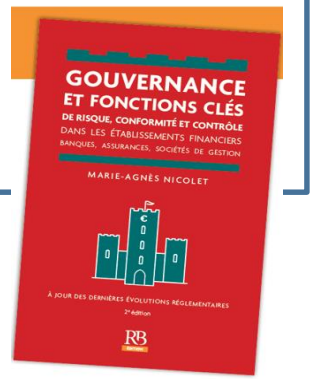
Conférence EIFR 20 juin - les enjeux de la régulation-LCB FT et PSEE



Marie-Agnès NICOLET
Présidente et fondatrice
REGULATION PARTNERS
35 Bd Berthier-75017 PARIS
marieagnes.nicolet@regulationpartners.com
mob : 06 58 84 77 40 | tél : 01 46 22 65 34

Sommaire

Champ d'application

Le rapport final de l'EBA sur les orientations relatives aux accords d'externalisation est applicable conjointement avec les dispositions prévues dans la Directive MIF2 2014/65/UE, le règlement délégué 2017/565 (Organisation des PSI), La Directive CRD IV 2013/36/UE, La Directive 2015/2366 DSP2 et la Directive 2009/110/CE EM, de ce fait les établissements assujettis sont :

- Les établissements de crédit ;
- Les entreprises d'investissement ;
- Les établissements de paiement et
- Les établissements de monnaie électronique (EME).

Ci-après dénommées « établissement(s) » ou « institution(s) ».

Modalités & Date d’application

Le rapport s’applique à compter du 30 septembre 2019 à tous les accords d'externalisation conclus, revus ou modifiés à cette date ou ultérieurement.

Le paragraphe 63 (b) relatif à l’externalisation des fonctions d'activités bancaires ou de services de paiement, dans la mesure où l'exercice de cette fonction nécessite une autorisation ou un enregistrement par une autorité compétente de l'État membre dans lequel elles sont autorisées, à un prestataire de services situé dans un pays tiers ne soit réalisée que si les conditions prévues par le rapport sont remplies : s'applique à compter du 31 décembre 2021.

Les institutions assujetties devraient examiner et modifier en conséquence les accords d'externalisation existants afin de s'assurer qu'ils sont conformes aux présent rapport.

Lorsque l'examen des accords d'externalisation de fonctions critiques ou importantes n'est pas achevé au 31 décembre 2021, les institutions devraient en informer leur autorité compétente, y compris les mesures prévues pour achever cet examen ou l'éventuelle stratégie de sortie.

Principe de proportionnalité & Particularité des groupes d'entreprises (1/3)

1. Principe de proportionnalité

- Le principe de proportionnalité vise à garantir que les modalités de gouvernance, y compris celles liées à l'externalisation, sont compatibles avec le profil de risque individuel, la nature et le modèle économique de l'institution, ainsi que l'ampleur et la complexité de ses activités, afin que les objectifs des exigences réglementaires soient effectivement atteints.

2. Externalisation au sein d'un groupe :

- Conformément à l'Article 109 (2) de la CRD IV 2013/36/EU, les dispositions prévues par l'EBA devraient s'appliquer sur la base sous-consolidée et consolidée du groupe. À cette fin, les entreprises mères dans un État membre de l'UE devraient veiller à ce que les dispositifs, processus et mécanismes de gouvernance internes dans leurs filiales, soient cohérents, bien intégrés et adéquats pour l'application effective du rapport de l'EBA.

Principe de proportionnalité & Particularité des groupes d'entreprises (2/3)

2. Externalisation au sein d'un groupe : (Suite)

- Les institutions, utilisant les dispositifs de gouvernance centralisés, devraient se conformer aux dispositions suivantes :
  - Lorsque ces institutions ont conclu des accords d'externalisation avec des prestataires de services au sein du groupe, l'organe de direction de ces institutions conserve l'entière responsabilité du respect de toutes les exigences réglementaires et de l'application efficace des dispositions du rapport ;
  - Lorsque ces institutions externalisent les tâches opérationnelles des fonctions de contrôle interne à un prestataire de services au sein du groupe, même pour le suivi et l'audit des accords d'externalisation, ces institutions devraient veiller à ce que ces tâches opérationnelles sont exécutées efficacement conformément aux dispositions en vigueur.

Principe de proportionnalité & Particularité des groupes d'entreprises (3/3)

Par ailleurs, les institutions au sein d'un groupe, les établissements qui sont un organisme central ou qui sont affiliés en permanence à un organisme central, ou les établissements qui sont affiliés à un régime de protection institutionnel devraient prendre en considération les éléments suivants:

- Lorsque le suivi opérationnel de l'externalisation est centralisé, les institutions devraient veiller à ce qu'il ait un suivi indépendant et un contrôle approprié, au moins pour les fonctions critiques ou importantes externalisées. Sur une base annuelle et sur demande de la fonction centrale, des rapports comprenant au moins une synthèse de l'évaluation des risques et du suivi des résultats.
- L'information de l'organe central de tout changement pertinent concernant les prestations externalisées, notamment pour les fonctions critiques et importantes ;
- Lorsque l'évaluation préalable à l'externalisation des accords d'externalisation est centralisée, chaque institution appartenant au groupe devrait recevoir un résumé de l'évaluation et veiller à prendre en compte la structure spécifique et les risques liés à cette externalisation dans le processus décisionnel ;
- Lorsque le registre de tous les accords d'externalisation existants est établi et maintenu de façon centralisée au sein d'un groupe, les institutions devraient pouvoir obtenir leur propre registre sans retard excessif. Ce registre devrait inclure tous les accords d'externalisation, y compris les accords d'externalisation conclus avec des prestataires de services au sein de ce groupe ;
- Lorsque les institutions s'appuient sur un plan de sortie pour une fonction critique ou importante qui a été établie au niveau du groupe ou par l'organe central, tous les établissements et établissements de paiement devraient recevoir un résumé du plan et être assurés que ce plan peut être effectivement exécuté.

L’évaluation des accords d’externalisation (1/2)

Les institutions assujetties devraient déterminer si un accord conclu avec un tiers relève de la définition de l'externalisation.

Dans le cadre de cette évaluation, il convient d'examiner les points suivants :

- si la fonction (ou une partie de celle-ci) qui est externalisée à un prestataire de services **est exercée de manière récurrente ou continue par ce dernier ; et**
- **si cette fonction (ou partie de cette fonction) relève normalement de fonctions qui seraient ou pourraient raisonnablement être exercées par des établissements assujettis**, même si cet établissement ou cet établissement ne s'est jamais acquitté de cette fonction dans le passé.

Lorsqu'un accord conclu avec un prestataire de services couvre plusieurs fonctions, les institutions devraient tenir compte de tous les aspects de l'accord dans leur évaluation, par exemple, si le service fourni comprend la fourniture de matériel de stockage de données et la sauvegarde des données, les deux aspects devraient être examinés ensemble.

L’évaluation des accords d’externalisation (2/2)

En règle générale, les institutions ne devraient pas considérer les éléments suivants comme de l'externalisation :

- Une fonction dont l'exercice est légalement requis par un prestataire de services, par exemple le contrôle légal des comptes ;
- Les services d'information sur les marchés (par exemple, fourniture de données par Bloomberg, Moody's, Standard & Poor's, Fitch) ;
- Les infrastructures de réseau mondiales (p. ex. Visa, MasterCard) ;
- Les mécanismes de compensation et de règlement entre les chambres de compensation, les contreparties centrales et les institutions de règlement et leurs membres ;
- Les infrastructures mondiales de messagerie financière qui sont soumises à la surveillance des autorités compétentes ;
- Les services de correspondants bancaires ; et
- L'acquisition de services comme les conseils d'un architecte, la fourniture d'avis juridiques et la représentation devant les tribunaux et les organes administratifs, le nettoyage, le jardinage et l'entretien des locaux de l'établissement, les services médicaux, le service des voitures de fonction, la restauration, les services des distributeurs automatiques, le service de secrétariat, les services de voyage, le service à la réception, les secrétaires et le standard) et de biens (cartes plastiques, lecteurs de cartes, fournitures de bureau, ordinateurs personnels, meubles) ou services publics (électricité, gaz, eau, ligne téléphonique).

Les fonctions critiques et importantes

Les institutions devraient toujours considérer une fonction comme critique ou importante dans les situations suivantes :

- Lorsqu'un défaut ou une défaillance dans l'exécution de ses fonctions porterait atteinte de façon importante :
  - au respect continu des conditions de leur autorisation ou des autres obligations qui leur incombent en vertu des réglementations en vigueur (CRD IV, MIFID2, DSP2, DEME…) ;
  - A leur rendement financier ; ou
  - A la solidité ou la continuité de leurs services et activités bancaires et de paiement ;
- Lorsque les tâches opérationnelles des fonctions de contrôle interne sont externalisées, à moins que l'évaluation n'établisse que le fait de ne pas fournir la fonction externalisée ou de la fournir de manière inappropriée n'aurait pas d'incidence négative sur l'efficacité de la fonction de contrôle interne ;
- Lorsqu'ils ont l'intention d'externaliser les fonctions d'activités bancaires ou de services de paiement dans une mesure qui nécessiterait l'autorisation d'une autorité compétente.

Cadre de gouvernance

Dans le cadre de contrôle interne global, les institutions devraient disposer d'un cadre global de gestion des risques à l'échelle de l'établissement qui s'étendrait à tous les secteurs d'activité et à toutes les unités internes.

Dans ce cadre, les institutions devraient identifier et gérer tous leurs risques, y compris les risques résultant d'accords avec des tiers. Le cadre de gestion des risques devrait également permettre aux établissements financiers de prendre des décisions éclairées en matière de prise de risques et de veiller à ce que les mesures de gestion des risques soient correctement mises en œuvre, notamment en ce qui concerne les cyber-risques. Ces institutions devraient :

- Attribuer clairement les responsabilités de la documentation et des accords d'externalisation ;
- Allouer les ressources suffisantes pour assurer le respect des exigences réglementaires, y compris les orientations de l'EBA, la documentation et le suivi de tous les accords d'externalisation ;
- **Créer une fonction d'externalisation ou désigner un cadre supérieur directement responsable devant l'organe de direction (par exemple, un titulaire d'une fonction clé d'une fonction de contrôle) et chargé de gérer et de superviser les risques liés aux accords d'externalisation dans le cadre du contrôle interne des institutions et de superviser la documentation relative à ces accords.**

Les institutions de petite taille et moins complexes devraient au moins assurer une répartition claire des tâches et des responsabilités en matière de gestion et de contrôle des accords d'externalisation et peuvent confier la fonction d'externalisation à un membre de l'organe de direction de l'établissement.

Pratiques de gouvernance et risques des tiers

L'externalisation des fonctions n'entraîne pas de délégation des responsabilités de la direction. Les établissements financiers devraient respecter toutes les obligations réglementaires. En particulier, la supervision de l'externalisation d'une fonction critique ou importante doit toujours être faite par l'établissement.

Le respect des conditions fixées par l'autorité compétente auxquelles l'établissement financier doit se conformer

L'organisation interne de l'établissement financier

La mise en place des stratégies relatives au business model et à la gestion des risques

La gestion quotidienne de l'établissement, y compris la gestion des risques associés à l'externalisation

le rôle de surveillance de l'organe de direction dans sa fonction de surveillance, y compris la surveillance et le contrôle du processus décisionnel de la direction.

L'identification, l'évaluation et la gestion des conflits d'intérêts.

La politique d'externalisation

La direction devrait approuver et maintenir une politique écrite d'externalisation et assurer sa mise en œuvre, sur une base consolidée, sous-consolidée et individuelle.

Les établissements financiers devraient veiller à ce que la politique couvre les effets potentiels des accords d'externalisation critiques ou importants sur le profil de risque, la capacité à superviser le prestataire et à gérer les risques, les mesures de continuité des activités et la performance des établissements.

La politique d'externalisation

La politique devrait inclure les principales phases du cycle de vie des accords d'externalisation et définir les principes, les responsabilités et les processus liés à l'externalisation. En particulier, la politique devrait couvrir au moins :

- Les responsabilités de la direction, des secteurs d'activité, des fonctions de contrôle interne ;
- La planification des accords d'externalisation (Business plan, critères, identification des risques, procédure, évaluation et gestion des conflits d'intérêts) ;
- La mise en œuvre, le suivi et la gestion des accords d'externalisation (évaluation continue de la performance du prestataire de service, le processus de renouvellement, procédure de notification et de réponses de modification de l'accord d'externalisation) ;
- les stratégies de sortie et les processus de résiliation, y compris l'exigence d'un plan de sortie documenté pour chaque fonction critique ou importante à externaliser lorsqu'une telle sortie est jugée possible compte tenu d'éventuelles interruptions de service ou de la résiliation imprévue d'un accord d'externalisation.

Conflits d’intérêts

Les institutions assujetties devraient identifier, évaluer et gérer les conflits d’intérêts en ce qui concerne les accords d’externalisation de l’établissement financier.

Lorsque l’externalisation crée des conflits d'intérêts importants, surtout entre des entités d'un même groupe, les établissements financiers doivent prendre les mesures appropriées pour gérer ces conflits d'intérêts.

Lorsque les fonctions sont assurées par un prestataire de services faisant partie d'un groupe, les conditions, y compris les conditions financières, du service externalisé devraient être fixées de manière indépendante. Toutefois, dans la tarification des services, des synergies résultant de la fourniture de services identiques ou similaires à plusieurs institutions au sein d'un groupe peuvent être prises en compte, pour autant que le prestataire de services reste viable sur une base autonome

Plan de continuité d’activité

Les institutions devraient avoir mis en place, maintenir et tester périodiquement des plans appropriés de continuité d'activité pour les fonctions critiques ou importantes externalisées. Les établissements faisant partie d'un groupe peuvent s'appuyer sur des plans de continuité d'activité établis au niveau central concernant leurs fonctions externalisées.

Les plans de continuité des opérations devraient tenir compte de l'éventualité où la qualité de la prestation de la fonction essentielle ou importante externalisée se détériore à un niveau inacceptable ou échoue. Ces plans devraient également tenir compte de l'impact potentiel de l'insolvabilité ou d'autres défaillances des prestataires de services et, le cas échéant, des risques politiques dans la juridiction du prestataire de services.

Fonction d’audit interne

Les activités de la fonction d'audit interne devraient couvrir, selon une approche fondée sur les risques, l'examen indépendant des activités externalisées. Le plan et le programme d’audit devraient notamment comprendre les accords d’externalisation de fonctions critiques ou importantes, y compris la pertinence des mesures de protection des données, des contrôles de gestion des risques et des mesures de continuité des activités mises en œuvre par le prestataire de services

En ce qui concerne le processus d'externalisation, la fonction d'audit interne devrait au moins vérifier :

- Que le cadre d'externalisation de l'établissement, y compris la politique d'externalisation, est correctement et effectivement mis en œuvre et est conforme aux lois et règlements applicables, à la stratégie en matière de risques et aux décisions de l'organe de direction ;
- L'adéquation, la qualité et l'efficacité de l'évaluation de la criticité ou de l'importance des fonctions ;
- L'adéquation, la qualité et l'efficacité de l'évaluation des risques pour les accords d'externalisation et le fait que les risques restent conformes à la stratégie de risque de l'établissement ;
- La participation appropriée des organes de gouvernance

Les exigences en matière d'externalisation « Registre » (1/5)

Dans le cadre de leur gestion des risques, les établissements devraient tenir à jour un registre d'informations sur tous les accords d'externalisation au sein de l'établissement et, le cas échéant, aux niveaux sous-consolidé et consolidé, et devraient dûment documenter tous les accords d'externalisation en vigueur, en faisant une distinction entre l'externalisation des fonctions critiques ou importantes et les autres accords d'externalisation.

Compte tenu du droit national, les institutions devraient conserver la documentation relative aux accords d'externalisation échus dans le registre et les pièces justificatives pendant une période appropriée.

Pour les établissements au sein d'un groupe, les établissements affiliés en permanence à un organisme central, le registre peut être tenu de manière centralisée.

Les exigences en matière d'externalisation « Registre » (2/5)

Le registre devrait comprendre au moins les renseignements suivants pour tous les accords existants :

- Un numéro de référence pour chaque accord ;
- La date de début et, le cas échéant, la prochaine date de renouvellement du contrat, la date de fin et/ou les délais de préavis pour le prestataire de services et pour l'établissement ;
- Une brève description de la fonction externalisée, y compris les données qui sont externalisées et si des données à caractère personnel (par exemple, en fournissant un oui ou un non dans un champ de données séparé) ont été transférées ou si leur traitement est sous-traité à un prestataire de services ;
- Une catégorie attribuée par l'établissement qui reflète la nature de la fonction décrite au point c) (par exemple, technologie de l'information (TI), fonction de contrôle), ce qui devrait faciliter l'identification des différents types de dispositifs ;
- Le nom du prestataire de services, le numéro d'immatriculation de la société, l'identifiant de la personne morale (le cas échéant), l'adresse enregistrée et les autres coordonnées pertinentes, ainsi que le nom de sa société mère (le cas échéant) ;
- Le ou les pays où le service doit être fourni, y compris l'emplacement (pays ou région) des données ;
- Si oui ou non (oui ou non) la fonction externalisée est considérée comme critique ou importante, y compris, le cas échéant, un bref résumé des raisons pour lesquelles la fonction externalisée est considérée critique ou importante;
- Dans le cas de l'externalisation à un fournisseur de services de cloud, les modèles de services et de déploiement, c'est-à-dire public/privé/hybride/communauté, et la nature spécifique des données à conserver et les lieux (c'est-à-dire les pays ou régions) où ces données seront stockées ;
- La date de l'évaluation la plus récente de la criticité ou de l'importance de la fonction externalisée.

Les exigences en matière d'externalisation « Registre » (3/5)

Pour l'externalisation de fonctions critiques ou importantes, le registre devrait comprendre au moins les informations supplémentaires suivantes :

- La date de la dernière évaluation des risques et un bref résumé des principaux résultats ;
- La personne ou l'organe de décision (par exemple, l'organe de direction) de l'institution qui a approuvé l'accord d'externalisation ;
- Le droit applicable du contrat ;
- Les dates des vérifications les plus récentes et des prochaines vérifications prévues, le cas échéant ;
- Le cas échéant, le nom des sous-traitants auxquels des parties importantes d'une fonction essentielle ou importante sont sous-traitées, y compris le pays où les sous-traitants sont enregistrés, où le service sera exécuté et, le cas échéant, le lieu (pays ou région) où les données seront stockées ;
- Un résultat de l'évaluation de la substituabilité du prestataire de services (comme étant facile, difficile ou impossible), la possibilité de réintégrer une fonction critique ou importante dans l'institutions ou l'impact de la suppression de la fonction critique ou importante ;
- L'identification d'autres prestataires de services ;
- La question de savoir si la fonction essentielle ou importante impartie appuie les opérations commerciales dont le délai d'exécution est critique ;
- Le coût budgétaire annuel estimé.

Les exigences en matière d'externalisation « Registre » (4/5)

Les institutions assujetties devraient, sur demande, mettre à la disposition de l'autorité compétente soit le registre complet de tous les accords d'externalisation existants, soit des sections spécifiques de ce registre, telles que des informations sur tous les accords d'externalisation. Les établissements et les établissements de paiement devraient fournir ces informations sous une forme électronique traitable (par exemple, un format de base de données couramment utilisé, des valeurs séparées par des virgules).

Les institutions devraient informer les autorités compétentes de manière adéquate au sujet de l'externalisation envisagée de fonctions critiques ou importantes et/ou lorsqu'une fonction externalisée est devenue critique ou importante.

Les exigences en matière d'externalisation « Registre » : Cas particulier (5/5)

Conformément à la DSP2 2015/2366, les institutions devraient informer les autorités compétentes de manière adéquate et en temps utile ou engager un dialogue prudentiel avec les autorités compétentes au sujet de l'externalisation envisagée de fonctions critiques ou importantes et/ou lorsqu'une fonction externalisée est devenue critique ou importante et fournir au moins les informations. Les institutions devraient documenter de manière appropriée les évaluations effectuées et les résultats de leur surveillance continue (par exemple, la performance du prestataire de services, le respect des niveaux de service convenus, les autres exigences contractuelles et réglementaires, les mises à jour de l'évaluation des risques).

Les institutions devraient informer en temps utile les autorités compétentes des changements importants et/ou des événements graves concernant leurs accords d'externalisation qui pourraient avoir une incidence importante sur la poursuite des activités commerciales de l'institution.

L'institutions devraient documenter de manière appropriée les évaluations effectuées et les résultats de leur surveillance continue (par exemple, la performance du prestataire de services, le respect des niveaux de service convenus, les autres exigences contractuelles et réglementaires, les mises à jour de l'évaluation des risques).

Le processus d'externalisation

Le rapport de l'EBA prévoit un processus à respecter avant l'externalisation d'une activité ou une fonction :

- Evaluer si l'externalisation concerne une fonction critique ou importante ;
- Mettre en place des Due Diligence sur le prestataire de services ;
- Identifier et évaluer tous les risques de l 'accord d'externalisation ;
- Identifier et évaluer les conflits d'intérêts que l'externalisation peut engendrer ;
- Prendre en compte les conséquences de l'endroit où se trouve le prestataire de services (pays tiers ou non) ;
- Déterminer si le prestataire de services fait partie du groupe de consolidation comptable de l'établissement, si c'est le cas il faut savoir dans quelle mesure l'établissement peut influencer les actions du prestataire.

Contrôle des fonctions externalisées

Les institutions devraient surveiller en permanence la performance des prestataires de services en ce qui concerne tous les accords d'externalisation selon une approche fondée sur les risques, l'accent étant mis principalement sur l'externalisation de fonctions critiques ou importantes, notamment la disponibilité, l'intégrité et la sécurité des données et des informations. Lorsque le risque, la nature ou l'ampleur d'une fonction externalisée ont sensiblement changé, les établissements devraient réévaluer la criticité ou l'importance de cette fonction.

Les institutions devraient veiller en permanence à ce que les accords d'externalisation, soient conformes aux normes de performance et de qualité appropriées, conformément à leurs politiques et notamment dans le cas des prestations critiques:

- S'assurer qu'ils reçoivent les rapports appropriés des fournisseurs de services ;
- Evaluer le rendement des fournisseurs de services à l'aide d'outils tels que des indicateurs de rendement clés, des indicateurs de contrôle clés, des rapports sur la prestation de services, l'auto-certification et des examens indépendants ; et
- Examiner tous les autres renseignements pertinents reçus du fournisseur de services, y compris les rapports sur les mesures de continuité des opérations

Stratégies de sortie

Les institutions devraient avoir une stratégie de sortie clairement définie pour toute externalisation de fonctions, en tenant compte au moins de :

- La possibilité de résiliation des contrats d'externalisation en cas de défaillance du prestataire de service ;
- En cas de défaillance du prestataire de service ;
- En cas de détérioration de la qualité du service fourni ou de la fonction ou en cas de perturbation sur l'activité ;
- En cas de risque important lié à la prestation.

Lors de l'élaboration d'une stratégie de sortie, les établissements devraient:

- Définir les objectifs de la stratégie de sortie ;
- Effectuer une analyse de l'impact sur l'établissement en fonction du risque des processus, services ou activités externalisés, afin d'identifier les ressources humaines et financières nécessaires pour mettre en œuvre le plan de sortie ;
- Attribuer les rôles, les responsabilités et les ressources suffisantes pour gérer les plans de sortie et la transition des activités ;
- Définir les critères de réussite pour la transition des fonctions et des données externalisées ;
- Définir les indicateurs à utiliser pour la surveillance de l'accord d'externalisation, y compris ceux basés sur la qualité de service qui pourraient inciter à résilier le contrat.

A. RÈGLEMENT DÉLÉGUÉ (UE) 2019/758 DE LA COMMISSION du 31 janvier 2019 complétant la directive (UE) 2015/849 du Parlement européen et du Conseil

- Ce règlement délégué **indique les actions à mettre en œuvre pour traiter efficacement** le risque de blanchiment de capitaux et de financement du terrorisme **lorsqu'une entité assujettie** détient majoritairement des succursales ou des filiales **localisées dans un pays ti**ers et que **le droit de celui-ci ne permet pas de mettre en œuvre les politiques et les procédures à l'échelle du groupe (*4ème Directive, art. 45*).**

- Les dispositions du présent règlement devraient également **être sans préjudice des mesures de vigilance renforcée** que les établissements de crédit et les établissements financiers sont tenus/obligés de prendre lorsqu'ils traitent avec des personnes physiques ou des entités juridiques établies dans des pays recensés par la Commission comme étant à haut risque en application de l'article 9 de la directive (UE) 2015/849.

Ce règlement délégué entre en application à compter du 3 septembre 2019.

1. Objet et champ d'application

L'article 45 de la 4ème directive précise : « Les États membres exigent des entités assujetties qui **font partie d'un groupe** qu'elles mettent en œuvre **des politiques et des procédures à l'échelle du groupe**, notamment des politiques de protection des données ainsi que des politiques et des procédures relatives au partage des informations au sein du groupe aux fins de **la lutte contre le blanchiment de capitaux et le financement du terrorisme.** Ces politiques et procédures sont mises en œuvre efficacement au niveau des succursales et des filiales détenues majoritairement, **établies dans les États membres et dans des pays tiers**. »

Le présent règlement définit un **ensemble de mesures supplémentaires**, dont des actions que doivent au minimum engager les établissements de crédit et les établissements financiers pour **traiter efficacement** le risque de blanchiment de capitaux et de financement du **terrorisme lorsque le droit d'un pays tiers ne permet pas de mettre en œuvre** les politiques et les procédures à l'échelle du groupe visées à l'article 45 de la 4ème la directive au niveau des succursales ou des filiales détenues majoritairement qui font partie du groupe et sont établies dans le pays tiers.

2. Obligations générales pour chaque pays tiers

Pour chaque pays tiers dans lequel ils ont établi une succursale ou sont un actionnaire majoritaire d'une filiale, les établissements de crédit et les établissements financiers veillent au moins :

- A évaluer les risques de blanchiment de capitaux et de financement du terrorisme auxquels leur groupe est exposé, à consigner cette évaluation, à la tenir à jour et à la conserver afin de pouvoir la partager avec leur autorité compétente;
- A faire en sorte que les risques cités précédemment soient dûment pris en compte dans leurs politiques et leurs procédures de lutte contre le blanchiment de capitaux et le financement du terrorisme à l'échelle du groupe;
- A obtenir d'un membre d'un niveau élevé de leur hiérarchie l'autorisation au niveau du groupe pour l'évaluation des risques et pour les politiques et les procédures de lutte contre le blanchiment de capitaux et le financement du terrorisme à l'échelle du groupe
- A fournir une formation ciblée aux membres du personnel concernés dans le pays tiers afin de leur permettre de recenser les indicateurs de risques de blanchiment de capitaux et de financement du terrorisme, et à veiller à ce que cette formation soit efficace.

3. Evaluations individuelles des risques 1/2 art 3

Lorsque le droit du pays tiers **restreint ou interdit l'application de politiques et de procédures** qui sont nécessaires pour **identifier et évaluer** correctement **les risques** de blanchiment de capitaux et de financement du terrorisme liés à une relation d'affaires ou à une transaction conclue à titre occasionnel en raison de restrictions d'accès aux informations pertinentes sur les clients et les bénéficiaires effectifs ou de restrictions de l'utilisation de ces informations à des fins de vigilance à l'égard de la clientèle, les établissements de crédit ou les établissements financiers veillent au moins :

A communiquer à l'autorité compétente de l'État membre d'origine sans délai indu, et en tout état de cause pas plus de 28 jours calendaires après avoir identifié le pays tiers, les informations suivantes:

- Le nom du pays tiers concerné;
- La manière dont la mise en œuvre du droit du pays tiers restreint ou interdit l'application de politiques et de procédures qui sont nécessaires pour identifier et évaluer les risques BC FT.

A faire en sorte que leurs succursales ou leurs filiales détenues majoritairement qui sont établies dans le pays tiers déterminent si l'accord de leurs clients et, le cas échéant, des bénéficiaires effectifs de leurs clients peut être utilisé pour contourner légalement les interdictions du pays tiers.

A faire en sorte que leurs succursales ou leurs filiales détenues majoritairement qui sont établies dans le pays tiers exigent de leurs clients et, le cas échéant, des bénéficiaires effectifs de leurs clients, qu'ils marquent leur accord pour contourner les interdictions, dans la mesure où cela est compatible avec le droit du pays tiers.

3. Evaluations individuelles des risques 2/2 art 3

Si les mesures citées précédemment ne sont pas réalisables, les établissements de crédit et les établissements financiers prennent des mesures supplémentaires

Si un établissement de crédit ou un établissement financier ne peut pas gérer efficacement les risques de blanchiment de capitaux et de financement du terrorisme, il devrait :

- Veiller à ce que la succursale ou la filiale détenue majoritairement mette un terme à la relation d'affaires ;
- Veiller à ce que la succursale ou la filiale détenue majoritairement n'exécute pas la transaction conclue à titre occasionnel ;
- Mettre un terme à certaines ou à l'ensemble des activités assurées par sa succursale ou sa filiale détenue majoritairement, établie dans le pays tiers.

Les établissements de crédit et les établissements financiers déterminent l'étendue des mesures supplémentaires en fonction de leur appréciation des risques et sont en mesure de démontrer à leur autorité compétente que l'étendue des mesures supplémentaires est appropriée au regard des risques de blanchiment de capitaux et de financement du terrorisme.

4. Partage et traitement des données des clients 1/2 art 4

Lorsque le droit d'un pays tiers restreint ou interdit **le partage ou le traitement des données des clients à des fins de lutte contre le blanchiment de capitaux et le financement du terrorisme au sein du groupe**, les établissements de crédit et les établissements financiers veillent au moins:

A communiquer à l'autorité compétente de l'État membre d'origine sans délai indu, et en tout état de cause pas plus de 28 jours après avoir identifié le pays tiers, les informations suivantes:

- Le nom du pays tiers concerné;
- La manière dont la mise en œuvre du droit d'un pays tiers restreint ou interdit le partage ou le traitement des données des clients à des fins de lutte contre le blanchiment de capitaux et le financement du terrorisme

A faire en sorte que leurs succursales ou leurs filiales détenues majoritairement qui sont établies dans le pays tiers déterminent si l'accord de leurs clients et, le cas échéant, des bénéficiaires effectifs de leurs clients peut être utilisé pour contourner légalement les interdictions du pays tiers.

A faire en sorte que leurs succursales ou leurs filiales détenues majoritairement qui sont établies dans le pays tiers exigent de leurs clients et, le cas échéant, des bénéficiaires effectifs de leurs clients, qu'ils marquent leur accord pour contourner les restrictions ou les interdictions, dans la mesure où cela est compatible avec le droit du pays tiers.

4. Partage et traitement des données des clients 2/2 art 4

- Dans les cas où cet accord ne peut être accordé, les établissements de crédit et les établissements financiers prennent **des mesures supplémentaires ainsi que leurs mesures** types de lutte contre le blanchiment de capitaux et le financement du terrorisme pour gérer les risques.

- Si un établissement de crédit ou un établissement financier **ne peut pas gérer efficacement les risques** de blanchiment de capitaux et de financement du terrorisme en appliquant les mesures citées précédemment, **il met un terme à certaines ou à l'ensemble** des activités assurées par sa succursale ou sa filiale détenue majoritairement**, établie dans le pays tiers.**

5. Divulgation d'informations relatives à des transactions suspecte art 5

Lorsque le droit du pays tiers interdit ou restreint **le partage d'informations** visées à l'article 33 de la 4ème directive de Lutte contre le blanchiment de capitaux et de financement du terrorisme par les succursales et les filiales détenues majoritairement, établies dans le pays tiers, avec d'autres entités de leur groupe, les établissements de crédit et les établissements financiers veillent au moins :

A communiquer à l'autorité compétente de l'État membre d'origine sans délai indu, et en tout état de cause pas plus de 28 jours après avoir identifié le pays tiers, les informations suivantes:

- Le nom du pays tiers concerné ;
- La manière dont la mise en œuvre du droit du pays tiers interdit ou restreint le partage ou le traitement du contenu des informations visées à l'article 33 de la 4ème directive identifiées par une succursale ou une filiale détenue majoritairement, établie dans un pays tiers, avec d'autres entités de leur groupe ;

A exiger de la succursale ou de la filiale détenue majoritairement qu'elle fournisse des informations pertinentes aux membres d'un niveau élevé de la hiérarchie de l'établissement de crédit ou de l'établissement financier, afin qu'ils soient en mesure d'évaluer les risques de blanchiment de capitaux et de financement du terrorisme liés à l'exploitation de cette succursale ou de cette filiale détenue majoritairement et l'incidence de ces risques sur le groupe, telles que:

- Le nombre de transactions suspectes signalées au cours d'une période déterminée;
- Les données statistiques agrégées, qui fournissent une vue d'ensemble des circonstances qui ont fait naître des suspicions.

6. Transfert de données des clients aux Etats membres 1/2 art 6

Si le droit du pays tiers interdit ou restreint **le transfert de données relatives aux clients** d'une succursale ou d'une filiale détenue majoritairement, établie dans un pays tiers, vers un État membre aux fins de la surveillance de la lutte contre le blanchiment de capitaux et le financement du terrorisme, les établissements de crédit et les établissements financiers veillent au moins:

A communiquer à l'autorité compétente de l'État membre d'origine sans délai indu, et en tout état de cause pas plus de 28 jours calendaires après avoir identifié le pays tiers, les informations suivantes :

- Le nom du pays tiers concerné ;
- la manière dont la mise en œuvre du droit du pays tiers interdit ou restreint le transfert de données liées aux clients aux fins de la surveillance de la lutte contre le blanchiment de capitaux et le financement du terrorisme;

A effectuer des examens renforcés, et notamment, lorsque cela est proportionné aux risques de blanchiment de capitaux et de financement du terrorisme liés à l'exploitation de la succursale ou de la filiale détenue majoritairement, établie dans le pays tiers, des vérifications sur place ou des audits indépendants, afin de s'assurer que la succursale ou la filiale détenue majoritairement met effectivement en œuvre des politiques et des procédures à l'échelle du groupe et qu'elle identifie, évalue et gère correctement les risques de blanchiment de capitaux et de financement du terrorisme;

6. Transfert de données des clients aux Etats membres 2/2 art 6

A fournir à l'autorité compétente de l'État membre d'origine, à sa demande, les résultats des examens visés au point précédent ;

A exiger de la succursale ou de la filiale détenue majoritairement, établie dans le pays tiers, qu'elle fournisse régulièrement toute information utile aux membres d'un niveau élevé de la hiérarchie de l'établissement de crédit ou de l'établissement financier, y compris au moins les informations suivantes :

- Le nombre de clients à haut risque et les données statistiques agrégées donnant un aperçu des raisons pour lesquelles les clients ont été classés à haut risque, comme le statut de personne politiquement exposée;
- Le nombre de transactions suspectes identifiées et signalées, ainsi que les données statistiques agrégées donnant un aperçu des circonstances qui ont fait naître des suspicions;

A fournir à l'autorité compétente de l'État membre d'origine, à sa demande, les informations citées au point précédent.

7. Conservation des documents et pièces art 7

Lorsque le droit du pays **tiers interdit ou restreint l'application des mesures de conservation de documents et pièces équivalentes** à celles décrites au chapitre V de la directive (UE) 2015/849, les établissements de crédit et les établissements financiers veillent au moins:

À communiquer à l'autorité compétente de l'État membre d'origine sans délai indu, et en tout état de cause pas plus de 28 jours après avoir identifié le pays tiers, les informations suivantes:

- Le nom du pays tiers concerné;
- La manière dont la mise en œuvre du droit du pays tiers interdit ou restreint l'application des mesures de conservation de documents et pièces équivalentes à celles énoncées dans la directive (UE) 2015/849;

À déterminer si l'accord du client et, le cas échéant, de ses bénéficiaires effectifs, peut être utilisé pour contourner légalement les restrictions ou les interdictions concernées.

À faire en sorte que leurs succursales ou filiales détenues majoritairement qui sont établies dans le pays tiers exigent des clients et, le cas échéant, des bénéficiaires effectifs de leurs clients, qu'ils marquent leur accord pour contourner interdictions concernées dans la mesure où cela est compatible avec le droit du pays tiers.

Dans les cas où ces mesures ne sont pas réalisables, les établissements de crédit et les établissements financiers prennent des mesures supplémentaires ainsi que leurs mesures types de lutte contre le blanchiment de capitaux et le financement du terrorisme pour gérer les risques.

B. Lignes directrices relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle

Publiées le 14 décembre 2018, les présentes lignes directrices présentent une analyse des obligations d'identification, de vérification de l'identité et de connaissance de la clientèle ainsi que de conservation des informations et documents, à des fins de LCB-FT.

Elles intègrent notamment :

- ✓ Le renforcement de l'approche par les risques dans la mise en œuvre des mesures de vigilance à l'égard de la clientèle ;
- ✓ La distinction expressément opérée entre l'identification et la vérification de l'identité de la clientèle ;
- ✓ Les nouveautés concernant les mesures de vérification de l'identité ;
- ✓ L'introduction de la notion de bénéficiaire effectif en dernier ressort.

1. Les mesures de vigilances à l'égard de la clientèle en relation d'affaires

Conformément à l'article L.561-2-1 du code monétaire et financier, la notion de relation d'affaires s'entend de la relation professionnelle ou commerciale avec le client, et inclut le cas échéant le bénéficiaire effectif. Une relation d'affaires est nouée lorsqu'une personne mentionnée à l'article L. 561-2 engage une relation professionnelle ou commerciale qui est censée, au moment où le contact est établi, s'inscrire dans une certaine durée.

Les mesures de vigilance à l'égard de la clientèle s'appliquent avant d'entrer en relation d'affaires. Elles portent sur :

L'identification et la vérification de l'identité du client (et le cas échéant, de son représentant), et le cas échéant, du bénéficiaire effectif ; et pour les contrats d'assurance **sur la vie ou de capitalisation, le bénéficiaire du contrat** et, le cas échéant, son bénéficiaire effectif ;

Ainsi que **la connaissance de l'objet et de la nature de la relation d'affaires et le recueil** de tout autre élément d'information pertinent.

1. Les mesures de vigilances à l'égard de la clientèle en relation d'affaires

a. L'identification et la vérification de l'identité du client : deux obligations complémentaires 1/3

❑ L'identification du client, et le cas échéant, de son représentant :

L'identification s'entend du recueil des éléments d'identité précisés à l'article R. 561-5 du CMF. Il s'agit, par exemple, pour les clients :

- **Associations : le nom et l'adresse du siège ainsi que le numéro d'immatriculation au répertoire national des associations (RNA)25 ;**
- **Fiducies ou trusts : les nom, prénom ainsi que les date et lieu de naissance des constituants (« *settlor* »), fiduciaires (« *trustees* »), bénéficiaires (« *beneficiaries* ») et, le cas échéant, des tiers (« *protectors* ») lorsqu'il s'agit de personnes physiques, ou leur dénomination sociale, forme juridique, numéro d'immatriculation ainsi que l'adresse de leur siège social lorsqu'il s'agit de personnes morales.**

Les entrepreneurs individuels sont identifiés comme des personnes physiques.

1. Les mesures de vigilances à l'égard de la clientèle en relation d'affaires

a. L'identification et la vérification de l'identité du client : deux obligations complémentaires 2/3

❑ La vérification de l'identité du client

- ❑ La vérification de l'identité d'un client et de son représentant, le cas échéant, repose, conformément au 2° de l'article L. 561-5 du CMF, sur la « *présentation de tout document écrit à caractère probant* ».
- ❑ En application de l'article R. 561-5-1, le document écrit à caractère probant peut être sur un support matériel ou sur un support numérique.

La vérification de l'identité en ayant recours à un moyen d'identification électronique

Les organismes financiers vérifient l'identité d'un client en ayant recours à un moyen d'identification électronique :

- Soit, **délivré dans le cadre d'un schéma français d'identification électronique** notifié à la Commission européenne en application du règlement européen n° 910/2014 **dit « eIDAS »** sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, ou notifié par un autre État membre de l'Union européenne dans les mêmes conditions, et qui présente un niveau de garantie élevé au sens dudit règlement ;
- Soit, **présumé fiable** au sens de l'article L. 102 du code des postes et des communications électroniques.

a. L'identification et la vérification de l'identité du client : deux obligations complémentaires 3/3

❑ La vérification de l'identité du client : le cas spécifique de l'entrée en relation d'affaires à distance :

L'entrée en relation d'affaires à distance **présente**, au regard des recommandations du GAFI comme de la 4ème directive anti-blanchiment, des risques plus élevés de BC-FT qui nécessitent **la mise en place de garanties suffisantes** en matière de vérification de l'identité. C'est la raison pour laquelle des mesures de vigilance complémentaires sont nécessaires en cas d'entrée en relation d'affaires à distance avec un client :

- ✓ **Lorsque ce dernier ou son représentant légal n'est pas physiquement présent, devant l'organisme financier, son tiers introducteur ou son prestataire externe, aux fins d'identification (par exemple, par internet) ;**
- ✓ **Et que la vérification de l'identité de celui-ci n'a pas été effectuée en ayant recours à un moyen d'identification électronique mentionné au 1° ou 2° de l'article R. 561-5-1, considéré comme équivalent à « du face à face ».**

Néanmoins, lorsqu'une **relation d'affaires est établie à distance avec une personne ou exclusivement pour un ou plusieurs produits présentant un faible risque** de BC-FT au sens du 2° de l'article L. 561-9 et qu'il **n'existe pas de soupçon**, les organismes financiers **ne sont pas tenus** de mettre en œuvre ces mesures complémentaires.

C. l'Arrêté du 21 décembre 2018 Rapport sur l'organisation des dispositifs de contrôle interne de LCBFT et GDA : modèle du rapport LCB-FT 1/4

Le document comprend les éléments suivants :

Préambule : description des faits marquants ayant affecté, au cours de la dernière année civile, les dispositifs de LCB-FT et de gel des avoirs de votre organisme, et/ou son exposition aux risques de BC-FT (1).

1. Principaux facteurs de risques BC-FT identifiés par votre organisme dans le cadre de la classification des risques et des procédures internes

- description des principaux **facteurs de risques faibles** de BC-FT identifiés dans le cadre de votre activité, autres que ceux prévus par la règlementation, et des **mesures de vigilance simplifiées** mises en œuvre en conséquence *(article L. 561-9 du CMF)* ;
- description des principaux **facteurs de risques élevés** de BC-FT identifiés dans le cadre de votre activité, autres que ceux prévus par la règlementation, et des **mesures de vigilance renforcées** mises en œuvre en conséquence *(article L. 561-10-1 du CMF)* ;

C. l'Arrêté du 21 décembre 2018 Rapport sur l'organisation des dispositifs de contrôle interne de LCBFT et GDA : modèle du rapport LCB-FT 2/4

– sur la **lutte contre le financement du terrorisme (FT)** :

(i) Description des **facteurs de risques propres au financement du terrorisme** identifiés par votre organisme *(article L. 561-4-1 du CMF) ;*

(ii) Présentation des **principaux critères et/ ou scénarios en matière de FT** mis en œuvre dans votre dispositif de surveillance et de détection des opérations atypiques.

2. Dispositifs de contrôle interne en matière de LCB-FT et de gel des avoirs

2.1 Description du dispositif de contrôle interne en matière de LCB-FT *(articles R. 561-38-3 et R. 561-38-4 du CMF)*

a) **Moyens humains mis en œuvre**

– effectifs ou ETP (au 31/12 de l'année N-1) en charge des **contrôles permanents de 2nd niveau** des activités LCB-FT (2) et du respect des procédures LCB-FT ;

– effectifs ou ETP (au 31/12 de l'année N-1) en charge **des contrôles périodiques** des activités LCB-FT et du respect des procédures LCB-FT. Si le contrôle périodique est externalisé, préciser le nom du (ou des) prestataire(s) pour l'exercice concerné.

b) **Critères et/ou seuils**

– description **des critères et/ou seuils** définis dans vos procédures de contrôle interne afin d'identifier les incidents importants et les principales insuffisances en matière de LCB-FT.

c) **Contrôle permanent**

– périmètre, date et fréquence du (ou des) contrôle(s) effectué(s) sur la dernière année civile ;

– incidents importants et principales insuffisances relevés ;

– mesures correctrices mises en œuvre, ou pour celles déjà engagées, date de réalisation prévisionnelle de ces mesures et état d'avancement de leur mise en œuvre à la date de rédaction du présent rapport.

d) **Contrôle périodique**

– périmètre et date du (ou des) contrôles effectués sur la dernière année civile ;

– incidents importants et principales insuffisances relevés au cours de la dernière année civile ;

– mesures correctrices mises en œuvre, ou pour celles en cours de réalisation, date de réalisation prévisionnelle de ces mesures et état d'avancement de leur mise en œuvre à la date de rédaction du présent rapport ;

– modalités de suivi des actions correctrices (outils, personnes en charge etc.).

C. l'Arrêté du 21 décembre 2018 Rapport sur l'organisation des dispositifs de contrôle interne de LCBFT et GDA : modèle du rapport LCB-FT 3/4

2.2 Description du dispositif de contrôle interne en matière de gel des avoirs *(article R. 562-1 du CMF qui renvoie aux articles R. 561-38-3 et R. 561-38-4 du CMF)*

(i) Indiquer si le filtrage des bases et des flux est automatisé ou manuel, et en particulier :

- pour le filtrage des bases « clientèle » (appelées aussi « bases tiers »), les catégories de personnes présentes dans les bases « clientèle » dont les éléments d'identification sont filtrés (3) ;
- pour le filtrage des flux, les opérations filtrées : indiquer notamment si le dispositif couvre les flux entrants et les flux sortants ; les flux nationaux et les flux internationaux, les donneurs d'ordre et les bénéficiaires ;

(ii) Préciser :

- la fréquence retenue pour le filtrage des bases et les modalités de filtrage à l'entrée en relation d'affaires ou lors de l'exécution d'une opération pour un client occasionnel ;
- la (ou les) liste(s) utilisée(s) pour le filtrage des bases et des flux, en précisant si celles-ci proviennent directement d'une autorité compétente ou sont fournies par un prestataire externe ;
- les modalités de rapprochement orthographique et/ou de date de naissance utilisées pour le filtrage des bases et des flux ;
- si votre organisme est doté d'un filtrage automatisé et dans ce cas, si un mécanisme de secours existe en cas de blocage des dispositifs de filtrage.

(iii) Préciser, en ce qui concerne le contrôle interne du dispositif de gel des avoirs, les éléments prévus aux points *b*, *c* et *d* du § 2.1 susmentionnés, ainsi que les modalités du suivi du traitement des alertes, à la fois sur les flux et sur les bases, et de mise en œuvre effective des mesures de gel.

3. Eventuelles insuffisances en matière de LCB-FT et de gel des avoirs relevées au cours de la dernière année civile par des autorités de contrôle étrangères (4)

Décrire :

- les principales insuffisances relevées par ces autorités, y compris les éventuelles sanctions et mesures administratives prises par les autorités de contrôle étrangères, lorsqu'elles impactent directement l'organisme ;
- et les éventuelles mesures correctrices mises en œuvre par l'organisme en conséquence.

4. Contrôle interne en matière de LCB-FT dans le cadre des dispositifs ou activités spécifiques

Préciser, pour chacun des dispositifs ou activités ci-dessous, si des incidents importants ou insuffisances mentionnés aux § 2 et 3 sont liés à l'un d'entre eux.

a) **Externalisation**

C. l'Arrêté du 21 décembre 2018 Rapport sur l'organisation des dispositifs de contrôle interne de LCBFT et GDA : modèle du rapport LCB-FT 4/4

– pour les organismes qui ont recours à **un ou des prestataire(s) externe(s) ou intra-groupe pour la mise en œuvre d'activités opérationnelles liées (i) à la LCB-FT ou (ii) au gel des avoirs,** préciser le nom du (des) prestataire(s), y compris des fournisseurs de bases de données et de dispositifs de filtrage, la nature des activités qui lui (leur) sont confiées et les contrôles réalisés sur les prestataires *(article R. 561-38-5 du CMF) ;*

– pour les organismes qui ont recours à **un ou plusieurs agents de services de paiement et/ou à une ou plusieurs personnes en vue de distribuer de la monnaie électronique au sens de l'article L. 525-8 du code monétaire et financier** *(articles L. 523-3 et L. 525-9 du CMF)* : décrire le processus de recrutement des agents et/ou personnes en vue de distribuer de la monnaie électronique, le dispositif de contrôle des agents et/ou distributeurs et préciser le pourcentage d'agents et/ou de personnes en vue de distribuer de la monnaie électronique ayant fait l'objet d'un contrôle au cours de la dernière année civile.

b) **Tierce introduction**

– pour les organismes qui ont recours à **un ou plusieurs tiers introducteur(s)** : préciser le nom du (des) tiers introducteur(s), décrire les modalités de contrôle de l'exécution de la (des) convention(s) passée(s) entre votre organisme et le(s) tiers introducteur(s) (*article R. 561-13 du CMF*).

c) **Transferts de fonds**

– pour les PSP qui réalisent des opérations de transmission de fonds (5) : présentation des **critères de distinction** entre les clients occasionnels et les clients en relation d'affaires (*article L. 561-2-1 du CMF*) ;

– pour les PSP intermédiaires et les PSP du bénéficiaire : décrire le **dispositif de détection des informations manquantes ou incomplètes** sur le donneur d'ordre ou le bénéficiaire, préciser notamment les contrôles prévus en temps réel et/ou *a posteriori (articles 7.2 et 11.2 du règlement européen (UE) 2015/847 du 20 mai 2015 sur les informations accompagnant les transferts de fonds et les orientations des autorités européennes de supervision relatives aux mesures que les prestataires de services de paiement doivent prendre pour détecter des informations manquantes ou incomplètes sur le donneur d'ordre ou le bénéficiaire, ainsi que les procédures devant être mises en place pour gérer un transfert de fonds qui n'est pas accompagné des informations requises, publiées le 16 janvier 2018).*

d) **Correspondance bancaire**

– pour les organismes qui proposent un service **de correspondance bancaire transfrontalière** : présenter les modalités d'échange d'informations avec l'établissement client prévues dans la convention de correspondance bancaire, les modalités de contrôle du respect de la convention et les mesures d'escalade en cas d'inexécution de la convention *(articles L. 561-10-3 et R. 561-21 du CMF).*

5. Compléments d'information concernant les succursales ayant leur siège social dans un autre Etat membre de l'Union européenne ou partie à l'accord sur l'Espace économique européen

– **l'éventuelle articulation entre la succursale et le siège/ou d'autres entités du groupe des dispositifs de LCB-FT/gel des avoirs**. Dans cette hypothèse, décrire la répartition, entre la succursale et le siège/ou d'autres entités du groupe, des activités opérationnelles mises en œuvre dans le cadre de ces dispositifs, ainsi que les modalités de formalisation de cette répartition. Préciser en particulier :