structures de détention d'actifs personnels ;
- d) Sociétés ayant des actionnaires fiduciaires (*nominee shareholders*) ou dont le capital est représenté par des actions au porteur ;
- e) Clients exerçant des activités impliquant des transactions à forte intensité de liquidités ;
- f) Structures de propriété ou de contrôle du client qui semblent inhabituelles ou excessivement complexes compte tenu de la nature de l'activité exercée par le client.

2 – Facteurs de risque inhérents au produit, au service, à l'exploitation ou au canal de distribution :

- a) Private Banking;
- b) Produits ou opérations susceptibles de favoriser l'anonymat ;
- c) Paiements reçus de tiers inconnus ou non associés au client ou à l'activité poursuivie par le client ;
- d) Nouveaux produits et nouvelles pratiques commerciales, y compris les nouveaux mécanismes de distribution et les nouvelles méthodes de paiement, ainsi que l'utilisation de technologies nouvelles ou en développement, tant pour les produits nouveaux que pour les produits existants.

3 – Facteurs de risque inhérents à la situation géographique

- a) Pays identifiés par des sources fiables, telles que des rapports publiés d'évaluation mutuelle, d'évaluation détaillée ou de suivi, comme ne disposant pas de systèmes efficaces de prévention et de lutte contre le blanchiment de capitaux et le financement du terrorisme, sans préjudice des dispositions de la présente loi concernant les pays tiers à risque élevé ;
- b) Pays ou juridictions identifiés par des sources crédibles comme ayant un niveau significatif de corruption ou d'autres activités criminelles ;
- c) Pays ou juridictions faisant l'objet de sanctions, d'embargos, d'autres mesures restrictives ou de contre-mesures supplémentaires imposées, entre autres, par les Nations unies et l'Union européenne ;
- d) Pays ou juridictions qui financent ou soutiennent des activités ou actes terroristes, ou sur le territoire desquels opèrent des organisations terroristes.