

Charte de la Conformité

**Groupe de travail « Contrôle et Conformité en Finance.
Second regard et qualité »,**

**Sous-groupe de travail « Charte de la Conformité et Statut du
Compliance Officer »**

Date du document	26 avril 2021
Version du document	

Les travaux du sous-groupe « Charte de la Conformité et Statut du Compliance Officer » ont été réalisés sous la direction de Nathalie de Larminat Bougnoux, Fondatrice et Gérante de TILIAS, Conseil en Conformité, Ethique des affaires & ESG, assistée de Nicolas Vetriak, Christine Wrucka et Marie-Elisabeth Moray, respectivement Président et Directeurs de NOVAMINDS.

Nos remerciements vont tout particulièrement :

- Aux membres du Groupe de travail, dont l'engagement sans faille a permis la construction de cette Charte : Jacques Beyssade (BPCE), Béatrice de Meaux-Becdelievre (ACOFI), Hubert de Vauplane (Kramer Levin Naftalis & Frankel LLP), Virginie Le Mée (UMR) ;
- A ceux qui nous ont apporté leur précieuse expertise : Céline Haye-Kiousis et Sophie Nerac (BPCE), Ingrid Belleil (UMR), Jacques Sudre et Ludovic de Mallmann (La Banque Postale).
- Et à Patrick Suet, François Delavenne et Sylvain de Forges, pour leur soutien indéfectible depuis l'origine du projet.

Préambule

Ce document est proposé comme modèle. En effet, si les principes fondamentaux qui structurent cette Charte de Conformité peuvent directement transposés à l'ensemble des institutions du secteur financier, du secteur non financier, et du secteur public, ses modalités de mise en œuvre peuvent être déclinées et adaptées en fonction des missions, du profil d'activités, de la sensibilité éthique, de l'appétit au risque et de l'organisation de chacun.

Table des matières

1. Objet.....	4
2. Périmètre	5
a) Chaîne de valeur de la Conformité.....	5
b) Socle juridique et réglementaire applicable en France aux secteurs bancaire, assurance, gestion d'actifs et émetteurs d'instruments financiers.....	5
c) Extension et circonscription du périmètre.....	7
3. Principes de conformité	7
a) Indépendance et proximité.....	7
b) Conseil expert et contrôle permanent.....	8
c) Inciter les instances dirigeantes à s'engager.....	9
4. Missions de la Fonction Conformité	9
a) Assurer la veille réglementaire, en liaison avec la Direction Juridique	9
b) Délivrer un conseil expert	9
c) Cartographier et gérer les risques de non-conformité dans toutes les composantes thématiques :.....	10
d) Circonscrire et assurer un programme ciblé de formation, sensibilisation, information :..	11
e) Gouvernance : être en relation avec les parties prenantes en matière de conformité : ..	11
5. Les responsabilités de la Fonction Conformité	11
a) La responsabilité opérationnelle de la Fonction Conformité	11
b) La responsabilité juridique de la Fonction Conformité.....	12
6. Organisation de la Fonction Conformité	12
a) Exemple de modèle d'organisation de la Fonction Conformité	12
b) Principes de gouvernance de la chaîne de conformité.....	13
c) Aptitudes professionnelles du Compliance Officer	15
d) Synergies autour du CO	15
e) Profil type d'un Compliance Officer senior	15

1. Objet

Qu'est-ce que la Conformité ?

- La Banque des Règlements Internationaux avait retenu une définition déjà large du risque de non-conformité : « The risk of legal and regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities » (in Bank for International Settlements, Basel Committee on Banking Supervision; “Compliance and the Compliance function in banks”, April 2005).
- L'arrêté ministériel du 3 novembre 2014 (article 10), qui s'applique aux établissements de crédits, reprend les termes de cette définition du risque de non-conformité : « Le risque de sanction judiciaire, administrative ou disciplinaire, de perte financière significative ou d'atteinte à la réputation, qui naît du non-respect de dispositions propres aux activités bancaires et financières, qu'elles soient de nature législative ou réglementaire, nationales ou européennes directement applicables, ou qu'il s'agisse de normes professionnelles et déontologiques, ou d'instructions des dirigeants effectifs, prises notamment en application des orientations stratégiques de l'organe de surveillance ».
S'assurer contre le risque de non-conformité, c'est s'assurer que l'établissement, l'entreprise ou l'organisme, agit conformément, à la législation et la réglementation en vigueur, nationales et extraterritoriales, à ses propres règles, notamment sa charte éthiques, son code de conduite professionnelle et son règlement intérieur, ainsi qu'à la jurisprudence, aux bonnes pratiques, positions et recommandations des superviseurs, les normes de place, ..., afin d'éviter tout risque d'irrégularité dans le fonctionnement de l'institution, de ses organes de gouvernance ou des collaborateurs, salariés ou non, et, partant, de l'ensemble de ses parties prenantes. Il s'agit donc de permettre à l'institution de circonscrire et gérer au mieux son exposition aux risques de sanctions judiciaires, administratives ou disciplinaires, de perte financière ou d'atteinte à sa réputation ou son image, encourus en cas de non-conformité, et dans le respect de sa sensibilité éthique et de son appétit au risque.
- Ces définitions réglementaires se trouvent aujourd'hui de plus en plus élargies en faveur du concept de « **Corporate Compliance** » qui prévaut aux Etats-Unis et s'ancre de plus en plus en Europe ; cette conception de la Conformité va très au-delà du respect de la loi bancaire par exemple ; ainsi, pour les sociétés cotées, le périmètre de surveillance de la Fonction Conformité s'étend de plus en plus à l'ensemble des règles AMF.

L'objet de la Charte de la Conformité : définir les principes, responsabilités et rôles fondamentaux des acteurs de l'ensemble de la chaîne de valeur de conformité, et en particulier de la Fonction Conformité, essentielle ligne de défense de 2^e niveau, et préciser le positionnement de la Fonction du Chief Compliance Officer (« CCO »), gardien du temple de cette chaîne de valeur au sein de l'institution, et dont la présente Charte est l'objet principal ; seront ainsi examinés/analysés sa mission, ses pouvoirs, ses responsabilités, son rattachement hiérarchique, ses modalités de fonctionnement et les attributs d'une posture équilibrée, l'ensemble permettant au Compliance Officer (« CO ») d'agir avec la plus grande efficacité.

2. Périmètre

a) Chaîne de valeur de la conformité

La conformité est souvent appréciée sous le seul prisme du contrôle, en lien avec les trois lignes de défense. Mais une attention particulière doit être apportée au rôle de conseil de la Fonction Conformité, qui apporte la fluidité de dialogue nécessaire entre ses différentes composantes des lignes de défense et concourt ainsi de manière cruciale à la force de l'ensemble de la chaîne de valeur de conformité. Cette chaîne de valeur comporte les maillons essentiels suivants :

- A la source de la prise de risque des principaux acteurs de la conformité sont les opérationnels eux-mêmes, qui sont à l'origine des opérations et donc de la prise de risque de conformité au sein de l'établissement, de l'entreprise ou de l'organisme, et leur management direct, qui apporte un second regard ;
- Le conseil apporté par les Compliance Officers lors de la validation des opérations (transactionnel, comités nouveaux produits, etc.) ;
- La définition du niveau d'appétit au risque donné par l'organe suprême de gouvernance (Conseil d'administration dans les SA).

Le risque de non-conformité est devenu stratégique pour l'ensemble des acteurs économiques, et emporte des responsabilités juridiques et opérationnelles fortes.

b) **Socle juridique et réglementaire applicable en France aux secteurs bancaire, assurance, gestion d'actifs et émetteurs d'instruments financiers**

- **Le cadre légal et réglementaire en France** repose pour l'essentiel sur les textes suivants :
 - Arrêté du 3 novembre 2014 relatif au contrôle interne (abroge le règlement CRBF 97-02)
 - Arrêté du 22 décembre 2020 (consiste en la mise à jour de l'Arrêté du 3 novembre 2014 relatif au contrôle interne et visant à transposer la Directive 2019/878 (CRD5) relative à certaines règles applicables en matière de rémunération). Les dispositions de cet Arrêté clarifient notamment le champ d'application de ces règles, aux établissements sur base individuelle et aux établissements et autres entités d'un groupe soumis à supervision consolidée. Les différents codes dont le Code Monétaire et Financier (CMF)
 - Les lois : LSF / LRBF / loi Hamon / Lagarde / Sapin 2 / droit de la concurrence
 - Les textes des autorités de supervision, notamment AMF, ACPR, AFA
 - Les avis, instructions, recommandations, principes d'application sectoriels de l'ACPR et de l'AMF
 - La notice ACPR sur la désignation des « dirigeants effectifs » et des « Responsables de Fonctions clés » dans le régime « Solvabilité II » du 2 novembre 2016
 - Les questionnaires ACPR sur la LCB/FT et sur la protection de la clientèle
- **Plus particulièrement, en matière de solvabilité, fonds propres, liquidité :**
 - Conventions, directives, Guidelines de l'European Banking Association (EBA)
 - Bâle II - Bâle III – Bâle IV
 - BRRD
 - Solvabilité II
 - CRD V / CRR 2

- **En matière de transparence et d'intégrité des marchés financiers :**
 - RG AMF
 - Réglementation EMIR
 - Réglementation Benchmarks (IBOR, ...)
 - Réglementation MIFID II / PRIiPs / IMD2 / UCIT V
 - MAD/MAR II, US DFA, etc.

- **Dans le domaine de l'externalisation, systèmes de paiement, données personnelles, ... :**
 - Les guidelines de l'EBA sur les prestations externalisées et sur la gouvernance interne
 - Les guidelines de l'ESMA et les orientations de l'EIOPA sur les prestations en Cloud
 - REMIT (Règlement sur l'intégrité et la transparence du marché de gros de l'énergie)
 - DSP2, DME2
 - RGPD, etc.

- **En matière de sécurité et criminalité financières :**
 - 3^{ème}, 4^{ème}, 5^{ème} et 6^{ème} Directive LCB / FT, dont la lutte contre la fraude fiscale, et la réglementation extraterritoriale FATCA
 - Loi Sapin II et les réglementations extraterritoriales anti-corruption, comme FCPA, UK Bribery Act
 - Réglementations embargos et sanctions internationales, nationales, européennes et internationales (BIS, US OFAC, etc.)
 - Fraude (hors fraude fiscale), etc.

- **Sur la protection et traitement équitable de la clientèle :**
 - Loi sur le Devoir de Vigilance
 - MiFID II
 - DDA (IDD), loi Eckert
 - Contrôle des pratiques commerciales, les publicités ainsi que les contrats, les produits et les services
 - Processus tels que notamment la création de produit, d'activité, de service, le contrôle interne ou encore la gestion de la relation clients
 - Renforcement du dispositif de contrôle du "Conduct Risk "
 - Communication des informations claires, exactes, précises et non trompeuses sur les caractéristiques et risques associés aux produits au travers de la documentation adressée aux clients ;
 - Adaptation de l'offre et devoir de conseil, notamment en fonction des besoins et du profil de risques des clients, et de l'horizon d'investissement dans le cas des instruments financiers ;
 - Facturation des produits de manière juste et équitable
 - Gestion de la politique RGPD de l'établissement (si elle entre dans le périmètre de responsabilité de la Fonction Conformité de l'institution)
 - Gestion des réclamations
 - Protection des personnes sensibles, fragiles et vulnérables

- **En matière de contrôle permanent de la conformité :**
 - Organisation et cohérence de l’articulation entre les 3 lignes de défense : contrôle permanent opérationnel du niveau 1 des Métiers opérationnels (« front-office to back-office ») ; contrôle permanent du niveau 2 de la Fonction Conformité indépendante des métiers opérationnels, en liaison étroite avec les autres fonctions de niveau 2, en particulier la Fonction Risques et la Fonction Finance ; et contrôle périodique du niveau 3 de l’Audit interne, indépendant des Métiers Opérationnels et de la Fonction Conformité.
 - Mise en place de contrôles visant à s’assurer de la conformité des opérations.
- **Et en matière éthique et déontologique, en particulier :**
 - Règles de bonne conduite professionnelle fixées au sein de l’établissement souvent matérialisées par une charte éthique et un code de conduite, qui s’inspirent en grande partie des exigences réglementaires ou des recommandations des régulateurs (Loi du 9 décembre 2016, dite « loi Sapin II »)
 - Identification et gestion des conflits d’intérêts.

c) **Extension et circonscription du périmètre**

Définition du périmètre, de ses limites et de son articulation avec d’autres thématiques : éthique des affaires ; risque de réputation et d’image ; Environnement, Social/Sociétal, Gouvernance (ESG) et Responsabilité Sociale/Sociétale et Environnementale (RSE) ; rapports intégrés et déclarations de performance extra-financière, etc.

Ce périmètre de responsabilité peut varier en fonction de l’organisation des entités ; ainsi, certaines des thématiques ne relèvent pas forcément du périmètre de responsabilité de la Fonction Conformité, comme parfois la lutte anti-corruption, la fraude, la surveillance de la protection des données personnelles (RGPD) avec l’identification du rôle du Data Protection Officer (DPO), la ligne d’alerte (« whistleblowing »), le profilage des fournisseurs (Know Your Supplier - KYS-), etc.

3. **Principes de conformité**

a) **Conjuguer indépendance et proximité**

- Conjuguer une Fonction Conformité intégrée (ou aussi intégrée que possible), l’indépendance des Compliance Officers, et leur proximité avec les opérationnels, sans laquelle la Fonction perd son efficacité et se réduit à un rôle plus administratif de contrôle, dénué d’ancrage au quotidien au sein des métiers opérationnels. Une Fonction intégrée est liée hiérarchiquement au sein d’une filière indépendante des métiers opérationnels, et en réfère directement à la Direction Générale.
- Fonction permanente de 2^e niveau →
 - **Pour les banques**, la Direction Générale désigne officiellement **un/e Responsable Conformité** (Directeur/trice de la Conformité/Chief Compliance Officer) dont le nom et les changements ultérieurs de nom sont communiqués à l’ACPR et lui accorde suffisamment de ressources humaines, financières et techniques pour réaliser les objectifs de conformité définis en lien avec l’appétit au risque de l’institution.

- **Pour les entreprises d'investissement**, cette Fonction est confiée à un/e Responsable de la Conformité des Services d'Investissement (**RCSI**) ou à un/e Responsable de la Conformité et du Contrôle Interne (**RCCI**) selon que l'on se trouve chez un prestataire de services d'investissement au sens large (transmission et exécution des ordres de bourse, conservation de titres, investissement pour compte propre etc...) ou bien dans une société de gestion de portefeuille. Les RCCI/ RCSI, qui rapportent à la Direction Générale, sont des collaborateurs de l'institution et ne sont pas nommés auprès du Superviseur, en revanche, leur fonction nécessite d'être en possession d'une carte professionnelle attribuée par l'AMF après un examen dédié.
- **Pour les assurances**, et comme les autres fonctions clés (actuariat, gestion des risques et audit interne), la Fonction de validation de la Conformité doit respecter des règles de compétence et d'honorabilité, rapporte au Conseil d'administration et à la Direction Générale, elle doit jouir d'une autorité suffisante et avoir accès à toute information nécessaire et elle doit avoir l'expertise et les ressources nécessaires. La personne responsable de cette Fonction est notifiée auprès de l'ACPR.
- Fonction indépendante :
 - Proche des opérationnels pour en garantir l'efficacité, cette Fonction doit toutefois être absolument impartiale et indépendante : la méthode pour déterminer la rémunération des personnes pertinentes dans la Fonction de Conformité ne peut en aucun cas mettre en péril leur objectivité ni donner l'impression qu'elles mettent cette objectivité et cette indépendance de jugement en péril ;
 - Mobilités : les personnes occupant un poste au sein de la Fonction Conformité ne peuvent pas être concernées par l'exécution de services et d'activités dont elles exercent la surveillance.

b) Conjuguer conseil expert et contrôle permanent de niveau 2

Le/la Compliance Officer assure à la fois un rôle de conseil et un rôle de contrôle de la chaîne de conformité. Ce rôle est défini de manière plus précise dans le cadre des missions de la Fonction Conformité *infra*. De manière synthétique, il/elle remplit les missions suivantes :

- Sensibilisation et mobilisation de l'ensemble de l'institution sur les risques de non-conformité, sa prévention et sa gestion, en fonction de l'appétit au risque arrêté par les instances de gouvernance
- Assistance et conseil des unités opérationnelles (niveau transactionnel) et instances dirigeantes (niveau corporate)
- Chef de file et « gardien du temple » sur certains processus clés (évaluation des tiers KYC, intégrité des marchés, criminalité financière, ...)
- Approche par les risques et plan de contrôle du dispositif de conformité
 - Contribution à la veille réglementaire
 - Cartographie des risques de non-conformité
 - Documentation normative
 - Formation, sensibilisation, communication
 - Gestion des événements et alertes de non-conformité
 - Procédure des contrôles de 2^e niveau et gardien de la cohérence et de la bonne articulation de la chaîne de contrôle de conformité de niveaux 1 et 2
 - Revue des contrôles de niveau 1 (sur base d'échantillons en général), réalisation des contrôles de 2^e niveau et documentation des résultats de ces contrôles
 - Mise en place d'actions correctrices (amélioration continue)

c) Inciter les instances dirigeantes à s'engager de manière forte

• **Direction Générale**

- Approuve la Charte de la Conformité
- Garantit que la Politique d'Intégrité est établie et respectée
- Améliore, autant que de besoin, cette politique et promulgue des sanctions en cas d'infractions graves
- Prend les mesures nécessaires afin que l'institution puisse disposer en permanence d'une Fonction de Conformité adaptée au niveau d'appétit au risque et indépendante
- Nomme le/la Chief Compliance Officer, en principe à temps plein ou sur une base permanente, et en communique le nom à l'Autorité de supervision
- Approuve le plan d'action de la Fonction Conformité et met les moyens requis à disposition en vue de son exécution.

• **Conseil d'administration**

- Corroboré par la recommandation de l'Agence Française Anticorruption (AFA) du 4 décembre 2020, le/la Chief Compliance Officer (CCO) fait rapport au Conseil d'administration, au moins chaque année, de l'évaluation du dispositif de conformité. Ce rapport intègre les objectifs réalisés, les moyens engagés (budget, ETP et autres moyens) ainsi que les activités (alertes, zones de fragilité, solutions préconisées, suivi).
- Il est devenu un standard, dans les grandes institutions du secteur financier, qu'un accès direct du/de la Responsable de la Conformité, et de plus en plus, des Responsables de la Conformité des pôles principaux d'activités opérationnelles, en réfèrent régulièrement au Conseil d'administration, dans un esprit de transparence et d'engagement.

4. Missions de la Fonction Conformité

a) Assurer la veille réglementaire, en liaison avec la Direction Juridique

- Identifier l'ensemble des lois et réglementations essentielles et pertinentes pour l'organisation
- Transposer les nouvelles normes dans les processus internes, à savoir dans les politiques, les chartes, les codes et les procédures opérationnelles
- Diffuser les résultats de la veille à l'ensemble du personnel selon son exposition aux risques et sa fonction.

Ainsi, dans l'exercice de ses fonctions et afin d'améliorer le développement du business de l'établissement, chaque agent/e est tenu au strict respect des procédures encadrant sa fonction.

b) Délivrer un conseil expert

- Agir en qualité de **conseiller auprès des opérationnels** sur des questions de conformité, en particulier, émettre un avis (« Compliance opinion ») sur des transactions ou sur les **nouveaux produits et services** (de l'émission d'un simple avis jusqu'à l'exercice d'un droit de veto, en fonction des orientations données par le Conseil d'administration et de la culture de chaque institution) ;

- **Conseiller la Direction** sur les lois, réglementations, règles et normes applicables et de l'informer de toutes évolutions dans ces domaines avec le concours de la Direction Juridique ;
- c) **Cartographier et gérer les risques de non-conformité dans toutes leurs composantes thématiques :**
- **Identifier et mesurer les risques de non-conformité dans une cartographie des risques (fréquence/impact)**, en précisant les risques de sanction afférents (en descendant lorsque nécessaire, jusqu'au maillon d'une thématique, par exemple le risque de corruption et de trafic d'influence, ou le risque d'abus de marché, puis par consolidation en maintenant la possibilité de « drill down » jusqu'à la thématique élémentaire) ; cela permet de mesurer l'exposition aux risques et les points de fragilité éventuelles,
 - **Gérer les risques de non-conformité et exercer un contrôle permanent :**
 - L'examen de la cartographie des risques permet ensuite de fixer les objectifs, les moyens et le programme de travail de la Fonction Conformité, selon une approche par les risques Cette responsabilité requiert une méthodologie robuste et doit rester lisible et transparente pour toute maille de la matrice organisationnelle de l'institution ;
 - **Réévaluer** régulièrement **les déformations de la cartographie des risques**, en procédant à des **évaluations et des analyses régulières** et exhaustives des risques de non-conformité ; **en signalant les résultats** sur une base régulière et dans les meilleurs délais, si nécessaire, à la Direction générale (voire au Conseil d'administration) ;
 - **Assurer le suivi de la documentation normative** relative aux risques de non-conformité (politiques, procédures et directives internes) ;
 - **Développer des indicateurs de mesure des risques** ; permet de déterminer la manière de qualifier et quantifier les risques précédemment identifiés ;
 - **Gérer les incidents risque** (identification / déclaration / évaluation / plan d'action / actualisation clôture) ;
 - **Organiser les comités de suivi** des risques de non-conformité ;
 - Mettre en place le **plan de contrôle des risques de non-conformité** et créer les **fiches de contrôle**, contrôler et assurer le suivi de toutes les mesures prises pour atténuer et gérer au mieux les risques de non-conformité ; établir et/ou superviser des vérifications et des **contrôles de conformité** appropriés (contrôles permanents de 2^e niveau), de manière articulée avec ceux du niveau 1 et ceux du niveau 3 - intervient au deuxième niveau de contrôle, comme défini dans l'arrêté du 3/11/2014 ; il revient en effet à la Fonction Conformité de s'assurer de la cohérence de la chaîne de conformité, front to end : en s'appuyant sur **des programmes de travail et de contrôle permanent établis et mis en œuvre sous son égide** concernant tout risque émergent, résultant du lancement d'une activité nouvelle / nouveau produit ou de l'évolution substantielle du profil de risque d'un produit / service existant ; et en s'appuyant sur les résultats des contrôles périodiques de 3^e niveau, effectués par l'Audit interne (et l'Inspection générale) dans le cadre de ses plans d'audit pluri-annuels, et des Commissaires aux Comptes et des Superviseurs le cas échéant ; à cet égard, il est louable de partager un même référentiel organisationnel commun aux 3 lignes de défense, afin de croiser les indicateurs pour identifier et ainsi mieux prévenir l'apparition de zones de fragilité et y remédier.

d) Circonscrire et assurer un programme ciblé de formation, sensibilisation, et information :

- Identifier les besoins et **former le personnel** en matière de conformité aux lois, règles et normes applicables, en fonction de l'exposition aux risques des différents collaborateurs, y compris les instances dirigeantes au plus haut niveau de l'organisation (sensibilisation, programmes de formation, communication)
- Accompagner à l'élaboration et assurer **l'application des principes d'éthique des affaires et des règles de conduite professionnelle.**

e) Gouvernance : être en relation avec les parties prenantes en matière de conformité :

- **Mettre en place un système d'alertes et de reporting** adéquats et adaptés aux activités opérationnelles de l'institution (internes / externes / réglementaires)
- **Assurer la liaison** avec les organes externes, régulateurs et organismes de réglementation pertinents sur les questions de conformité.

5. Les responsabilités de la Fonction Conformité

a) La responsabilité opérationnelle de la Fonction Conformité

Le/la Compliance Officer est un acteur essentiel de la protection de son établissement contre le risque réglementaire, éthique et de conduite des affaires ; il/elle joue notamment un rôle dans la protection contre la criminalité financière, de l'intégrité des marchés et est garant de la primauté des intérêts des clients.

- Promulgue des directives dans le cadre de la Politique d'Intégrité
- Établit des codes de conduite professionnelle, les procédures de conformité et développe des contrôles
- Etablit le plan de formation, en liaison avec les Métiers et les RH ; sensibilise, dispense une formation permanente au personnel, y compris les propres agents et veille à ce qu'une formation suffisante soit dispensée/prévue.
- Fait office de point de contact pour les Autorités de supervision et Auditeurs externes sur le périmètre de responsabilité de la Fonction Conformité ; met, volontairement et sur une base régulière, des rapports à la disposition de ces Autorités
- Établit un système (de contrôle) dans les domaines de travail de conformité et exécute des examens lorsque cela s'impose (par exemple monitoring dans le cadre de la prévention de blanchiment de capitaux, de conflits d'intérêts, ...)
- Donne des conseils au quotidien et en formalisant une « Compliance opinion » lors du lancement de nouveaux produits/activités ou l'entrée sur de nouveaux marchés
- Suit les nouvelles législations et réglementations dans des domaines de compliance, les interprète et conseille le management en cas d'évolutions dans ces domaines, en liaison avec la Direction juridique
- La fonction de Conformité a accès à toutes les informations qui ne sont pas des résultats de la Fonction de Conformité en soi (entre autres, Rapports d'Audit internes, rapports de la Direction Générale ou du Conseil d'Administration ou documents externes tels que des rapports d'audit ou la correspondance avec les Autorités)
- Fait rapport trimestriellement à la Direction Générale et annuellement au Conseil d'administration
- Établit un plan d'action écrit, qui repose sur une analyse méthodique des risques (approche par les risques)

- Réaliser un diagramme « en charge » / « contribue » tout le long de la chaîne de conformité, en fonction du domaine (l'AFA présente les rôles et responsabilités de l'ensemble des intervenants au sein de chaque processus de l'organisation).

b) La responsabilité juridique de la Fonction Conformité

En France, il n'existe pas de régime spécifique de responsabilité du Responsable de la Conformité ou d'un membre de la Conformité, différent de celui applicable à tout préposé dans le cadre de son contrat de travail.

La responsabilité juridique de la mise en œuvre des dispositifs de conformité aux obligations professionnelles pèse avant tout sur les dirigeants. En pratique, l'instance dirigeante délègue à la Fonction Conformité les missions opérationnelles de pilotage, de la mise en œuvre, de l'évaluation et de l'actualisation des dispositifs de conformité et de contrôles internes. Cette délégation doit prendre la forme d'une délégation de pouvoirs.

En cas de manquement à ses obligations professionnelles, le Responsable de la Conformité peut également faire l'objet de sanctions disciplinaires. Cette responsabilité est notamment appréciée au cas par cas, en fonction des négligences, du manque de compétence et du non-respect des éléments de reporting hiérarchique.

En cas de manquement à ses obligations professionnelles, le Responsable de la Conformité, qui occupe par ailleurs des fonctions de dirigeant, pourrait engager sa responsabilité civile, administrative, disciplinaire et pénale. A ce titre, il convient de différencier les fautes commises dans le cadre de ses fonctions de dirigeant, des fautes personnelles.

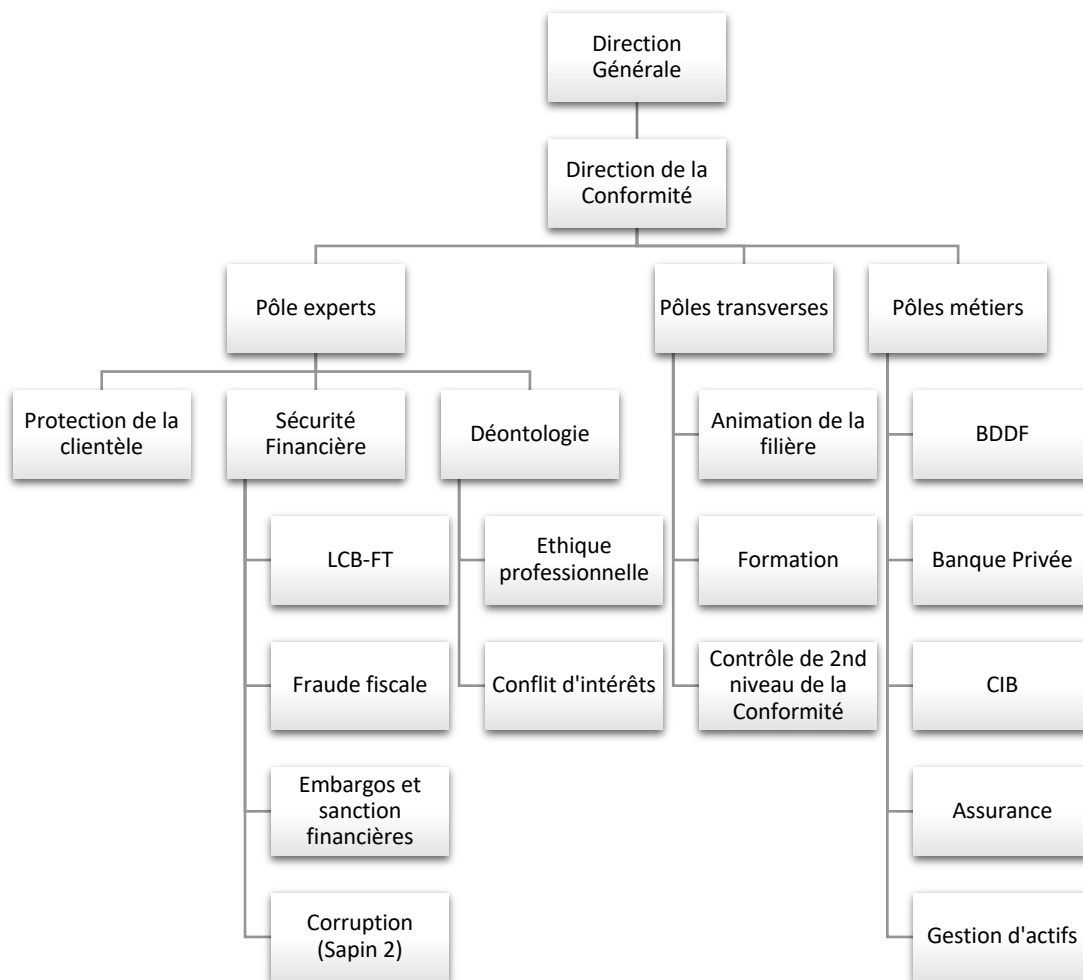
Selon l'organisation propre à chaque entreprise, il est possible d'inclure le Responsable de la Conformité dans l'assurance D&O¹.

6. Organisation de la Fonction Conformité

a) Exemple de modèle d'organisation de la Fonction Conformité

Au regard des différents modèles organisationnels retenus par les grandes institutions financières de la Place, se trouve ci-dessous un modèle parmi les plus aboutis actuellement de la Fonction Conformité. Le schéma sera bien sûr adapté en fonction de la taille, des métiers et du profil de l'établissement lui-même. Souvent, les CCO de région sont rattachés aux CCO des Pôles Métiers (Europe/UK, AMER et ASIA au Pôle CCO CIB, Afrique au Pôle Retail international, etc.). Les évolutions réglementaires tendent aujourd'hui à pousser vers une séparation du pôle expert Sécurité/Criminalité Financière de la Direction de la Conformité ; le/la responsable LAB-FT, qui valide la Politique Groupe en la matière, tend ainsi à en être indépendant/e.

¹ D&O : Directors & Officers



b) Principes de gouvernance de la chaîne de conformité

- **L'engagement crucial des instances dirigeantes, non exécutives et exécutives :**

- **Responsabilités du Conseil d'administration**

- Définir le niveau d'appétit au risque de l'établissement en matière de conformité ;
- Valider la cartographie des risques de non-conformité ;
- Examiner les rapports d'alertes et incidents majeurs et leur remédiation.

- **Responsabilités des dirigeants exécutifs (Direction générale, Directoire) :**

- La Direction générale doit approuver officiellement, sur proposition de la Fonction Conformité, la Politique de Conformité établie. L'efficacité de la mise en œuvre de cette politique doit être évaluée sur une base annuelle au moyen d'un rapport formalisé ;
- La Direction générale est responsable de la mise en œuvre d'une Politique de Conformité et d'une Fonction Conformité permanente, comme défini dans l'arrêté du 3/11/2014 ;
- Pour le secteur bancaire, un/e Responsable doit être officiellement désigné/e pour être chargé/e de la Fonction Conformité et son nom doit être communiqué à l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) ainsi que tous changements ultérieurs ;

- La Direction Générale est tenue d'évaluer, à intervalles réguliers, l'adéquation de la Politique de Conformité et de vérifier sa mise en œuvre sans réserve et son suivi par le personnel. La Politique doit exposer les principaux risques de non-conformité auxquels les entités sont confrontées ainsi que les mesures préventives à mettre en œuvre pour atténuer ces risques. Elle doit également comporter l'établissement d'une Fonction Conformité permanente, d'une Charte de la Conformité et d'un programme de formation continue à l'attention du personnel, qui traite de questions liées à la conformité ;
- Assurer un soutien indéfectible à la Fonction Conformité et valoriser la Fonction (rémunérations, reconnaissance, parcours de carrière, promotions et passerelles business, etc.).
- **Le/la Responsable de la Conformité Groupe :**
 - Un/e Responsable unique mondial de la Conformité dans les banques et les entreprises d'investissement
 - Si la filière est indépendante (budget unique, recrutement, évaluation, promotion de l'ensemble des collaborateurs de la filière, ...), alors les Responsables Conformité des entités seront rattachés hiérarchiquement à ce/tte Responsable groupe, avec un lien fonctionnel sur le/la Responsable de l'entité ou en double lien hiérarchique
 - Si la Conformité n'est pas organisée en filière totalement indépendante, ou en fonction d'exigences réglementaires locales, alors un double rattachement peut s'opérer : fonctionnel sur la Conformité groupe et hiérarchique sur le Responsable de l'entité
 - Evolution des fonctions Risques, Conformité et Contrôle dans les établissements bancaires et financiers, les sociétés d'assurance, les mutuelles et les sociétés de gestion d'actifs : ces fonctions ont subi une profonde mutation et convergé au fil du temps, sous l'effet des normes réglementaires internationales, européennes et françaises. Partant, les exigences en matière de gouvernance, de responsabilités et de compétences des Fonctions clés des établissements ont été structurellement modifiées du fait des évolutions des directives européennes et de leur transposition nationale :
 - Assureurs et mutuelles, soumises à la surveillance prudentielle de l'ACPR, Solvabilité II, la Notice ACPR sur la désignation des « dirigeants effectifs » et des « Responsables de Fonctions clés » dans le régime « Solvabilité II », 4 fonctions clés encadrent le dispositif de contrôle interne : actuariat, gestion des risques, audit interne et fonction de la validation de la Conformité
 - Banques et entreprises d'investissement : Directive 2019/878 (CRD 5), Arrêté du 22 décembre 2020 modifiant l'Arrêté du 3 novembre 2014 relatif au contrôle interne et visant à transposer la Directive 2019/878 (CRD5) relative à certaines règles applicables en matière de rémunération
 - En Asset Management, les normes de contrôle des risques et des rémunérations ont également évolué, des normes plus contraignantes encadrant les rémunérations des preneurs de risques et des Fonctions risques et contrôles, sont mises en place par les Autorités européennes de supervision
 - Bien que différentes du fait de la spécificité de leurs activités respectives, les responsabilités et compétences de la Fonction Conformité des différents établissements, ont évolué de concert.

- **Le rôle crucial des Opérationnels dans la chaîne de conformité** (Métiers et Fonctions supports) : il est clé car ce sont les collaborateurs les plus exposés aux risques ; ils constituent la 1^{ère} ligne de défense incontournable.

c) Aptitudes professionnelles du Compliance Officer

Un/e collaborateur/trice exerçant une responsabilité de « Compliance Officer » (CO) doit disposer des capacités et aptitudes nécessaires à l'exécution correcte et professionnelle des tâches qui lui sont confiées.

Cela requiert une formation continue et le recyclage réglementairement obligatoire, un travail de pensée personnel et des contacts étroits avec ses collègues, afin de conserver et d'approfondir leurs connaissances.

- Compétences requises :
 - Autorité, capacité d'organisation, communication orale et écrite ;
 - Forte capacité de synthèse voire de vulgarisation des connaissances pour extraire, à partir des constats techniques, les éléments réellement pertinents pour le Groupe et les expliquer clairement aux dirigeants effectifs ;
 - Capacité en termes de management d'équipe ;
 - Capacité d'évaluer les impacts possibles de tout changement de l'environnement réglementaire sur le Groupe et d'identifier et évaluer le risque de non-conformité ;
 - Commande linguistique.
- Certification, délivrée par les Autorités de surveillance. En France, en cas de départ du CO de l'établissement, la certification sera normalement caduque.

d) Synergies autour du CO

- Articulation de la Fonction Compliance Officer avec les autres acteurs : fonction de niveau 2, ses missions, son organisation, ses compétences, doivent être bien articulées avec les acteurs de niveau 1 et de niveau 3 de la chaîne de conformité, et avec les autres fonctions de niveau 2 (Risques et Finances principalement), mais également avec les autres Fonctions avec lesquelles une interaction est fréquente (Juridique, RH, etc.).
- A ce titre, une lettre de mission aide à délimiter les périmètres d'intervention de chacune des fonctions, sans pour autant nuire à une nécessaire transversalité d'action.

e) Profil/compétences d'un Compliance Officer senior

- « Hard skills » :
 - Maîtrise de la réglementation (LCB-FT, Bâle II, III et IV, RG AMF, loi Sapin II, RGPD, Arrêté du 3 novembre 2014, MAD/MAR, MIF I et MIF II, ...)
 - Connaissance et compréhension des métiers / produits / services ; vision transversale métier ;
 - Connaissance en finance, comptabilité et analyse des risques
 - Qualités rédactionnelles, documents appréhendables aussi bien par les Opérationnels que par les Autorités de contrôle et les Dirigeants de l'institution.
- « Soft skills » :
 - Ethique des affaires, savoir-être, posture : capacité à adopter une posture équilibrée entre indépendance de jugement et proximité des opérationnels (métiers et fonctions supports), afin de favoriser le dialogue et le soutien de l'activité

- opérationnelle tout en agissant avec indépendance et fermeté ; capacité à traiter en toute discrétion et fiabilité de l'information sensible ;
- Transparence : se faire toujours expliquer les transactions et les activités ; pragmatisme pour répondre aux questions posées et prise en compte à la fois de la réglementation et des aspects « business » ;
 - Privilégier le verbal, justifier toujours ses positions, prohiber les arguments d'autorité ; *in fine*, c'est à l'opérationnel, mais au bon niveau de l'organisation, de décider (il est rémunéré pour cette prise de risque en toute connaissance de cause), par processus d'escalade en cas de désaccord de la Fonction Conformité ; certaines institutions attribuent à la Fonction Conformité un droit de véto) ;
 - Rigueur et méthode pour prioriser les demandes (urgence / importance) ; respect des délais et réactivité pour répondre rapidement à des demandes urgentes, de la part de la Fonction Conformité et exigence d'un dossier convenablement documenté, de la part des Opérationnels, c'est une question de crédibilité et de reconnaissance mutuelles, et donc d'efficacité de la chaîne de conformité ;
 - Pédagogie afin de sensibiliser l'ensemble des opérationnels aux exigences de la Conformité et expliquer clairement et aussi simplement que possible des situations complexes
 - Sens du travail en équipe pour travailler en synergie avec d'autres services ; la Fonction Conformité est par essence transversale
 - Aisance relationnelle, car les relations sont nombreuses en interne (service comptable, juridique, ...) comme en externe (CAC, cabinets de conseil, avocats, ...).