Industrialisation et Digitalisation des dispositifs de Lutte Anti-Blanchiment et Anti-Terrorisme :

Le prochain challenge des établissements financiers

AURORE DISITI-DIT-DISSIDI

JUIN 2020

noveo conseil

L'ACPR (Autorité de Contrôle Prudentiel et de Résolution) concentre ses efforts sur la lutte contre le blanchiment et le financement du terrorisme depuis plusieurs années. Elle a, pour ce faire, sensiblement accru son niveau d'exigence envers les établissements financiers.

Depuis la création de Tracfin (Traitement du renseignement et action contre les circuits financiers clandestins) et les premières déclarations de soupçons dans les années 90, le cadre réglementaire s'est considérablement étoffé autour de Directives, lignes directrices et ordonnances successives pour lutter plus efficacement contre le blanchiment d'argent et le financement du terrorisme (LCB FT).

En un peu plus de 5 ans, 2 Directives au niveau européen et leur déclinaison au niveau national ont été adoptées visant à rendre plus performant le dispositif de lutte anti-blanchiment à l'échelon européen.

La 5eme Directive, la plus récente (juillet 2018), vient apporter des précisions sur les attentes du régulateur en matière de dispositif de contrôle et élargir le scope des établissements assujettis, en particulier à ceux opérant sur des actifs numériques.

Ces séries d'évolutions règlementaires ont été mises en place sous l'impulsion d'une part de l'actualité économique, sociale et financière de ces 30 dernières années (attaques terroristes, blanchiment d'argent, affaire des « panama papers»…), mais aussi au fil des retours d'expérience du superviseur faisant suite aux audits réalisés.

Quatre textes récents fixent les obligations et dictent la norme en matière de lutte contre le blanchiment et le financement du terrorisme

	Evolution du Cadre Réglementaire			
	3 novembre 2014	14 décembre 2018	Juillet 2018	Février 2020
Textes de référence	4ème Directive anti-blanchiment	Transposition de la 4ème Directive en droit français	5eme directive anti-blanchiment	Transposition de la 5ème Directive en droit français
Obligations énoncées	▪ Évaluation des risques ▪ Identification et vérification de l'identité des clients et de leurs bénéficiaires effectifs ▪ Mesures de vigilance à l'entrée et tout au long de la relation d'affaires ▪ Obligation de déclaration à TRACFIN ▪ Contrôle interne et le Reporting à l'AMF ▪ Mise en œuvre des mesures de gel des avoirs.		▪ Renforcement de la transparence des personnes morales et des structures juridiques complexes en élargissant l'accessibilité des registres des bénéficiaires effectifs ▪ Harmonisation des mesures de vigilance renforcées à mettre en œuvre à l'égard des relations d'affaires ou des opérations impliquant des pays tiers à haut risque ▪ Précision sur les mesures à mettre en œuvre en cas d'entrée en relation d'affaires à distance ▪ Assujettissement aux règles LCB-FT de certains prestataires de services liés aux actifs numériques	

Ces textes imposent un certain nombre de points de contrôle aux organismes financiers avec, à la clef, une obligation de moyens mais aussi de résultat sous peine de se voir sanctionné.

Dans les grandes lignes, 8 principes clefs sont à retenir :

1. **Connaissance de son client (KYC : Know Your Customer)** : les organismes financiers se doivent d'être vigilants vis-à-vis de leurs relations d'affaires tant dans l'entrée en relation que dans le suivi de leurs opérations. Le régulateur demande la mise en place d'un dispositif de suivi et d'analyse de la clientèle ;
2. **Mise à jour régulière des KYC** (en fonction de la situation de la relation d'affaires et de ses critères de sensibilité) ;
3. **Évaluation « juste » de leur niveau de risque** reposant sur la définition d'une classification des risques en fonction de la nature des produits ou services offerts, des conditions de transactions proposées, des canaux de distribution utilisés, des caractéristiques du client ainsi que du pays ou territoire d'origine ou de destination des fonds ;
4. **Des comportements clientèle en ligne avec le profil attribué ;**
5. **Une capacité à détecter, analyser et traiter les anomalies ;**
6. **Un contrôle interne et un contrôle permanent efficaces sur le dispositif de suivi et la surveillance des relations d'affaires** y compris en cas d'externalisation de certaines fonctions ;
7. La capacité à répondre à **l'obligation d'information et de déclaration à Tracfin ;**
8. Le déploiement d'un **dispositif de filtrage en matière de gel des avoirs.**

Ces 8 obligations fixent la « norme » attendue de la part de l'ACPR et de Tracfin en matière de dispositif LCB FT, générant par la même une pression accrue sur les organismes financiers, en les obligeant à mettre à niveau leur dispositif de contrôle et leur organisation.

Pour répondre aux exigences du régulateur et atteindre ce niveau de standard les établissements financiers ont essayé de s'adapter à renfort de moyens.

Dans l'attente de la transposition de la 5eme Directive, déclinée récemment en droit français (février 2020), les organismes financiers ont tenté de répondre aux exigences de la 4eme. Ils ont travaillé plus spécifiquement sur la classification des risques et son adéquation par rapport aux opérations du client.

Dans les faits, l'exercice est loin d'être facile et s'avère même ténu dans son exécution compte tenu de la complexité des Directives, du délai important entre l'entrée en vigueur d'une « norme » et sa déclinaison en droit français.

Face à ce constat et à la demande des organismes financiers, l'ACPR et TRACFIN publient en complément des textes règlementaires, des lignes directrices dont la vocation est de préciser les attentes de la cellule de renseignement financier et celles du superviseur.

La dernière en date remonte à octobre 2018 et apporte un certain nombre d'éclaircissements » sur 4 sujets :

- **L'obligation de vigilance à l'égard de la clientèle ;**
- **L'obligation de déclaration de soupçon ;**
- **L'articulation entre l'obligation de déclaration de soupçons et les autres dispositifs de contrôle dont le gel des avoirs ;**
- **Les communications systématiques d'information (COSI) à Tracfin.**

Ces lignes directrices n'ont pas de caractère contraignant mais apportent des éclaircissements sur les actions attendues de la part des établissements financiers.

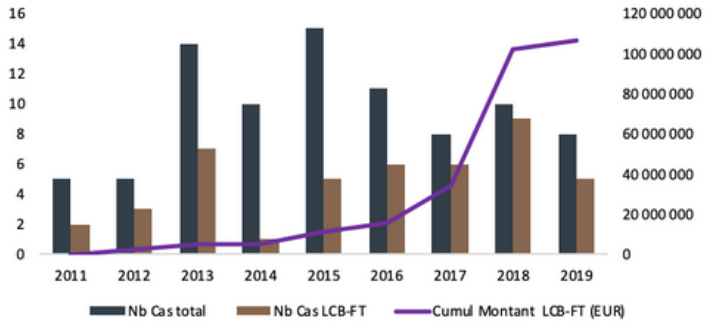
Banques et assurances, en particulier, ont donc dû faire des efforts importants au cours de ces dernières années pour être en mesure de répondre à ces demandes. Dans un premier temps, ils se sont dotés d'outils permettant de détecter les opérations dites sensibles devant faire l'objet de contrôles plus poussés.

En parallèle, les organismes financiers ont dû également faire face à la problématique des compétences des équipes et former l'ensemble du personnel à ces sujets. Dans la majorité des cas, le parcours, long, difficile et couteux, passe par un triptyque incontournable :

- **Des programmes de formation pour sensibiliser l'ensemble des équipes à ces sujets** et pas uniquement les équipes en lien direct avec la clientèle ;
- **Un volet organisationnel reposant sur un service Conformité plus étoffé**, prévoyant une montée en charge progressive :
  - d'une équipe dite de Niveau 1 dont la vocation est de traiter les alertes : vérifier les flux et mener à bien les contrôles nécessaires pour lever le doute ou bien confirmer la nature « sensible de l'opération »
  - et des équipes de Niveau 2 qui auront pour mission de mener des recherches plus approfondies et prendre la décision de geler les avoirs si nécessaire. Elles seront amenées également à réaliser la déclaration de soupçon auprès de Tracfin si cela s'avère nécessaire et informer les autorités compétentes.
- **Un volet informatique** avec la définition d'outils capables de détecter des comportements/ des opérations identifiées comme potentiellement à risque et générer les alertes idoines.

Globalement, des progrès considérables ont été faits en quelques années sur l'ensemble de ces axes, mais le challenge reste encore de taille d'autant que le superviseur porte une attention accrue sur ce sujet.

Sanctions de l'ACPR dans le cadre de la LCB-FT

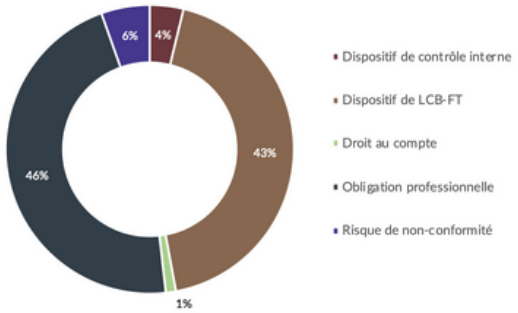


Le contrôle des dispositifs LCB FT des organismes financiers constitue un réel sujet d'attention pour l'Autorité de contrôle. Sur ces 9 dernières années, 50% des sanctions énoncées portent sur les manquements observés en matière de dispositif LCB FT et représentent plus de 43% du montant global.

En 2011, on ne dénombrait que 2 cas de sanctions pour un montant global de 150 KEUR contre 9 cas en 2018 pour un montant cumulé de 103 MEUR, dont 68,7 MEUR sur cette seule et même année.

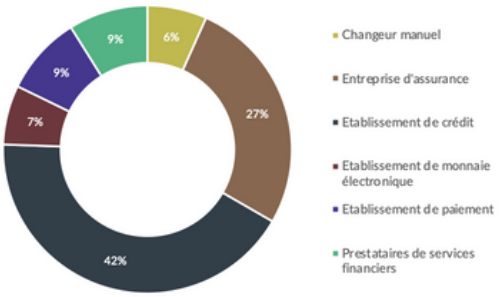
En proportion, les griefs pour manquement au dispositif LCB – FT sont aussi significatifs que les amendes énoncées par l'ACPR pour manquement aux obligations professionnelles (43% du montant total des sanctions depuis 2011 versus

Répartition en montant des types de sanction 2011 à 2020
(Base : Total des cas)



La revue des sanctions et blâmes énoncés par l'ACPR met clairement en exergue les difficultés des acteurs à mettre à niveau leur dispositif et à atteindre cette « norme », en particulier pour les établissements de crédit et les assureurs.

Répartition des cas 2011 à 2020
(Base : Dispositif de LCB-FT)



Enfin, les organismes les plus sanctionnés sur leur dispositif LCB – FT demeurent les établissements de crédit et les assureurs qui concentrent respectivement 42% et 27% des cas de sanctions.

Le régulateur se montre, par ailleurs, très vigilant vis-à-vis des établissements de monnaie électronique.

Ces dispositifs restent donc encore fragiles et perfectibles : peu ou pas industrialisés, ils requièrent des moyens humains importants et se déclinent souvent difficilement dans un environnement de travail à distance.

Dans bien des cas, cette mise à niveau s'est traduite par la mise en place de task force et le recours massif à des opérateurs pour revoir les KYC, mettre à jour le niveau de risque, la piste d'audit et se mettre en capacité de détecter les cas de fraude sur les opérations.

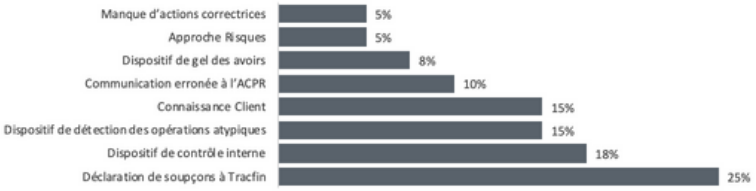
Six ans après la mise en application de la Directive 4, les difficultés des acteurs restent réelles et les dispositifs présentent encore des zones de faiblesses importantes voire des manquements dans certains cas.

Bien consciente de ces difficultés, l'Autorité de contrôle a d'ailleurs largement concentré ses audits ces dernières années sur ces dispositifs pour s'assurer du bon respect des principes édictés. Ces missions ont donné lieu à des amendes de montants significatifs voire des retraits d'autorisation d'exercer pour certains établissements.

Sur ces 9 dernières années, 6 sociétés ont dû s'acquitter de 86 millions d'euros d'amende - soit plus de 80% du montant total des sanctions énoncées- compte tenu des défaillances observées dans leur dispositif.

	LA BANQUE POSTALE	BNP PARIBAS	BANQUE B	SOCIÉTÉ GÉNÉRALE	CNP ASSURANCES	GENERALI VIE	RAGURAM INTERNATIONAL	TRANSACTION SERVICE INTERNATIONAL
	50 M€	10 M€	8 M€	5 M€	8 M€	5 M€	Retrait d'agrément	Blâme
	21/12/2018	30/05/2017	22/03/2018	19/07/2017	26/07/2018	24/07/2015	08/04/2019	12/06/2018
Manque d'actions correctrices	✓			✓				
Approche Risques			✓		✓			
Dispositif de gel des avoirs	✓				✓		✓	
Communication erronée à l'ACPR	✓			✓			✓	✓
Connaissance Client					✓	✓	✓	✓
Dispositif de détection des opérations atypiques		✓	✓	✓		✓		✓
Dispositif de contrôle interne	✓	✓	✓	✓		✓		✓
Déclaration de soupçons à Tracfin		✓	✓	✓	✓	✓		

Focus sur les principales sanctions par thématique



Les sujets les plus sensibles demeurent :

- la déclaration de soupçon à Tracfin (25% des griefs énoncés sur ces 9 cas) dont la production reste encore très manuelle et la qualité insuffisante
- le dispositif de contrôle interne (18%) et de surveillance en particulier sur les opérations atypiques (15%) et/ou sensibles nécessitant un examen renforcé, qui présente souvent des faiblesses à plusieurs niveaux dont le 1er est la connaissance du client (15%).

La montée en puissance du niveau d'exigence du régulateur, cumulé à l'attente des déclinaisons définitives des directives en droit français génèrent un certain nombre de problèmes opérationnels :

- les procédures ne sont pas toujours complètement déclinées ou stabilisées ;
- les contrôles encore très manuels sur l'ensemble de la chaîne de traitement requièrent un nombre d'ETP important laissant apparaître une sensibilité forte à la volumétrie ;
- l'évolution constante « du standard » oblige à un effort important de formation des équipes.

Cette sensibilité aux volumes s'observe même auprès de grands acteurs de la place. Elle tient le plus souvent à la conjonction d'outils informatiques et d'un dispositif de contrôle qui ne sont pas encore bien « calibrés ».

En amont, les outils de détection ne permettent pas une gestion optimisée de l'identification et du traitement des cas d'alertes :

- un trop grand nombre de cas d'alertes est remonté alors qu'il s'agit en fait de fausses alertes (faux positifs) liées entre autre à des cas d'homonymie
- le traitement de ces alertes est encore très manuel : contrôle dans les systèmes de production, recherche dans les référentiels et sur internet pour les due diligences, prise de contact avec l'extérieur sont réalisés au cas par cas à la main.

En aval, les déclarations de soupçons, très peu industrialisées, nécessitent de nombreux débrayages manuels.

La faiblesse des outils et le manque d'industrialisation des procédures se répercutent donc sur la capacité de traitement des équipes de contrôle, difficulté qui se trouve dans certains cas, accentuée par une gouvernance insuffisante au sein même de la Conformité :

- le contrôle de niveau 1 est souvent submergé par une volumétrie élevée d'alertes ;
- la répartition des rôles et des responsabilités est insuffisamment spécifiée entre le contrôle de niveau 1 et celui de niveau 2, aboutissant à un trop grand nombre de cas soumis au niveau 2 ;
- Un niveau 2 qui se trouve en conséquence « engorgé » et quelque peu dépassé ;
- Un nombre encore trop important de déclarations à Tracfin dont la qualité, par ailleurs, reste encore largement perfectible.

Ce manque d'automatisation et de digitalisation entraine un certain nombre de rigidités qui, au delà d'un coût humain et financier importants, rend épineux la déclinaison de ces points de contrôle dans un environnement de travail à distance (cette difficulté s'est particulièrement faite ressentir dans le contexte du COVID 19).
Cette pandémie et le confinement qui en a découlé ont imposé le travail à distance comme une norme, obligeant les entreprises à adapter leurs infrastructures et leurs procédures pour maintenir un niveau de contrôle satisfaisant.

Ce passage au télétravail « à marche forcée » s'est parfois réalisé difficilement, voire dans l'urgence. Post confinement, une nouvelle « normalité » s'installe et laisse entrevoir une situation qui demande un certain nombre d'ajustements tant au niveau des procédures que des outils et la mise en place de task force parfois même pour travailler sur l'apurement de backlogs.

Ce constat est particulièrement vrai dans le cas des contrôles des opérations dites sensibles ou encore des déclarations de soupçons évoquées au préalable, requérant souvent des contrôles dans les systèmes de production, classés sensibles, dont les accès ne sont pas toujours disponibles à distance pour les services de contrôle (accès réservés aux équipes de production).

Répondre à l'ensemble des contraintes imposées par le régulateur, tout en étant en mesure d'exécuter ces tâches à distance, sans dégrader le niveau de contrôle ou de risques opérationnels, dans un contexte de maîtrise des coûts opérationnels ne s'avère pas évident. Il s'agit, en fait, d'un véritable challenge.

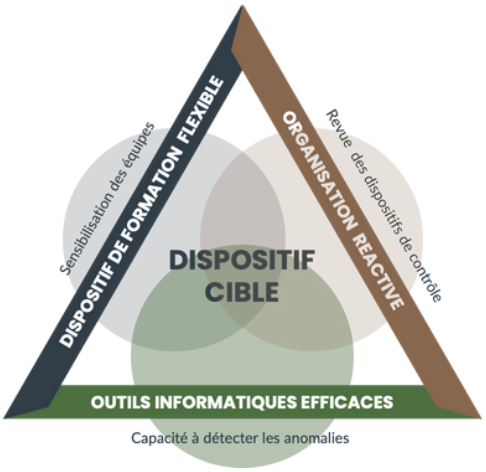
L'industrialisation des outils et des procédures dans un environnement de travail à distance constitue donc un réel enjeu.

Les organismes financiers doivent maintenant stabiliser et améliorer l'existant en termes d'organisation et faire face à un challenge d'automatisation pour être plus efficaces, réaliser les contrôles plus rapidement et à moindre coût.

La nécessité de pouvoir adapter facilement le niveau de contrôle, dans un environnement de cout maîtrisé, sans dégradation du niveau de risque opérationnel sera donc le prochain enjeu.

Trois grands axes sont à privilégier pour gagner en robustesse et en efficacité :

- une meilleure maîtrise des données, de leur qualité et de leur exploitation pour permettre une amélioration continue au niveau de la définition des scénarios de détection de fraudes et un calibrage plus aisé des outils ;
- une amélioration des outils existants :
  - En amont au niveau (i) de la détection des alertes une fiabilisation des outils pour permettre une diminution du nombre de faux positifs, le recours au machine learning est l'une des pistes pour gagner en flexibilité et robustesse et (ii) la mise en place d'outils de gestion des cas pour assurer une traçabilité optimale des contrôles réalisés en particulier pour les cas jugés sensibles depuis l'identification jusqu'à la déclaration de soupçons et/ou le gel des avoirs ;
  - En aval une industrialisation des procédures de contrôle et de réalisation des déclarations de soupçons grâce aux RPA et OCR pour limiter les débrayages manuels et renforcer la qualité des reportings produits ;
  - Une restitution des données efficaces des cas analysés, des services impactés pour permettre



un meilleur pilotage tant au niveau des équipes de conformité que des métiers impactés ;
  - La captation de ces cas et données pour réutilisation dans la sensibilisation et la formation des équipes ce qui suppose des outils de formation auto apprenant type chatbot pour réduire la maintenance évolutive des supports de formation et rester toujours à jour vis-à-vis des exigences du régulateur en matière de standard de contrôle ;
  - Et bien entendu la possibilité de gérer l'ensemble de ces contrôles à distance.
- Une gouvernance plus explicite
  - Un RACI clair entre les différents services intervenants depuis la 1ere ligne de contrôle lors de l'entrée en relation jusqu'au service en charge de la déclaration de soupçons .

Près de 50% des sanctions énoncées par l'ACPR en valeur et en nombre durant ces 10 dernières années portent à eux seuls sur des griefs consécutifs au non-respect des obligations liées à la lutte contre le blanchiment et au financement du terrorisme. La 5ème Directive vient encore renforcer les exigences du régulateur tant en matière de contrôle que d'activités assujetties.

Le prochain challenge des établissements financiers portera donc sur leur capacité à digitaliser et industrialiser les procédures de contrôle et de détection de fraude et plus largement de l'ensemble du dispositif de manière à s'adapter plus facilement et à moindre coût aux évolutions de normes. Cette automatisation devrait faciliter, par ailleurs, sensiblement le traitement à distance de ce type de contrôle et accroître par la même la résilience de ces établissements.

GENÈVE

8, rue du Conseil Général
1205 Genève, Suisse
+41 22 322 13 52
philippe.perles@noveoconseil.com

LUXEMBOURG

26 boulevard Royal
2449 Luxembourg
+352 22 99 99 2417
geoffroy.gailly@noveoconseil.com

PARIS

13 rue Lafayette
75009 Paris, France
+33 1 72 89 72 54
olivier.laloum@noveoconseil.com

AURORE DISITI-DIT-DISSIDI

JUIN 2020

noveo conseil