Conformité et *compliance* : panorama des réglementations et des pratiques internationales

Si les grands principes de la fonction *compliance* sont identiques dans l'ensemble des pays, le périmètre de la fonction peut être très variable. Au-delà du respect des lois, cette fonction a également pour but de renforcer la déontologie et de limiter le risque d'image.

Marie-Agnès Nicolet
Associée
Audisoft Consultants

1. Conformité et compliance : des définitions qui impactent l'organisation

■ En France, la dernière modification du CRBF 97-02 (arrêté du 31 mars 2005) définit le risque de non conformité comme 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, ou qu'il s'agisse de normes professionnelles et déontologiques ou d'instructions de l'organe exécutif prises notamment en application des orientations de l'organe délibérant".*

Le comité de Bâle va plus loin. Dans sa publication d'avril 2005 [1], il insiste sur l'absolue nécessité d'instaurer une culture de l'éthique au niveau le plus haut de l'organisation, en recherchant non pas le simple respect des lois, mais l'esprit de la loi, dans la manière dont un établissement conduit l'ensemble de ses activités et dans ses comportements vis-à-vis des actionnaires, des clients, des salariés, et des marchés.

La définition bâloise des risques de conformité est ainsi globalement conforme à la définition française, mais le périmètre bâlois inclut spécifiquement la prévention du blanchiment et la lutte contre le financement du terrorisme, et peut s'étendre à la fiscalité des produits ou des clients. À cet égard, le texte du comité de Bâle met en garde les établissements bancaires contre les risques de *compliance* qui pèseraient sur eux lorsqu'ils participent, par exemple, à des montages qui seraient non-conformes à la législation fiscale.

Par ailleurs, le comité de Bâle insiste sur les différents types d'organisation possibles. Les grandes banques, notamment, peuvent disposer de fonctions au niveau du groupe, mais aussi au niveau local, ou positionnées dans les différents métiers. Dans les établissements plus petits, la fonction sera localisée uniquement en central. Par ailleurs, il peut exister des unités spécialisées dans certains domaines de la *compliance* comme la protection des données ou la prévention du blanchiment. Le texte bâlois indique également que les banques peuvent gérer les risques de *compliance* dans leurs structures de gestion globale des risques, ou très proches des risques opérationnels, compte tenu des relations étroites entre risques opérationnels et conformité.

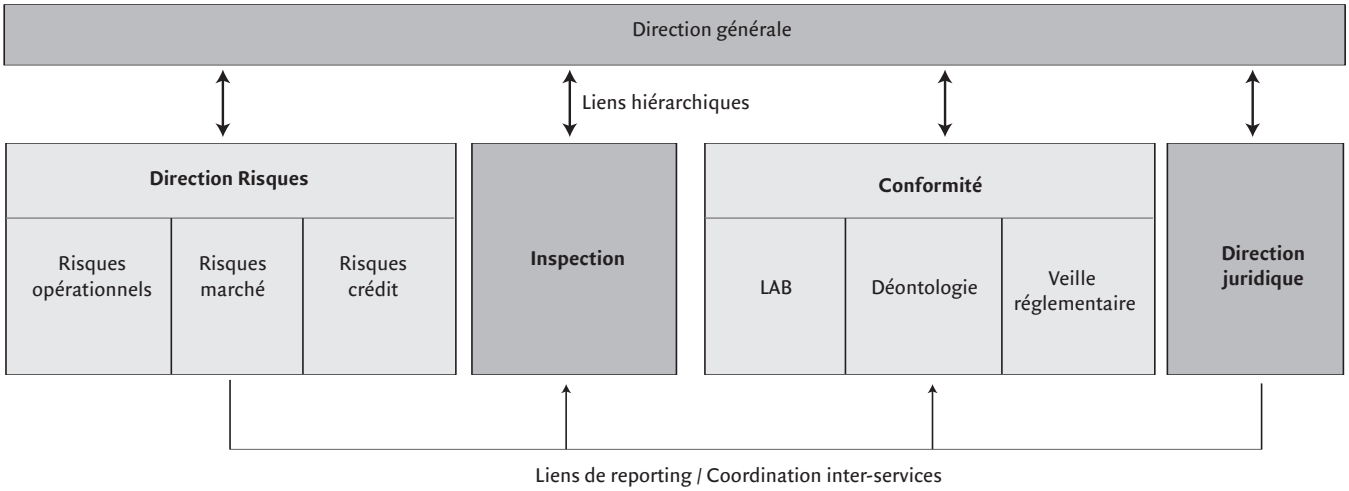
Cette proximité entre risques opérationnels et conformité est également évoquée par le texte luxembourgeois sur la *compliance* diffusé en septembre 2004 [2].

L'obligation de se doter d'une fonction de *compliance* visant à *"assurer le respect des règles d'intérêt général, dont celles relatives à la lutte contre le blanchiment et le financement du terrorisme, les règles de conduite du secteur financier et de protection des intérêts des investisseurs et des clients ainsi que les réglementations relatives aux domaines pour lesquels la Commission de surveillance du secteur financier conserve une responsabilité de contrôle…"* est également applicable aux succursales luxembourgeoises d'établissements d'origine communautaire.

Par risque de *compliance*, le texte luxembourgeois entend le risque de préjudices qu'un établissement peut subir suite au fait que les activités ne sont pas exercées conformément aux normes en vigueur. Il peut comporter une variété de risques tels que le risque de réputation, le risque légal, le risque de contentieux, le risque de sanctions ainsi que certains aspects du risque opérationnel.

Un tour d'horizon des réglementations internationales montre une assez grande homogénéité des définitions, avec toutefois, quelques différences en matière de périmètre et quelques précisions sur les moyens ou le positionnement de la fonction.

1. Exemple de schéma type d'organisation



LAB : lutte antiblanchiment.

Ainsi, le principe d'indépendance de la fonction par rapport aux opérationnels est un principe unanimement partagé. Dans la réglementation de la Financial Services Authority britannique (FSA) diffusé en janvier 2002 [3], il est précisé que la fonction de conformité doit disposer d'un accès illimité aux informations stockées par l'établissement (à l'instar des fonctions d'audit interne) et avoir un accès direct à la direction de la banque. Le texte français, quant à lui, indique que la fonction de conformité doit être prise en charge par une fonction indépendante des opérations commerciales, financières ou comptables et reporter à l'organe exécutif ou à l'un des responsables du contrôle permanent.

La Suisse, pour sa part, vient de diffuser un projet de modification de son texte de contrôle interne (projet de circulaire de la Commission fédérale des banques). La fonction *compliance* y est définie comme un fonction qui "assiste la direction et les collaborateurs de l'établissement en matière de *compliance*". Cette assistance consiste en général en des prestations de conseil, d'information, de formation, de surveillance et de recherche des manquements à la *compliance*, ainsi qu'en des rapports adressés à la direction. Dans les attributions de la fonction *compliance* devrait figurer notamment une appréciation au moins annuelle du risque de *compliance* et l'élaboration d'un plan d'action axé sur les risques. Ce projet de texte précise en outre que cette fonction peut constituer un département commun avec d'autres fonctions, comme le juridique, ou le contrôle des risques, dans la mesure où il n'existe pas entre elles de conflits d'intérêts.

Périmètre de la fonction de conformité et compliance

Le champ de la conformité est, en France, limité aux textes spécifiques aux activités bancaires et financières. Le droit social et fiscal est exclu de l'activité du responsable de la conformité, puisque ces réglementations ne sont pas spécifiquement bancaires. La définition de ce périmètre correspond également à la majorité des organisations bancaires en France, pour qui le droit du travail est sous la responsabilité des directions des ressources humaines, le risque fiscal dépendant d'une direction spécifique.

En revanche, une lecture extensive du texte français peut amener à élargir le périmètre de la fonction au respect de la conformité de l'ensemble des normes de la banque, puisque le risque de non-conformité est aussi lié au non-respect "d'instructions de l'organe exécutif prises notamment en application des orientations de l'organe délibérant".

C'est aussi la vision des réglementations japonaises et de celle de Hong Kong [4]: *"Staff performing the compliance function, in conjunction with management, establish and maintain sufficiently detailed compliance procedures covering legal and regulatory requirements including where applicable registration / licensing and financial resources requirements; record keeping (for management and regulatory reporting, audit and investigations); business practices; prevention of money laundering; internal control matters; and compliance with the relevant client, firm proprietary and staff dealing requirements."*

La FSA japonaise a également diffusé des *check-lists* très détaillées devant permettre aux établissements d'évaluer leurs dispositifs [5]. Dans ces deux derniers cas, le respect des procédures internes fait partie intégrante de la *compliance*.

2. Méthodologie des mesure des risques de non-conformité et connections avec les démarches risques opérationnels

Exemple 1

Catégories d'activité	Ingénierie financière	Opérations de marché/ négociation titres	Banque de détail	Opérations commerciales	Paiements et règlements	Services à la clientèle (dont conservation titres)	Gestion d'actifs	Réception/ transmission d'ordres

Processus		Événements de risque	Points de contrôle cible	Événements de risque couverts
P2	Réception des ordres			
E1		Litiges clients sur des ordres téléphoniques non confirmés par écrit (courrier, fax)	Contrôle de l'existence d'une confirmation écrite pour tout ordre téléphonique avant saisie de l'ordre	E1
E2		Litiges cliens suite au non-horodatage des tickets ou à un horodatage erroné.	• Mise en place de blocages informatiques (rejets des tickets non horodatés). • Contrôle de l'horodatage des tickets d'opéré par le back-office.	E2
E3		Pertes liées à une erreur de saisie de l'ordre du client dans le carnet d'ordre.	Contrôle de cohérence par un rapprochement des ordres saisis avec les confirmations des contreparties.	E3
E4		Litiges clients suite à une insffisance d'information du client sur les risques relatifs à l'opération transmise.	Formalisation des informations (fiches d'information) pouvant être communiquées aux clients (ordres téléphoniques et par internet)	E4, E5
E5		Litiges liés à un défaut de conseil ou à des conseils imprécis		
E6		Pertes ou litiges suite à des ordres clients émanant d'une personne non habilitée (usurpation d'identité)	• Contrôle systématique des pouvoirs des transmetteurs d'ordres (odres téléphoniques) • Attribution de codes d'accès pour les ordres par internet	E6, E7
E7		Litiges suite à la non vérification des pouvoirs des transmetteurs d'ordres (identité, capacité juridique...)		
E8		Litiges clients suite à une indisponibilité du site internet (sous capacité)	Contrôle régulier de la capacité et de la volumétrie des canaux à distance (stress scénario)	E8

Exemple 2

Catégories d'activité	Ingénierie financière	Opérations de marché/ négociation titres	Banque de détail	Opérations commerciales	Paiements et règlements	Services à la clientèle (dont conservation titres)	Gestion d'actifs	Réception/ transmission d'ordres

Processus		Réglementation AML*	Réglementation AMF	Réglementation CRBF	Autres réglementations
P1	Conservation de titres				
			Système de traitement de l'information non adapté à la taille du teneur de compte et aux volumes d'opérations traites (Art. 332-12)	Sécurité informatique inadaptée.	
			Absence de suivi d'indicateurs de fréquence des incidents informatiques (Art. 332-15).	Absence de comptabilité matière retraçant les entrées et sorties des avoirs détenus pour comptes de tiers.	
			Réalisation de mouvements d'instruments financiers hors délais fixés par les règles de marchés et systèmes de R/L (Art. 332-34).	Absence de surveillance des retards de réglement/livraison.	
			Non évaluation des risques relatifs à la mise en oeuvre des processus de règlement/livraison (Art. 332-43).	Défaut d'appréhension des différentes phases du processus de règlement/livraison (Art. 31-1, CRBF 97-02).	

* Anti-money laundering

La méthodologie de cartographie des risques opérationnels comme de non-conformité passe par une analyse des processus de l'identification des risques associés à chacun d'entre eux.

2. Benchmark des organisations existantes

Suite à la diffusion des modifications du CRBF 97-02, les établissements bancaires français ont commencé à organiser leur dispositif de suivi de la conformité. L'organisation la plus répandue est une fonction de conformité, séparée de la direction des risques et, bien sûr de l'Inspection générale ou de l'audit interne (*encadré 1*). Cependant, certains établissements réfléchissent à la possibilité de créer des directions conjointes comprenant à la fois les risques opérationnels et la conformité.

La plupart des établissements ont, contrairement à certains de ses homologues anglo-saxons, séparé la direction conformité de la direction juridique, même si certaines des missions de la fonction conformité, comme la veille réglementaire, peuvent être menées en commun.

Certains établissements internationaux font d'ailleurs des distinctions subtiles entre les différentes catégories de risques, et, en tout cas, entre le risque juridique et le risque de conformité. C'est le cas d'une grande banque suisse, qui dans son rapport annuel, distingue les risques suivants :

- *"transaction processing risk arises from errors, failures or shortcomings at any point in the transaction process, from deal execution and capture to final settlement*
- *compliance risk is the risk of financial loss due to regulatory fines or penalties, restriction or suspension of business, or costs of mandatory corrective action. Such risks may be incurred by not adhering to applicable laws, rules and regulations, local or international best practice (including ethical standards), or UBS's own internal standards*
- *legal risk is the risk of financial loss resulting from the non-enforceability of UBS's actual or anticipated rights arising under law, contract or other arrangement*
- *liability risk is the risk that we, or someone acting on our behalf, fail to fulfill the obligations, responsibilities or duties imposed by law or assumed under a contract and that claims are therefore made against us*
- *security risk is the risk of loss of confidentiality, integrity or availability of our information or other assets*
- *tax risk is the risk of additional tax arising from technically incorrect positions taken on tax matters, or failure to comply with tax withholding or reporting requirements on behalf of clients or employees; and the risk of claims by clients or counterparties as a result of UBS involvement in tax sensitive products or transactions."*

(source : UBS, rapport annuel 2003)

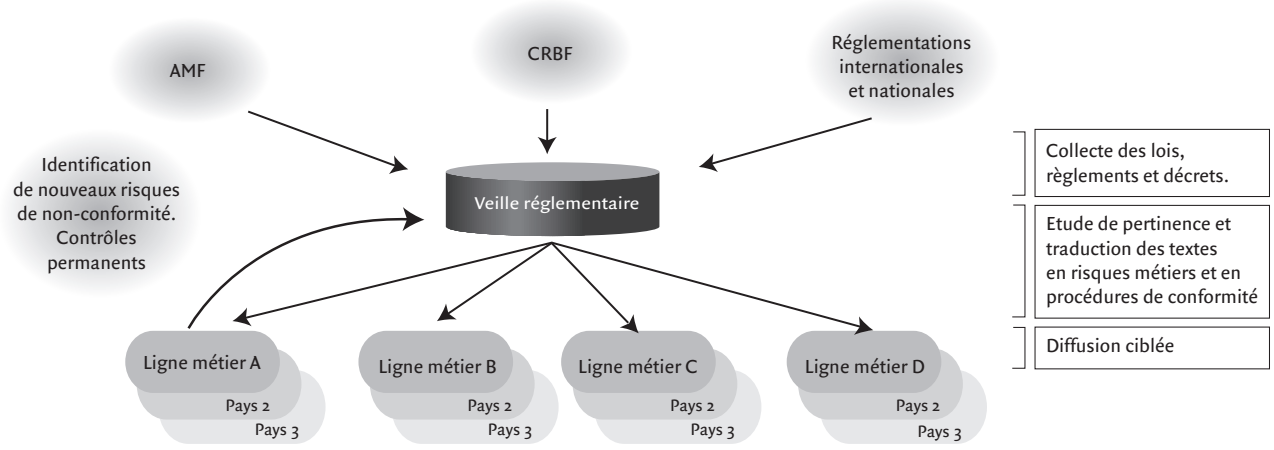
Risques opérationnels et conformité : des méthodologies convergentes ?

Les raisons pour lesquelles les directions de la conformité et des risques opérationnels peuvent être proches, voire sous la même responsabilité, sont assez évidentes. Tout d'abord, ces risques de conformité sont une partie importante d'une des catégories bâloises de risques opérationnels, la catégorie "clients-produits". Par ailleurs, dans certains domaines d'activités, fortement régulés, comme la conservation-titres, la gestion d'actifs ou la réception transmission d'ordres, une très grande partie des risques opérationnels sont en fait des risques de non-conformité (*encadré 2*).

Le principal enjeu de la mise en place de la fonction de conformité est ainsi de bien définir les responsabilités entre la conformité et les autres entités de la banque, notamment pour ne pas dupliquer les missions et assurer une exhaustivité des contrôles. Il est important que conformité et direction juridique par exemple, se coordonnent pour assurer la veille réglementaire (encadré 3), mais également que la conformité organise sa filière en se basant sur les autres centres d'expertise (par métiers ou pays) déjà en place. Par ailleurs, cette fonction doit assurer une coordination des contrôles de la conformité et organiser en conséquence la remontée des dysfonctionnements. Cette partie de la fonction n'est pas la plus simple, et c'est dans ce cadre qu'il est indispensable de capitaliser sur les démarches existantes de cartographies de risques opérationnels et de mise en œuvre de plans de contrôle plus généraux. ●

1. "Compliance and the compliance function in banks", Comité de Bâle, avril 2005
2. "La fonction compliance", circulaire de la CSSF 04/155, septembre 2004
3. "Senior Management Arrangements-Systems and Controls (SYSC)", FSA handbook, janvier 2002-
4. "Management, supervision and internal control Guidelines for persons licensed by or registered with the Securities and Futures Commission", Securities and Futures Commission, avril 2003.
5. "Guidelines for supervision", FSA

3. Organisation de la veille réglementaire



L'enjeu de la veille réglementaire au sein d'un groupe multinational consiste notamment à répartir cette veille par centres de compétences métiers et géographiques. La fonction de conformité groupe aura un rôle de consolidation, de mise à disposition d'information et de rediffusion aux entités concernées.