Caixa Geral de Depositos

POLITIQUE DE PREVENTION ET DE GESTION DU RISQUE DE FRAUDE EXTERNE

MARS 2024

1. Cadre général

La présente Politique définit les principes, responsabilités et règles générales en matière de Prévention et de Gestion du Risque de Fraude Externe au sein de Caixa Geral de Depósitos, Succursale France (ci-après désignée la « Banque »).

Afin de protéger sa réputation et de répondre à ses obligations légales et réglementaires, la Banque adopte des mesures responsables visant à minimiser le risque de fraude externe ainsi que d'autres infractions connexes au sein de l'ensemble de son organisation.

Dans ce cadre, les risques de fraude externe sont définis en interne et des contrôles internes appropriés sont mis en œuvre en temps utile afin de prévenir, détecter et répondre à la fraude et aux autres infractions connexes.

La Politique adoptée repose sur un environnement de contrôle incluant un programme dans lequel la direction générale de la Banque montre l'exemple, et dans lequel sont promues des actions de formation et de communication visant à sensibiliser les collaborateurs et à instaurer une culture éthique et transparente.

La Politique de Prévention et de Gestion du Risque de Fraude Externe fournit des lignes directrices sur l'identification des fraudes, les contrôles à mettre en place pour prévenir et détecter les fraudes, ainsi que les étapes à suivre pour construire une réponse robuste, afin de protéger les intérêts de la Banque et de ses clients.

2. Définition de fraude

On peut définir la fraude comme la commission d'un acte illicite, intentionnel et de mauvaise foi, réprimé par la loi, par un fraudeur, dans le but de tromper ou de nuire à une personne ou à une organisation, en vue d'en tirer un bénéfice personnel ou au profit de tiers, d'éviter une obligation ou encore de causer des pertes à une organisation.

S'agissant de la fraude externe, elle peut être définie comme les pertes potentielles résultant d'activités frauduleuses menées par des clients de la Banque ou par des tiers (autres parties prenantes, à l'exception des collaborateurs).

Ainsi, la fraude externe survient lorsque les actes correspondant à la définition de la fraude sont commis par des personnes ou entités extérieures au Groupe CGD.

3. Les Dimensions du Processus de Prévention et de Gestion de la Fraude

Les processus de prévention et de gestion de la fraude sont structurés selon trois dimensions principales :
i) Planification et prévention
ii) Détection, diagnostic, analyse et résolution
iii) Contrôle et évaluation

3.1 PLANIFICATION ET PRÉVENTION

Afin de promouvoir une culture de gestion des risques et de renforcer les dispositifs de contrôle, la Banque est organisée conformément aux bonnes pratiques en matière de prévention du risque de fraude (« PRF »), avec une définition claire des rôles et responsabilités des différentes entités concernées, ainsi que des forums dans lesquels le risque de fraude est analysé et évalué de manière régulière et préventive.

3.1.1 Onboarding

Dans le cadre de l'établissement d'une relation d'affaires avec un nouveau client ou une nouvelle contrepartie, la Banque applique les diligences requises par les exigences Know Your Customer (« KYC »), conformément aux règles de prévention du blanchiment de capitaux et de lutte contre le financement du terrorisme (LCB/FT).

Ces procédures KYC, au-delà de leur rôle dans la lutte contre le blanchiment de capitaux et le financement du terrorisme (BC/FT), contribuent également à réduire l'exposition de la Banque aux risques financiers, réglementaires et/ou réputationnels.

3.1.2 Authentification

Afin de prévenir les risques de fraude, les risques réputationnels et réglementaires, ainsi que les violations ou vols de données, la Banque a mis en place des contrôles permettant de minimiser le risque d'accès non autorisé aux comptes et opérations des clients.

Ainsi, les méthodes d'authentification en vigueur à la Banque reposent sur une approche fondée sur les risques, et des mesures d'authentification renforcées (authentification forte) sont appliquées pour les opérations considérées comme présentant un risque accru.

3.1.3 Cybersécurité

La Banque publie en permanence sur son site institutionnel (www.cgd.fr) des alertes et recommandations de sécurité relatives à la protection contre les risques de fraude informatique (tels que le phishing et autres techniques similaires), afin de promouvoir une utilisation sécurisée d'internet et des services de paiement électroniques.

3.1.4 Sensibilisation des clients

La Banque met à disposition de ses clients et autres contreparties des matériaux de sensibilisation relatifs à la Prévention du Risque de Fraude (PRF), notamment via son site institutionnel et d'autres canaux de communication.

Elle y partage des informations sur les thématiques liées à la fraude, telles que les tendances actuelles, les campagnes en cours, et des alertes concernant des situations récurrentes.

3.2. DETECTION, DIAGNOSTIC, ANALYSE ET RESOLUTION

Dans le cadre de son approche fondée sur les risques, la Banque documente l'identification des pratiques frauduleuses potentielles et des activités suspectes. Cette approche intègre les processus, technologies et systèmes utilisés pour détecter les activités frauduleuses.

Afin de détecter les pratiques de fraude et les activités suspectes, la Banque a mis en place des contrôles proportionnés au niveau de risque de fraude identifié.

Tous les cas de fraude détectés sont gérés conformément aux processus internes définis dans le cadre de la PRF (Prévention du Risque de Fraude), et font l'objet d'un examen fondé sur l'ensemble des informations disponibles, en vue de déterminer s'il s'agit d'un incident de fraude potentiel.
Les cas suspects sont escaladés à un niveau supérieur de révision, accompagnés de la documentation justificative.

La Banque dispose d'un audit trail (traçabilité) pour tous les cas de fraude analysés, ainsi que des décisions prises et des actions menées pour atténuer le risque associé, permettant un reporting périodique des cas identifiés.

Dans le cadre de l'activité de Prévention du Risque de Fraude (PRF), en cas de suspicion d'incidents

de fraude externe et lorsque cela s'avère applicable, la Banque procède à un signalement auprès des autorités compétentes.

En complément, la Banque entretient une relation active et efficace avec les autorités, facilitant ainsi le partage d'informations, le soutien à la gestion des attaques frauduleuses, et une coopération renforcée dans les enquêtes relatives aux cas de fraude externe.

La Banque veille à répondre à toutes les demandes des autorités judiciaires ou de police dans les délais impartis par celles-ci.

3.3. CONTROLE ET EVALUATION

3.3.1 Évaluation des risques

La Banque réalise périodiquement une évaluation des risques métier en matière de fraude externe. Cette évaluation permet non seulement de déterminer les risques inhérents à la fraude externe, mais aussi d'apprécier l'efficacité des contrôles en place et d'identifier les opportunités d'amélioration.

La Banque applique une tolérance zéro à l'égard des incidents de fraude externe.

L'évaluation des risques comprend, a minima :

i) l'identification des risques propres à chaque domaine d'activité, en fonction de leur structure, produits, services et canaux de distribution ;

ii) l'identification des processus et contrôles existants mis en œuvre pour atténuer ces risques ;

iii) l'identification des lacunes ou faiblesses dans le dispositif de contrôle face à ces risques.

3.3.2 Évaluation de l'efficacité, amélioration continue et reporting

Les organes de structure concernés par la PRF réalisent des tests de contrôle afin d'évaluer la pertinence, la conception, et l'efficacité opérationnelle de leurs procédures, systèmes et contrôles antifraude.

Ces tests sont fondés sur les risques et adaptés aux spécificités de chaque entité impliquée dans la PRF, avec une attention particulière portée sur les transactions, les vulnérabilités client et les activités à plus haut risque de fraude.

Pour chaque incident de fraude détecté, la Banque effectue une analyse des causes, notamment en ce qui concerne le traitement des alertes, la résolution du cas et la réponse au client.
Les résultats de ces analyses alimentent les ajustements à apporter aux contrôles, aux procédures et aux évaluations de risque.

Les métriques de fraude constituent des outils essentiels pour quantifier et rendre compte de la nature des risques de fraude auxquels la Banque est exposée.
La collecte et l'analyse régulière et rapide des données sont indispensables à une gestion efficace, au reporting et à la supervision du risque de fraude.

Un rapport trimestriel est établi à destination de la Direction Générale, présentant les principales activités menées dans le cadre de la prévention et de la gestion de la fraude externe.

3.3.3 Archivage

Conformément aux bonnes pratiques en matière de conservation documentaire, la Banque conserve toute la documentation relative à la prévention et à la gestion du risque de fraude

externe pendant une durée minimale de 7 ans.

La Banque a mis en place des procédures, systèmes et contrôles documentés afin de garantir la conservation et l'accessibilité appropriée des documents mentionnés.

Tous les documents doivent être lisibles, audités, et récupérables, et la Banque veille à respecter l'ensemble des dispositions légales applicables en matière de confidentialité, de secret professionnel et de protection des données.

Christophe PINTO
Compliance Officer