Le contrôle de la conformité : les « incontournables » de la sécurité financière

Comment une entreprise peut-elle se préparer à une mission de contrôle sur le dispositif « conformité » ? Des contrôles internes ou externes, quels sont les « points clés » sur lesquels le contrôle est réalisé ?

Un tel dispositif comprend, en principe, les thématiques suivantes : le dispositif « Lutte contre le blanchiment de capitaux et le financement du terrorisme – (LCBFT) », le respect des sanctions financières internationales et le programme « anticorruption ».

Cet article propose une synthèse « clé en main » sur les « jalons incontournables » du contrôle « compliance » en vue de garantir la sécurité financière.

I. Gouvernance

1) Celle-ci est structurée, en fonction des organisations, avec une comitologie dédiée. Le contrôle vérifie (i) l'existence de ces comités (qui en sont les membres permanents), (ii) à quelle fréquence le comité se réunit, (iii) la tenue et la formalisation des procès-verbaux.

2) Par ailleurs, les fiches postes des chargés de conformité (Compliance officers) et de tous ceux impliqués dans les processus sécurité financière doivent être bien formalisées.

3) Le contrôle est également effectué sur le corps procédural qui doit formaliser les règles et mentionner les processus en place à appliquer.

II. Connaissance de la relation

Les clients (KYC[1]), les fournisseurs (KYS[2]), les intermédiaires (KYI), les employés (KYE[3]) et autres KY nécessitent d'avoir un cadre clair pour répondre aux exigences réglementaires.

1) **La collecte des informations** lors de l'entrée en relation et aux dates de revue fixées en fonction de la sensibilité de la relation.
i. énumérer en détails les informations à collecter suivant le type du tiers ;
ii. formaliser la nécessité d'identifier les Personnes Politiquement Exposées (PPE) ;
iii. s'assurer de la tenue de logs d'activités, qui vont permettre l'enregistrement des activités de criblage et donc la production de la preuve ;
iv. traiter l'alerte générée par le *screening* des listes « PPE » est également un sujet de contrôle.

2) **L'évaluation des informations** à la lumière du risque que peut représenter la relation. Ainsi, un système de *scoring* doit être mis en place pour évaluer la sensibilité des clients et déterminer le niveau de risque de la relation (faible, standard ou élevé).

3) **Le processus de décision de l'entrée en relation.** Celui-ci doit être formalisé notamment lorsque la vigilance est renforcée. Pour les clients les plus risqués, on se réfère à la validation par la direction générale et la conformité.

III. Supervision des transactions

1) Il s'agit de mettre en place un **système automatisé** pour la surveillance des opérations des clients. Celui-ci intègre différents scenarii qui couvrent les risques de non-conformité. Le contrôle couvre à la fois l'existence d'un outil et son paramétrage, les scenarii et leur activation et les éventuelles exemptions de clients de cette supervision.
2) Le niveau des alertes générées par l'outil de supervision (volume des alertes *vs.* nombre de transactions) fait également l'objet de contrôle. Des seuils trop élevés fixés pour ces scenarii peuvent réduire le nombre d'alertes et donc, ne pas couvrir le risque.
3) Le dispositif de supervision des transactions est également couvert par deux autres canaux : (i) les escalades d'alertes manuelles (UAR (*Unusual activity report*)) et (ii) les alertes externes reçues du régulateur.
4) Les alertes doivent être traitées dans le délai imparti. Un commentaire doit être renseigné pour expliquer le traitement à la lumière des éléments du KYC. Il a été considéré par l'Autorité de contrôle prudentiel et de résolution (ACPR) qu'un commentaire « alerte cohérente » n'était pas pertinent.
5) Enfin, le contrôle vérifie l'existence du processus en place pour effectuer les déclarations de soupçons (DS) à Tracfin[4] : décision de faire une DS et respect du délai imparti.

IV. Gel des avoirs et sanctions financières internationales

Les mesures de gel des avoirs sont une des catégories de mesures prises dans le cadre du dispositif des sanctions internationales.

S'agissant du dispositif « Sanctions Financières Internationales », il permet la vérification des noms des tiers contre les listes de sanctions pour prévenir toute entrée en relation avec une personne sanctionnée. De même, les noms sont vérifiés tout au long de la relation contre ces mêmes listes. Ce dispositif nécessite la mise en place d'un outil automatisé pour le criblage/balayage des noms des clients ou tout autre tiers contre les listes de sanctions.

1 - KYC : Know Your Customers
2 - KYS : Know Your Suppliers
3 - KYE : Know Your Employees
4 - Tracfin (Traitement du renseignement et action contre les circuits financiers clandestins) est le service de renseignement français dédié à la lutte contre le blanchiment d'argent et le financement du terrorisme.

1) Le paramétrage de l'outil automatique est important pour fixer le niveau/taux de similarité à partir duquel l'alerte (ou hit) est générée.
2) Les listes de sanctions contre lesquelles les vérifications sont effectuées sont à définir pour couvrir les exigences réglementaires imposées à l'entreprise. Des listes internes peuvent être ajoutées et le sont généralement. Le contrôle va donc s'assurer des listes retenues.
3) Le contrôle examine la fréquence du criblage/balayage du portefeuille clients/tiers. L'obligation est bien celle de mettre en place le processus adéquat pour le criblage des noms des clients/tiers. Ce dispositif de criblage permettra le blocage des comptes des personnes désignées (lorsque la mesure de gel des avoirs est requise).
4) Un autre point est le dispositif mis en place pour identifier et prévenir tout contournement des sanctions financières. Aujourd'hui, des nouvelles règles sont en place pour condamner et sanctionner le contournement des sanctions européennes.

V. Contrôle permanent

Le contrôle permanent est composé de deux niveaux avec un premier niveau qui contrôle les opérationnels et un second niveau qui est celui de la Conformité.

1) Les points examinés par les missions de contrôle ciblent la formalisation d'un plan annuel de contrôles (interne). Ce plan doit être formalisé à la lumière des risques identifiés dans la cartographie.
2) De même, la cartographie des risques doit être en place avec une mise à jour régulière et les éléments constituant la cartographie des risques (méthodologie suivie et contenu) doivent être formalisés.

3) Le processus de déclarations des incidents doit être en place et être accessible aux personnes en charge. Le suivi de ces incidents est également contrôlé.

VI. Formation

Le dispositif « Conformité » - et plus particulièrement celui de la LCBFT - doit comprendre la mise en place d'un programme de **sensibilisation et de formation continue** des collaborateurs intégrant les sujets de la sécurité financière.

VII. Dispositif « Anticorruption »

La mise en place du dispositif « Anticorruption » comprend les huit axes de la Loi Sapin II, qui sont tous ciblés par les missions de contrôle. Ci-après quelques exemples[5] :
1) **L'engagement de l'équipe dirigeante** est contrôlé à travers différents éléments y compris la participation de l'instance dirigeante aux décisions impliquant des dossiers avec des faits de corruption.
2) L'existence d'un **code « anticorruption »** qui peut être intégré à un autre code. Cela est examiné par les missions de contrôle ainsi que la diffusion et la sensibilisation faite pour disséminer la culture des règles du code.
3) La **cartographie des risques de corruption** doit être réalisée séparément de celle des risques LCBFT pour identifier, analyser et hiérarchiser les risques de corruption externe et ce, en fonction des activités de l'entité.

Nathalie Sabek,
Vice-Présidente du Cercle de la Compliance

5 - Liste non-exhaustive.

Veille RGPD

Comité européen sur la protection des données (EDPB)

CEF 2025 : Lancement d'une mise en oeuvre coordonnée du droit à l'effacement. Le comité européen de la protection des données (CEPD) a, ce 5 mars 2025, annoncé avoir lancé son action relative au cadre coordonné de mise en oeuvre (CEF) pour 2025. À la suite d'une action coordonnée d'un an sur le droit d'accès en 2024, le CEF se concentrera cette année sur la mise en oeuvre d'un autre droit à la protection des données, à savoir le droit à l'effacement ou le « *droit à l'oubli* » (article 17 du RGPD). *https://veille.portail-rgpd.com/comite-europeen-sur-la-protection-des-donnees-edpb-29/*

CJUE – Arrêt C-203/22

Évaluation de crédit automatisée : la personne concernée a droit à ce qu'on lui explique comment la décision a été prise à son égard.
Dans un arrêt du 27 février 2025, la Cour de Justice a estimé qu'en matière d'évaluation de crédit automatisée (« *credit score* »), le responsable du traitement doit décrire la procédure et les principes concrètement appliqués de telle manière que la personne concernée puisse comprendre lesquelles ses données à caractère personnel ont été utilisées de quelle manière lors de la prise de décision automatisée.
https://veille.portail-rgpd.com/cjue-arret-c-203-22/

AEPD (autorité espagnole)

L'autorité espagnole a infligé des sanctions à 24 entités du groupe bancaire Caja Rural suite à une violation de données personnelles.
L'AEPD a, tout au long du mois de février, publié 24 décisions à l'encontre des entités du goroupe Caja Rural n raison de failles de sécurité ayant abouti à une violation de données en lien avec leur système d'authentification, géré par une autre entité du groupe agissant en tant que sous-traitante. Au total, 1,1 million d'euros d'amendes ont été prononcées. *https://veille.portail-rgpd.com/aepd-autorite-espagnole-34/*

CNIL

Sanctions et mesures correctrices : bilan 2024 de l'action de la CNIL.
L'année 2024 est marquée par une forte augmentation de l'ensemble des mesures correctrices prononcées par la CNIL : le nombre de sanctions a doublé et les mises en demeure et rappels aux obligations légales sont en constante hausse. Le nombre total de sanctions prononcées est passé de 21 en 2022 à 42 en 2023 puis 87 en 2024.
https://veille.portail-rgpd.com/cnil-47/

Etienne ORLEANSKI
Juriste en protection des données chez Airbus
Veille RGPD réalisée par le site Portail RGPD
https://veille.portail-rgpd.com/