Numéro 6 – Mars 2024
Service Audit

LA SÉCURITÉ SOCIALE - **2024**

CAHIER MÉTHODOLOGIQUE

Guide pour la mise en place d'un dispositif de lutte contre l'abus et la fraude

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Santé
et de la Sécurité sociale

Inspection générale de la sécurité sociale

Sommaire

1 INTRODUCTION

Dans le cadre de l'implémentation des éléments de bonne gouvernance introduits par la Loi du 9 août 2018[1], les institutions de sécurité sociale et le Fonds national de solidarité (ci-après dénommée(s) « *institution(s)* ») déterminent les règles de gouvernance à appliquer dans l'exécution de leurs missions et envers les parties prenantes dans lesquelles la politique de communication interne et externe, la politique de sécurité ainsi que la politique de lutte contre l'abus et la fraude jouent un rôle central[2].

La politique de lutte contre l'abus et la fraude (ci-après dénommée « *politique LAF »*) est un élément clé du dispositif de lutte contre l'abus et la fraude interne et externe (ci-après dénommé *« dispositif LAF »*) qui matérialise l'engagement de l'institution et oriente le pilotage des activités menées dans le cadre de la mise en œuvre dudit dispositif.

Le dispositif LAF, émanant du dispositif de gestion des risques et de contrôle interne, participe à l'amélioration de la gouvernance des institutions et contribue à la consolidation du lien de confiance entre les systèmes de sécurité sociale et les parties prenantes. Pour établir une vue globale et consolidée de tous les risques identifiés et évalués au sein de l'institution, le contrôle interne ou tout autre service désigné de la deuxième ligne de maîtrise, doit s'appuyer sur une seule méthodologie ainsi que sur des terminologies et une échelle de cotation des risques harmonisées. L'institution doit ainsi mettre en place des mesures garantissant que les ressources qui lui sont confiées sont utilisées à bon escient et sont protégées contre tout détournement ou toute utilisation abusive.

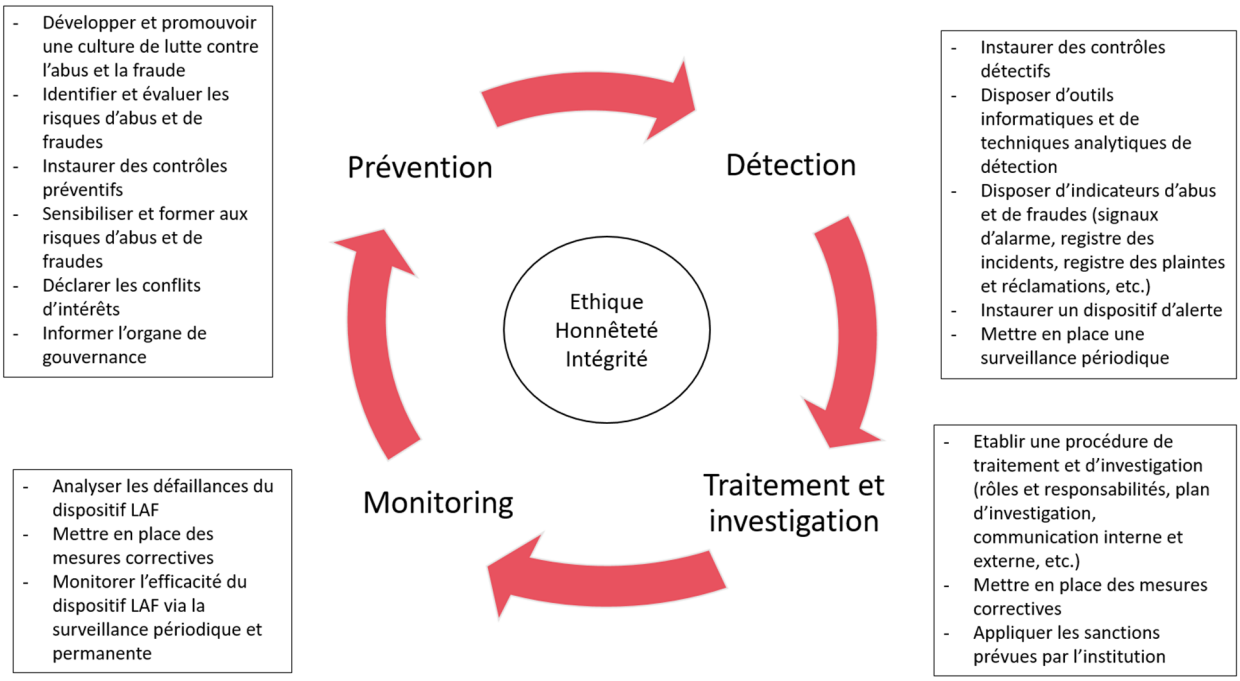
Un dispositif LAF est un procédé cyclique s'articulant autour de quatre grandes composantes, à savoir :

- La prévention ;
- La détection ;
- Le traitement et l'investigation ;
- Le monitoring.

[1] Loi du 9 août 2018 modifiant :
1. le Code de la sécurité sociale ;
2. la loi du 27 juin 2018 ayant pour objet l'organisation de l'Université du Luxembourg ;
3. la loi modifiée du 30 juillet 1960 concernant la création d'un fonds national de solidarité modifiant certaines dispositions du Code de la sécurité sociale.

[2] Code de la sécurité sociale (2023), Livre VI, Titre Ier, Chapitre Ier, article 408bis

Le dispositif de lutte contre l'abus et la fraude interne et externe[3]



La **prévention**, première composante du dispositif LAF, correspond notamment aux actions de sensibilisation et de dissuasion mises en place au sein de l'institution pour éviter la survenance de l'abus et de la fraude. Lorsque le passage à l'acte survient malgré tout, une **détection** rapide est primordiale afin d'en minimiser les conséquences (par exemple financières et réputationnelles). Les indicateurs d'abus et de fraudes et les contrôles détectifs font partie des outils pouvant être utilisés dans le cadre de la détection de l'abus et de la fraude. La détection passe également par le signalement des soupçons par les parties prenantes internes, externes ou tous autres tiers. Tout soupçon fait ensuite l'objet d'un **traitement** rigoureux impliquant, si nécessaire, une **investigation** en plusieurs étapes, la mise en place de mesures correctives et l'application de sanctions le cas échéant. Enfin, le dernier maillon du dispositif LAF comprend le **monitoring** de l'efficacité du dispositif dans son ensemble en vue de son amélioration continue.

Ce guide vise à accompagner les institutions lors de l'implémentation d'un dispositif LAF et de la rédaction de leur propre politique LAF en leur fournissant un cadre structuré et pratique. Dans ce contexte, le guide commence par la présentation du cadre légal européen et national (chapitre 2), la définition des thématiques en jeu, à savoir l'abus et la fraude (chapitre 3) ainsi que les facteurs déclenchants de l'abus et la fraude (chapitre 4). Les méthodologies et les bonnes pratiques ayant orienté la rédaction de ce guide sont énoncées au chapitre 5.

Le chapitre 6 informe sur la gouvernance d'un dispositif LAF et fait référence au Modèle des Trois Lignes de l'Institute of Internal Auditors (IIA).

Les chapitres 7, 8, 9 et 10 sont dédiés respectivement aux mesures de prévention et de détection, au dispositif d'alerte et au processus de traitement et d'investigation déployés dans le cadre d'un dispositif LAF.

Le chapitre 11 se concentre sur le monitoring de l'efficacité du dispositif LAF au travers de la surveillance permanente et de la surveillance périodique.

Le dernier chapitre du guide traite des aspects liés à la communication qui sont essentiels pour un dispositif LAF efficace.

Un ensemble d'annexes accompagne ce guide afin d'illustrer, par des exemples concrets et pratiques, les principes fournis tout au long du document.

Les éléments présentés dans ce document ont vocation à guider les institutions dans l'implémentation d'un dispositif LAF et dans rédaction de leur propre politique LAF. Ces derniers devront être adaptés au contexte organisationnel de chaque institution et tenir compte de la méthodologie retenue par l'institution en matière de gestion des risques et de contrôle interne. Plus particulièrement, les rôles et responsabilités de chaque acteur dans la lutte contre l'abus et la fraude devront être cohérents avec le mode de gouvernance et la structure organisationnelle propres à chaque institution.

[3] Illustration inspirée du document IFACI (2010), *La fraude – Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*

2 CADRE LÉGAL EUROPÉEN ET NATIONAL

La politique LAF fait partie intégrante, avec la politique de communication interne et externe et la politique de sécurité, des règles de gouvernance à appliquer par les institutions dans l'exécution de leurs missions et envers leurs parties prenantes[4].

Étant donné que chaque institution dispose d'une structure organisationnelle et de statuts qui lui sont propres, il appartient à chaque institution de préciser et de compléter les références légales et règlementaires applicables à son contexte.

2.1 Niveau européen

Au niveau européen, le cadre légal et règlementaire applicable se compose notamment :

- Du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données) ;
- De la Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union.

2.2 Niveau national

Au niveau national, le cadre légal et règlementaire applicable se compose notamment :

- De l'article 408bis du chapitre Ier, Titre Ier, Livre VI du Code de la sécurité sociale (2023) ;
- De l'article 419 du chapitre III, Titre Ier, Livre VI du Code de la sécurité sociale (2023) ;
- Des articles 445, 447, 449, 451 et 452 du chapitre III, Titre II, Livre VI du Code de la sécurité sociale (2023) ;
- Des articles 240, 246 à 249 et 251 à 253 du Chapitre II, Titre IV, Livre II du Code pénal (2023) ;
- Des articles 489 à 509-7, du Chapitre II, Titre IX, Livre II du Code pénal (2023) ;
- De l'article 10 au Point I, A, 2, Chapitre 5 du Code administratif de la fonction publique (2024) ;
- Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union ;
- Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État ;
- Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale ;
- Loi du 13 février 2011 renforçant les moyens de lutte contre la corruption et portant modification :
  1. du Code du travail,
  2. de la loi modifiée du 16 avril 1979 fixant le statut des fonctionnaires de l'État,
  3. de la loi modifiée du 24 décembre 1985 fixant le statut général des fonctionnaires communaux,
  4. du Code d'instruction criminelle et,
  5. du Code pénal.

[4] Code de la sécurité sociale (2023), Livre VI, Titre Ier, Chapitre Ier, article 408bis

3 DÉFINITIONS CLÉS

L'abus et la fraude sont des termes génériques visant des situations et des actions très variées. La définition de ces deux notions constitue le fondement de tout dispositif LAF.

3.1 Fraude

La notion de fraude est définie comme *« un acte intentionnel ou toute omission intentionnelle ayant pour but de tromper autrui, et qui entraîne une perte pour la victime et/ou un avantage pour le fraudeur »*[5].

En complément, suivant l'IIA, cette notion vise *« tout acte illégal caractérisé par la tromperie, la dissimulation ou la violation de la confiance sans qu'il y ait eu violence ou menace de violence. Les fraudes sont perpétrées par des personnes et des organisations afin d'obtenir de l'argent, des biens ou des services, ou de s'assurer un avantage personnel ou lié à l'activité »* [6].

Ces deux définitions mettent en évidence les éléments clés suivants de la fraude[7] :

Factuel

La fraude se matérialise par des actes et des comportements.

La falsification, la dissimulation, la dégradation intentionnelle ou encore le vol de biens appartenant à l'institution (fournitures, matériels, données, etc.), l'escroquerie et le détournement de fonds (fausses factures, manipulation de liquidités, etc.), ou encore les fausses déclarations (notes de frais fictifs, indicateurs, rapports ou contrôles falsifiés, etc.) constituent tous des actes factuels pouvant être qualifiés de frauduleux.

Illégal ou illégitime

L'acte est contraire à une disposition légale et/ou règlementaire, à une règle et/ou à une procédure interne instaurée par l'institution.

Intentionnel

La fraude est un acte ou une omission volontaire et délibérée (par exemple un assuré fournit de fausses pièces justificatives ou n'actualise pas sa situation afin de continuer à percevoir une prestation indue).

Avantage indu

L'acte frauduleux a pour objectif de faire bénéficier d'un gain financier, matériel ou personnel qui n'aurait pas été obtenu si l'acte n'avait pas été perpétré. Cet avantage peut être accordé au bénéfice ou au détriment de l'institution (par exemple la famille d'un assuré atteste de la persistance des droits sur la pension de vieillesse, alors que le bénéficiaire est décédé).

Fraude interne, externe voire mixte

La fraude est dite *« interne »* lorsqu'elle est commise par une partie prenante interne de l'institution sans distinction de son niveau hiérarchique.

La fraude est considérée *« externe »* lorsqu'elle est commise par une partie prenante externe de l'institution ou par un autre tiers, personne physique ou organisation.

La fraude peut également revêtir un caractère mixte (collusion) lorsque des parties prenantes internes et externes à l'institution ou tous autres tiers s'accordent ensemble pour procéder à un acte frauduleux.

[5] COSO, ACFE (2016), *Guide de gestion du risque de fraude - Synthèse*

[6] IIA (2017), *Cadre de référence international des pratiques professionnelles de l'audit interne*

[7] IFACI (2010), *La fraude – Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*

Au Luxembourg, la fraude sous forme d'escroquerie et de tromperie, constitue un délit passible d'une peine d'emprisonnement de quatre mois à cinq ans et d'une amende allant de 251 à 30.000 euros[8].

Exemples de fraude interne, externe et de collusion[9] :

Les exemples de fraude interne sont :

- Un collaborateur modifie le relevé d'identité bancaire (RIB) dans un dossier existant pour détourner un paiement ou un remboursement vers son propre compte bancaire ;
- Un collaborateur crée un dossier fictif (individu, carrière, demande de liquidation, etc.) pour détourner une pension de vieillesse ;
- Un collaborateur falsifie les états financiers ;
- Un collaborateur utilise le profil d'un autre utilisateur pour réaliser des transactions frauduleuses dans les systèmes d'information.

Les exemples de fraude externe sont :

- Un professionnel de santé facture des actes qu'il n'a pas réalisés ;
- Un assuré falsifie à son bénéfice la durée de l'arrêt de travail prescrit ;
- Un assuré fournit de fausses pièces justificatives ou n'actualise pas sa situation familiale pour continuer à percevoir des prestations indues ;
- Un assuré exerce une activité non autorisée pendant un arrêt de travail indemnisé ;
- Un assuré et son employeur se concertent pour déclarer un faux accident de travail ;
- Un professionnel de santé facture des actes de façon répétée et non justifiée par l'état de santé de ses patients.

Les exemples de collusion sont :

- Un collaborateur de l'institution réalise des remboursements indus sur le compte bancaire d'un proche ;
- Un collaborateur et un fournisseur se concertent pour des services ou des produits qui n'ont jamais été prestés/fournis mais qui ont toutefois été facturés et payés.

3.2 Abus

La notion d'abus est définie comme l'usage excessif, mauvais, injustifié ou injuste d'un droit, d'un privilège ou d'une prérogative ayant pour conséquence l'atteinte des droits d'autrui. L'abus de confiance est un type particulier d'abus qui consiste à détourner ou dissiper des fonds ou biens au préjudice d'autrui alors que ces biens avaient été confiés ou remis à la condition d'en faire un usage défini et particulier.

L'abus peut également revêtir un caractère mixte (collusion) lorsque des parties prenantes internes et externes à l'institution ou tous autres tiers s'accordent ensemble pour procéder à un acte abusif.

Au Luxembourg, l'abus de confiance constitue un délit passible d'une peine d'emprisonnement d'un mois à cinq ans et d'une amende allant de 251 à 5.000 euros[10].

[8] Code pénal (2023), Livre II, Titre IX, Chapitre II, articles 496 à 504

[9] Sources :
IFACI (2015), *Dispositifs de maîtrise des risques de fraude à l'assurance, à la retraite complémentaire et à l'action sociale, Cahier de la Recherche*, pages 33 à 66
IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*
Assurance maladie Alsace (2017), *Lutte contre les abus et les fraudes à l'Assurance Maladie en Alsace : les résultats pour l'année 2016, Conférence de presse, 19 mai 2017*
Assurance maladie Alsace (2016), *Lutte contre les abus et les fraudes à l'Assurance Maladie en Alsace : les résultats pour l'année 2015, Dossier de presse du 23 mai 2016*

[10] Code pénal (2023), Livre II, Titre IX, Chapitre II, articles 491 à 495

Exemples d'abus interne et externe[11] :

Les exemples d'abus interne sont :

- Un collaborateur pointe à la place de son collègue de travail ;
- Pour la rentrée scolaire, un collaborateur se sert des fournitures de bureau de l'entité (cahiers, stylos, etc.) pour les donner à son enfant.

Les exemples d'abus externe sont :

- Un professionnel de santé prescrit un arrêt de travail non justifié par l'état de santé du patient (assuré) ;
- Un assuré consulte deux ou plusieurs professionnels de santé pour se faire prescrire davantage de traitements médicamenteux non justifiés par son état de santé.

3.3 Erreur

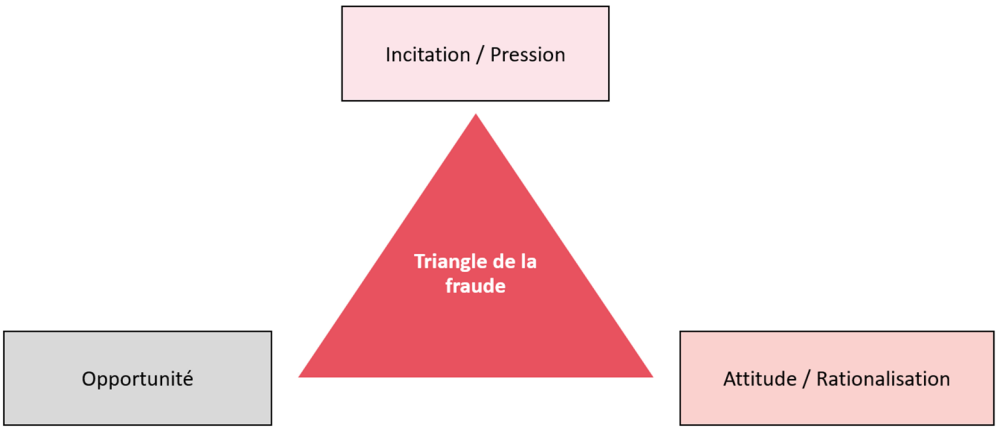
L'erreur est définie comme l'acte de se tromper ou comme tout acte, comportement inconsidéré, maladroit ou regrettable[12]. L'élément essentiel de distinction entre la fraude (respectivement l'abus) et l'erreur réside dans le caractère intentionnel ou non de l'acte qui est à l'origine de l'anomalie générée. En effet, à la différence de l'abus et de la fraude, l'erreur ne comporte ni un caractère intentionnel, ni une volonté de dissimuler[13].

Ainsi, tandis que l'abus et la fraude nécessitent un comportement volontaire, l'erreur est un acte involontaire.

[11] Sources :
IFACI (2015), *Dispositifs de maîtrise des risques de fraude à l'assurance, à la retraite complémentaire et à l'action sociale, Cahier de la Recherche*, pages 33 à 66
IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*
[12] Dictionnaire Larousse
[13] Norme internationale d'audit (ISA) 240 – *Les obligations de l'auditeur en matière de fraude lors d'un audit d'états financiers*

4 FACTEURS DÉCLENCHANTS : LE TRIANGLE DE LA FRAUDE

La théorie du triangle de la fraude permet d'illustrer les facteurs déclenchant le passage à l'acte frauduleux. Suivant cette théorie, la survenance d'une fraude résulte de la combinaison de trois facteurs. Chaque facteur est représenté par le côté d'un triangle qui, une fois combiné aux autres, favorise la survenance de la fraude[14].



Facteurs cumulatifs	Définition	Exemples
Opportunité	Le contexte et les circonstances créent des occasions ou des possibilités pour un acteur de commettre un acte frauduleux	• Absence de contrôles ou possibilité de les contourner • Séparation des tâches inadéquate • Non-traçabilité des logs et des actions utilisateurs • Niveau de confiance élevé envers un collaborateur
Incitation / Pression	Une situation (besoin) interne ou externe à l'organisation incite ou exerce une pression sur un acteur pour commettre un acte frauduleux	• Difficultés financières ou personnelles • Objectifs opérationnels exigeants • Liens de familiarité (assuré, médecin, fournisseur…) • Désir de pouvoir, d'influence ou d'estime
Attitude / Rationalisation	L'auteur avance des arguments rationnels pour justifier son acte et/ou possède des valeurs morales et éthiques lui permettant de commettre sciemment et intentionnellement des actes malhonnêtes	• « Tout le monde fait pareil » • « J'allais le rembourser plus tard » • « Juste pour cette fois » • « Ce n'est pas grave, personne ne le remarquera et/ou ne s'en souciera »

Dans le cadre du dispositif LAF, ces facteurs peuvent également être à l'origine d'un abus.

Étant donné qu'il s'avère difficile d'agir sur la rationalisation (qui varie d'un individu à l'autre), il sera nécessaire d'adopter des méthodes permettant d'influencer la motivation (incitation/pression) et les opportunités de passage à l'acte. Afin de contrer les actes abusifs et frauduleux, les collaborateurs de l'institution doivent être sensibilisés aux facteurs organisationnels et personnels à l'origine de ces actes dans la mesure où ils augmentent le risque d'abus et de fraudes. Des exemples de facteurs déclenchants sont repris à l'annexe 1 du présent guide. L'annexe 2 vise à illustrer les principales faiblesses dans un dispositif de contrôle interne.

Pour en savoir plus

- IFACI (2015), Dispositifs de maîtrise des risques de fraude à l'assurance, à la retraite complémentaire et à l'action sociale, Cahier de la Recherche :
  - Partie 1 - Introduction
- IFACI (2010), La fraude – Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche :
  - Partie 1 - De quoi parle-t-on ?

[14] Illustration inspirée du document IIA (2021), *OECD Global Anti-corruption & Integrity Forum, Webinar on Accountability, Actions and Assurance in Fighting Fraud*

5 MÉTHODOLOGIES PROPOSÉES POUR LA MISE EN PLACE D'UN DISPOSITIF DE LUTTE CONTRE L'ABUS ET LA FRAUDE

Le présent guide a été rédigé en considérant un ensemble de méthodologies et bonnes pratiques en la matière, telles que :

- ACFE, Grant Thornton (2020), Anti-fraud playbook - The best defense is a good offense ;
- ACFE, AICPA, IIA (2008), Managing the Business Risk of Fraud - A Practical Guide ;
- AISS (2019), Les lignes directrices de l'AISS en matière de bonne gouvernance ;
- AISS (2019), Les lignes directrices de l'AISS en matière d'erreur, d'évasion et de fraude dans les systèmes de sécurité sociale ;
- CGMA (2012), Report Fraud risk management - A guide to good practice ;
- COSO, ACFE (2016), Fraud Risk Management Guide ;
- IFACI, PWC (2013), COSO Référentiel intégré de contrôle interne - Principes de mise en œuvre et de pilotage ;
- IFACI (2015), Dispositifs de maîtrise des risques de fraude à l'assurance, à la retraite complémentaire et à l'action sociale, Cahier de la Recherche ;
- IFACI (2011), Des clés pour la mise en œuvre et l'optimisation du contrôle interne, Cahier de la Recherche ;
- IFACI (2010), La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche ;
- IIA (2020), Le Modèle des Trois Lignes de l'IIA, Version 2020 des Trois Lignes de Maîtrise ;
- IIA (2019), Prise de position Fraude et Audit interne : Fournir une assurance sur les contrôles anti-fraude est indispensable pour garantir leur efficacité.

Les références à ces méthodologies et bonnes pratiques sont indiquées dans le corps du texte et/ou les notes de bas de pages du présent guide. De même, les renvois vers des documents, textes ou exemples repris sous *« Pour en savoir plus »* détaillent ou illustrent les informations traitées dans les chapitres respectifs.

6 GOUVERNANCE DU DISPOSITIF DE LUTTE CONTRE L'ABUS ET LA FRAUDE

L'établissement d'un dispositif de gestion des risques et de contrôle interne, dont émane le dispositif LAF, repose notamment sur la définition et la formalisation de politiques et de procédures ainsi que sur une structure organisationnelle de gestion des risques et de contrôle interne avec des rôles et responsabilités bien définis, compris et délimités.

Tout en respectant le Code de la sécurité sociale (CSS), la transposition du Modèle des Trois Lignes de l'IIA permettra aux institutions de définir un cadre visant la mise en cohérence des dispositifs et fonctions impliqués dans la gestion des risques, le contrôle interne et par conséquent, la lutte contre l'abus et la fraude.

Toutefois, en fonction du contexte spécifique à chaque institution, la structure organisationnelle, les missions, le périmètre et les rôles et responsabilités de chaque acteur dans la gestion des risques en général et dans la lutte contre les abus et les fraudes internes et externes en particulier, ainsi que leur manière de collaborer, pourront varier. Il incombe donc à chaque institution d'adapter son modèle de gouvernance et d'organisation à ses propres objectifs, défis, contraintes et spécificités.

6.1 Rôles et responsabilités de la « Première ligne de maîtrise »

Selon le modèle de l'IIA, la première ligne de maîtrise, assurée par les managers opérationnels (personnel d'encadrement des activités *« cœur de métier »* et *« support »*) et leurs équipes, endosse et gère les risques au quotidien, y compris les risques d'abus et de fraudes. Ainsi, ils s'assurent que, dans le périmètre de leurs activités respectives, les risques sont bien identifiés et évalués, que des contrôles ont été mis en place pour les mitiger et, le cas échéant, que des mesures correctives sont mises en œuvre pour pallier les faiblesses des processus et des contrôles existants. Dans ce contexte, ils peuvent recevoir une aide méthodologique de la part des acteurs de la deuxième ligne de maîtrise.

Les managers opérationnels s'assurent ainsi de la mise en place d'un dispositif de gestion des risques et de contrôle interne efficace en supervisant les activités de leurs équipes au travers de contrôles adéquats et en veillant au respect des règles et procédures internes de l'institution.

La première ligne de maîtrise rapporte au président, ou selon l'article 397 alinéa 3 du CSS, à un fonctionnaire de l'État, un fonctionnaire y assimilé ou un employé assimilé à un employé de l'État de l'institution de sécurité sociale.

6.2 Rôles et responsabilités de la « Deuxième ligne de maîtrise »

La deuxième ligne de maîtrise, rapportant au président (et/ou au collaborateur désigné suivant les dispositions de l'article 397 alinéa 3 du CSS), assure des activités d'appui à la gestion des risques et au contrôle interne. Cette ligne est chargée de fournir un support méthodologique aux managers opérationnels et à leurs équipes (1ère ligne de maîtrise), d'apporter une expertise, une assistance, un suivi et des critiques constructives sur les questions ayant trait aux risques ainsi que de produire des analyses et des rapports sur l'adéquation et l'efficacité de la gestion des risques (contrôle interne y compris). Suivant le modèle de l'IIA, la deuxième ligne de maîtrise est composée des métiers axés sur les risques tels que la gestion des risques, la conformité, le contrôle interne, la sécurité des systèmes d'information, l'assurance qualité, etc.

Dans le cadre de la lutte contre l'abus et la fraude, un service dédié à la lutte contre l'abus et la fraude (ci-après dénommé *« service LAF »*) peut être créé et positionné au niveau de la deuxième ligne de maîtrise dudit modèle[15]. En l'absence d'un service LAF, un service de la deuxième ligne de maîtrise devra être désigné pour assumer les rôles et responsabilités dudit service. Dans la suite du guide, il est supposé qu'un service LAF est en place au sein des institutions.

Ainsi, le service LAF peut par exemple assister les managers opérationnels et leurs équipes (1ère ligne de maîtrise) dans l'identification et l'évaluation des risques d'abus et de fraudes (Point 7.2.), coordonner et soutenir l'implémentation de contrôles adéquats et de mesures correctives en cas de défaillances (Point 7.3.), conduire les investigations lorsqu'un soupçon d'abus ou de fraudes est signalé (Chapitre 10), etc.

[15] IIA (2020), *Le Modèle des Trois Lignes de l'IIA, Version 2020 des Trois Lignes de Maîtrise*

Le service LAF, qui peut également avoir pour responsabilité d'élaborer la politique LAF et de mener des campagnes de sensibilisation en la matière (Point 7.4.), rapporte périodiquement à l'organe de gouvernance. L'organe de gouvernance se compose du conseil d'administration (CA), du président et de tous les collaborateurs désignés suivant les dispositions de l'article 397 alinéa 3 du CSS.

Des exemples de rôles et responsabilités dans un dispositif LAF sont fournis à l'annexe 3 du présent guide.

Dans la suite du guide, une vue plus détaillée des rôles et responsabilités de chaque acteur par composante (prévention, détection, traitement et investigation, monitoring) du dispositif LAF est fournie.

Le rôle de la troisième ligne de maîtrise est abordé sous le point 11.2.1.

À noter que l'organe de gouvernance ne fait partie d'aucune des trois lignes de maîtrise. Toutefois, il a pour responsabilité ultime la conception, la mise en place et la surveillance de la gestion des risques et du contrôle interne, y inclus le dispositif LAF. Aussi, il doit rendre compte envers les parties prenantes au sujet de la surveillance et de la supervision de l'institution.

Pour en savoir plus

- IIA (2020), Le Modèle des Trois Lignes de l'IIA, Version 2020 des Trois Lignes de Maîtrise
- ACFE, AICPA, IIA (2008), Managing the Business Risk of Fraud - A Practical Guide :
  - Section 1 - Fraud risk governance
  - Appendix B - Sample framework for a fraud control policy
  - Appendix C - Sample fraud policy
- CGMA (2012), Report Fraud risk management - A guide to good practice :
  - Appendix 2 - A sample fraud policy
- COSO, ACFE (2016), Fraud Risk Management Guide :
  - Chapter 1 - Fraud risk governance
  - Appendix F-4 - Sample fraud risk management policy
  - Appendix I-1 - Fraud risk governance scorecard
- IFACI (2010), La fraude – Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche :
  - Partie 3 - Construction et pilotage du dispositif anti-fraude
  - Annexe 3 - Exemple de politique anti-fraude

7 PRÉVENTION DE L'ABUS ET DE LA FRAUDE

Le dispositif LAF émane du dispositif de gestion des risques et de contrôle interne de l'institution. Ce dernier permet à chaque institution de gérer ses risques et de faciliter la réalisation de ses objectifs. Tel que pour le dispositif de gestion des risques et de contrôle interne de l'institution, la prévention est un maillon essentiel du dispositif LAF. Les mesures de prévention visent à empêcher la survenance d'un abus ou d'une fraude et à réduire les risques de passage à l'acte en mettant l'accent sur le développement d'une culture fondée sur l'honnêteté et l'intégrité, sur la compréhension des risques et leur maîtrise et sur la sensibilisation des collaborateurs.

7.1 Culture de lutte contre l'abus et la fraude

Un dispositif LAF doit avant tout reposer sur un environnement et une culture commune de lutte contre l'abus et la fraude. L'organe de gouvernance de l'institution doit promouvoir une culture en accord avec les principes d'honnêteté et d'intégrité de l'institution. Il montre l'exemple en la matière *(« Tone at the top* »). Au travers de cette culture commune, chaque collaborateur doit se sentir responsable d'adopter les bons comportements et de montrer l'exemple en veillant à ce que les dispositions légales et/ou règlementaires, les procédures et politiques internes, ainsi que le code de conduite soient respectés.

En plus de l'implication de l'organe de gouvernance, une culture de lutte contre l'abus et la fraude requiert également une communication structurée entre les services, ainsi que des actions de sensibilisation contre l'abus et la fraude.

Par ces moyens, l'institution peut créer un climat propice au succès du dispositif LAF en s'assurant de l'engagement de tous à la protection de l'institution contre des événements qui pourraient lui nuire financièrement ou rompre la relation de confiance qu'elle a nouée avec ses parties prenantes.

Le service LAF, ou tout autre service de la deuxième ligne de maîtrise, peut être le point de contact et conseiller les collaborateurs ayant des interrogations, doutes ou inquiétudes en rapport avec les thématiques d'abus et de fraudes.

7.2 Identification et évaluation des risques d'abus et de fraudes

L'identification et l'évaluation des risques d'abus et de fraudes doivent être menées conformément à la méthodologie retenue dans la politique de gestion des risques et de contrôle interne de l'institution, qui décrit entre autres les référentiels, méthodes et outils retenus.

La prévention de l'abus et de la fraude a pour but principal de comprendre les risques associés et d'éviter leur réalisation. Il est donc essentiel que les risques d'abus et de fraudes auxquels l'institution est exposée soient identifiés et évalués pour chaque activité et/ou processus (Annexe 4).

Préalablement à son analyse, l'institution doit avoir défini une catégorisation des risques d'abus et de fraudes. Une fois la catégorisation déterminée, l'analyse des risques commence par l'identification des scénarios (également appelés schémas) d'abus et de fraudes, puis l'évaluation de la probabilité d'occurrence et des impacts qu'ils peuvent engendrer pour l'institution afin de définir les contrôles adéquats à mettre en place. Cette analyse sera documentée dans une cartographie des risques d'abus et de fraudes afin d'obtenir une vue globale sur lesdits risques.

En utilisant le concept de *« thinking like a fraudster »*[16] (penser comme un fraudeur), des scénarios d'abus et de fraudes peuvent être développés sur base :

- De cas avérés et d'investigations passées ;
- De risques déjà identifiés (grâce à d'autres mesures de gestion des risques établies, grâce à des discussions avec les collaborateurs en charge des processus et les parties prenantes, etc.).

Les étapes pour l'identification et l'évaluation des risques d'abus et de fraudes sont résumées à l'annexe 5 du présent guide.

[16] ACFE, Grant Thornton (2020), *Anti-fraud playbook – The best defense is a good offense, Play 3*

Une vue synthétique des risques d'abus et de fraudes et des contrôles y relatifs, est communiquée périodiquement par le service LAF à l'organe de gouvernance de l'institution dans le cadre de son rôle de surveillance et de supervision.

La fréquence, les modalités de distribution, le contenu et la granularité des reportings dépendent des attentes de l'organe de gouvernance et doivent être détaillés dans la politique LAF.

7.2.1 Catégorisation des risques d'abus et de fraudes

La catégorisation des risques d'abus et de fraudes a pour objectif de favoriser la compréhension et l'identification des scénarios d'abus ou de fraudes y afférents.

Ainsi, en pratique, sur base des activités de l'institution, il s'agit de définir des catégories de risques d'abus et de fraudes pour pouvoir rattacher les risques identifiés à des scénarios d'abus et de fraudes.

Il incombe à chaque institution d'adapter la catégorisation des risques d'abus et de fraudes à ses spécificités, à son environnement et à son dispositif LAF. Ce dernier devra se baser, respectivement émaner, du dispositif de gestion des risques et de contrôle interne spécifique à chaque institution.

Avant de définir ladite catégorisation, il est recommandé de considérer le registre des risques émanant du dispositif de gestion des risques et de contrôle interne de l'institution.

Des exemples de catégorisation des risques d'abus et de fraudes sont fournis à l'annexe 6 du présent guide.

7.2.2 Impacts et conséquences liés au risque d'abus et de fraudes

Le risque d'abus et de fraudes est un risque opérationnel bien souvent sous-estimé et pouvant impacter significativement l'organisation d'une institution.

L'illustration ci-dessous reprend à titre d'exemples et de façon non exhaustive différents impacts et conséquences possibles du risque d'abus et de fraudes :

	Impacts				
	Opérationnel	Réputation	Financier	Légal	Humain
Conséquences	Non-atteinte des objectifs opérationnels et stratégiques	Image et crédibilité affectées	Perte financière directe ou indirecte	Plaintes et réclamations auprès de l'institution	Démotivation du personnel
	Non-réalisation des projets	Confiance minée dans la fiabilité et les valeurs éthiques de l'institution	Augmentation des coûts de gestion et de recouvrement des abus et des fraudes	Sanctions ou pénalités légales	Mal-être, honte, burn out
	Perturbation des tâches opérationnelles (p.ex. augmentation des incidents, retards dans le traitement des dossiers, erreurs dans les montants remboursés)	Dégradation des relations vis-à-vis des tiers	Coûts additionnels (p.ex. consultance externe, avocats)	Condamnation de l'institution	Démissions volontaires

7.3 Contrôles préventifs

Le COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) définit une activité de contrôle préventive comme *« une procédure ou un processus spécifique conçu pour empêcher la survenance d'une fraude »*[17]. La prévention de l'abus et de la fraude passe donc notamment par la mise en place de contrôles visant à prévenir les risques d'abus et de fraudes.

Ainsi, des contrôles préventifs (mais aussi détectifs : Point 8.1.) peuvent être mis en place sur base de la cartographie des risques d'abus et de fraudes telle qu'élaborée au préalable. Cette cartographie des risques doit être tenue à jour et se faire en parallèle de l'évolution du dispositif de gestion des risques et de contrôle interne afin de garantir une cohérence entre les deux.

La première ligne de maîtrise (Point 6.1.), avec le support méthodologique de la deuxième ligne de maîtrise (service LAF) sélectionnent les activités et/ou processus à contrôler de manière prioritaire, définissent l'étendue et la fréquence des contrôles à réaliser et mettent en œuvre des actions correctives si nécessaire. L'ensemble de ces activités doit être documenté.

Les managers opérationnels de la première ligne de maîtrise sont donc responsables des contrôles réalisés dans le périmètre de leurs activités. Ils les déploient auprès de leurs équipes généralement par le biais de règles et procédures en s'assurant de la bonne compréhension des risques qu'impliquent les processus en question.

La première ligne de maîtrise rapporte au président et/ou au collaborateur désigné suivant les dispositions de l'article 397 alinéa 3 du CSS.

7.4 Sensibilisation et formation aux risques d'abus et de fraudes

Dans le cadre des mesures préventives, l'organe de gouvernance de l'institution doit veiller à ce que l'ensemble de ses collaborateurs soit sensibilisé et s'assurer qu'ils comprennent les risques d'abus et de fraudes ainsi que leurs potentielles conséquences sur l'institution. La sensibilisation permet de responsabiliser chacun des collaborateurs contre les actes abusifs ou frauduleux.

Pour ce faire, le service LAF peut tenir des sessions de formation auxquelles tous les collaborateurs devront participer. Ces formations permettent d'informer les collaborateurs sur les mesures mises en place dans le cadre du dispositif LAF pour la prévention, la détection, le signalement (y incluant le dispositif d'alerte, le respect de l'anonymat et la protection des données/des lanceurs d'alerte, etc.), le traitement des incidents et les sanctions encourues en cas d'abus ou de fraude avéré(e).

Des formations plus spécifiques peuvent également être envisagées dans les services les plus sensibles. De même, il incombe au service LAF de suivre des formations continues, nationales et/ou internationales facilitant le partage d'expérience et d'expertise dans le domaine LAF.

Des bonnes pratiques en matière de formation anti-fraude sont reprises à l'annexe 7 du présent guide.

La sensibilisation des collaborateurs peut aussi se faire par la diffusion de guides pratiques, la mise en place d'affiches, la diffusion de bulletins d'informations sur le site internet et intranet ou bien via des groupes de travail.

La sensibilisation passe également par une communication claire et transparente. En effet, comme recommandé par les lignes directrices 30 et 31 de l'Association Internationale de la Sécurité Sociale (AISS) en matière d'erreur, d'évasion et de fraude dans les systèmes de sécurité sociale, une communication transparente sur les actions et les résultats du dispositif LAF peut dissuader et prévenir les comportements abusifs ou frauduleux aussi bien en interne qu'en externe (Chapitres 11 et 12).

7.5 Déclaration des conflits d'intérêts

Pour éviter les situations à risque, l'institution peut aussi demander à toutes ses parties prenantes internes de déclarer annuellement tout conflit d'intérêt (réel ou perçu) qu'elles pourraient avoir avec une ou plusieurs parties prenantes de l'institution.

[17] COSO, ACFE (2016), *Guide de gestion du risque de fraude - Synthèse*, page 10

Rôles et responsabilités clés

- L'organe de gouvernance doit promouvoir une culture et un environnement favorable à la lutte contre l'abus et la fraude. Il montre l'exemple en la matière (« Tone at the top ») ;
- Le service LAF sensibilise les collaborateurs de l'institution à la théorie du triangle de la fraude, qui permet d'illustrer les facteurs déclenchant le passage à l'acte abusif et frauduleux ;
- Les collaborateurs doivent adopter les bons comportements et respecter le cadre légal et règlementaire, les procédures et politiques internes ainsi que le code de conduite de l'institution ;
- Le service LAF détermine en concertation avec le service juridique, les références légales et règlementaires applicables à l'institution ;
- Le service LAF définit la catégorisation des risques d'abus et de fraudes internes et externes en tenant compte du dispositif de gestion des risques et de contrôle interne de l'institution ;
- Sur base de cette catégorisation, la première ligne de maîtrise, avec le support méthodologique du service LAF, déterminent ensuite les scénarios (schémas) d'abus et de fraudes les plus pertinents pour chaque activité et/ou processus de l'institution ;
- La première ligne de maîtrise, avec le support méthodologique du service LAF, identifient et évaluent les risques d'abus et de fraudes pour chaque activité et/ou processus de l'institution en tenant compte de la méthodologie émanant du dispositif de gestion des risques et de contrôle interne de l'institution. Sur cette base :
  - Le service LAF élabore et tient à jour la cartographie des risques d'abus et de fraudes ;
  - La première ligne de maîtrise conçoit et met en œuvre des contrôles préventifs (mais aussi détectifs : Point 8.1.) nécessaires.
- Le service LAF communique périodiquement à l'organe de gouvernance sur les risques d'abus et de fraudes de l'institution ainsi que sur les contrôles y relatifs ;
- Le service LAF se charge des programmes de sensibilisation, dont par exemple l'organisation de formations sur les risques d'abus et de fraudes auxquelles tous les collaborateurs devront participer ;
- Le service LAF suit des formations continues, nationales et/ou internationales dans le domaine LAF ;
- Les collaborateurs s'informent et renforcent leur compréhension des risques d'abus et de fraudes ;
- Les parties prenantes internes déclarent annuellement tout conflit d'intérêt (réel ou perçu) qu'elles pourraient avoir avec une ou plusieurs parties prenantes de l'institution.

Pour en savoir plus

- ACFE (2023), *Fraud Risk Templates,* Fraud-Risk-Management-Tool-2.xlsm (live.com)
- ACFE (2023), *Anti-Fraud Data Analytics Tests,* Anti-Fraud Data Analytics Tests (acfe.com)
- ACFE (2021), Fraud awareness training – Benchmarking report
- ACFE (2020), Report to the Nations, 2020 Global Study on Occupational Fraud and Abuse. Government Edition
- ACFE, Grant Thornton (2020), Anti-fraud playbook – The best defense is a good offense :
  - Play 2 - Create a culture
  - Play 3 - Think like a fraudster
  - Play 4 - Discover what you don't know
  - Appendix B - Fraud risk map template
  - Appendix C - Implementation checklists
- ACFE, AICPA, IIA (2008), Managing the Business Risk of Fraud - A Practical Guide :
  - Section 2 - Fraud risk assessment
  - Appendix D - Fraud risk assessment framework example
  - Appendix E - Fraud risk exposures
  - Appendix F - Fraud prevention scorecard
- COSO, ACFE (2016), Fraud Risk Management Guide :
  - Chapter 1 - Fraud risk governance
  - Chapter 2 - Fraud risk assessment
  - Chapter 3 - Fraud control activities
  - Appendix G - Fraud risk exposures
  - Appendix H - Fraud risk assessment example
  - Appendix I-2 - Fraud risk assessment scorecard
  - Appendix I-3 - Fraud control activities scorecard
- IFACI (2015), Dispositifs de maîtrise des risques de fraude à l'assurance, à la retraite complémentaire et à l'action sociale, Cahier de la Recherche :
  - Partie 1 - Introduction
  - Partie 2 - Prévenir et détecter la fraude au travers de scénarios
  - Annexe 1 - Modèle de fiche
- IFACI (2013), La cartographie des risques, Cahier de la recherche :
  - Partie 3 - Identification et évaluation des risques
- IFACI (2010), La fraude – Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche :
  - Partie 3 - Construction et pilotage du dispositif anti-fraude
  - Partie 5 - Un outil de prévention et d'anticipation : la cartographie des risques de fraude
  - Annexe 2 - Illustration de l'arborescence des types de fraude
  - Annexe 4 - Exemple de typologie de risques

8 DÉTECTION DE L'ABUS ET DE LA FRAUDE

Malgré les actions préventives contre l'abus et la fraude mises en place par l'institution, le risque zéro n'existe pas. De ce fait, il est nécessaire d'inclure au dispositif LAF des mesures de détection permettant de déceler et de contrer rapidement les actes abusifs ou frauduleux existants.

Les mesures de détection participeront également à l'effort de prévention, dans la mesure où elles auront un effet dissuasif sur un potentiel collaborateur ou toute autre partie prenante (ou tiers) qui serait tenté(e) d'abuser ou de frauder.

8.1 Contrôles détectifs

Le COSO définit une activité de contrôle détective comme *« une procédure ou un processus spécifique conçu pour détecter rapidement une fraude si elle survient »*[18]. Dans ce contexte, le dispositif LAF inclut notamment des contrôles manuels et automatisés dédiés à la détection d'abus et de fraudes. Ces contrôles ont pour but d'identifier suffisamment tôt de potentiels abus ou fraudes (mais aussi des erreurs) afin de réduire, le cas échéant, leurs impacts et de les traiter avec une plus grande efficacité. De tels contrôles incluent par exemple des réconciliations, des recomptages et inspections physiques ainsi que des autorisations.

Les contrôles détectifs à mettre en place dépendront des scénarios et des risques d'abus et de fraudes identifiés au préalable (Point 7.2.). Ils pourront donc varier au fil du temps en fonction de leur efficacité et de l'identification de nouveaux risques.

La première ligne de maîtrise collabore avec le service LAF (2ème ligne de maîtrise) pour définir de potentiels scénarios d'abus et de fraudes et les types de transactions que ces scénarios génèreront. En fonction de ces scénarios, ils sélectionnent des contrôles détectifs (mais aussi préventifs : Point 7.3.) à mettre en place et à réaliser.

La mise en place de contrôles récurrents ou en continu (par exemple la réconciliation des transactions journalières, la mise en place et le suivi de tableaux de bord et d'indicateurs, les requêtes informatiques, les rapports d'exception) permet de détecter d'éventuels écarts ou anomalies. Elle peut être facilitée et perfectionnée par l'implémentation de contrôles automatisés sur entre autres de larges bases de données, en utilisant des techniques d'analyse et d'exploration des données (Point 8.2.).

La première ligne de maîtrise et/ou le service LAF (en fonction des spécificités organisationnelles de chaque institution) collaborent ensuite avec le service informatique pour mettre en place ces mesures de détection automatiques. Si l'institution décide de recourir à ce type de contrôles, elle devra veiller au respect de la législation européenne et nationale en vigueur en matière de protection des données personnelles.

Des exemples de contrôles anti-fraude sont fournis à l'annexe 8.

L'efficacité des contrôles détectifs résultera en premier lieu de la qualité des mesures de prévention mises en place, qui permettront notamment de sensibiliser les collaborateurs aux risques d'abus et de fraudes et ce faisant, augmenteront leur vigilance pour détecter des incohérences dans les processus, les tendances, les comportements et/ou les transactions. Ces mesures permettront également de développer leur esprit critique pour ainsi éviter qu'ils se contentent d'explications superficielles lors de la justification d'écarts ou d'anomalies.

8.2 Outils informatiques et techniques analytiques

Il existe différentes techniques analytiques (par exemple l'analyse de données sur base de modèles connus, la détection d'anomalies, l'analyse prédictive, l'analyse relationnelle, l'analyse de texte) susceptibles d'être sélectionnées et configurées en fonction des scénarios d'abus et de fraudes identifiés sur base des besoins et risques spécifiques à chaque institution (Annexe 9).

Ces techniques peuvent permettre d'identifier des anomalies dans les processus, les tendances, les comportements ou les transactions, qui constituent des signaux potentiels d'actes abusifs ou frauduleux. Elles peuvent permettre, par exemple, de vérifier le respect des cycles de validation et des seuils de déclenchement et, le cas échéant, de produire des rapports d'exception ou des listes d'anomalies à analyser. Par ailleurs, elles peuvent également

[18] COSO, ACFE (2016), *Guide de gestion du risque de fraude - Synthèse*, page 10

détecter, en explorant les bases de données, des situations dans lesquelles la combinaison de certains facteurs prédéfinis pourrait présenter un risque d'abus ou de fraudes pour l'institution.

8.3 Indicateurs d'abus et de fraudes

8.3.1 Signaux d'alarme

Le processus d'élaboration des indicateurs consiste à examiner comment les abus et les fraudes pourraient être perpétrés et quelles « empreintes » ou « traces » ceux-ci pourraient laisser derrière eux. Lorsqu'une réflexion a lieu pour détecter de potentiels actes abusifs ou frauduleux (Points 7.2., 8.1. et 8.2.), il est utile de considérer les empreintes et traces que l'auteur pourrait laisser derrière lui pour les dissimuler. En effet, il est fort probable qu'un abus ou une fraude laisse des traces non intentionnelles et souvent inévitables. Ces dernières peuvent concerner la transaction, l'auteur ou la méthode de dissimulation de l'abus et de la fraude.

Ces empreintes et traces constituent des signaux d'alarme d'abus et de fraudes auxquels les collaborateurs de l'institution devront être attentifs. Ces signaux d'alarme, qui devront être analysés, peuvent être subdivisés en deux catégories[19] :

Indicateurs liés à l'organisation, tels que :

- Des transactions passées à des heures inhabituelles ;
- Des transactions passées par du personnel non autorisé ;
- Des accès aux locaux à des jours ou à des heures inhabituelles ;
- Une absence de justification et de documentation des écarts dans les réconciliations ;
- Des variations importantes et/ou inexpliquées par rapport à un benchmark ou à une norme ;
- Des valeurs anormales dans le montant ou la nature des opérations ;
- Un nombre important de doublons ou d'annulations de transactions et/ou d'écritures comptables sur une période déterminée ;
- L'utilisation de copies dans la documentation administrative (au lieu d'originaux) ;
- Des ratures et/ou des éléments effacés sur la documentation administrative ;
- Des incohérences dans les processus opérationnels habituels ;
- Un non-respect des procédures d'autorisation habituelles ;
- Etc.

Indicateurs liés aux comportements, tels que :

- Un collaborateur qui ne prend jamais de congés, qui a tendance à venir très tôt au travail et/ou à repartir très tard, bien avant et/ou après ses collègues ;
- Un collaborateur qui s'efforce de tout contrôler, réticent au partage des tâches ;
- Un collaborateur qui traite exclusivement certaines opérations ou certaines relations (assurés, fournisseurs, etc.) ;
- Etc.

Si les collaborateurs de l'institution devront être vigilants vis-à-vis de ces signaux d'alarme, il convient de noter cependant que toute anomalie, comportement ou opération inhabituelle ne signifie pas systématiquement qu'il y a eu un abus ou une fraude. De ce fait, en premier lieu, il s'agira d'analyser ces exceptions, en essayant d'identifier et de comprendre leurs causes et leur origine. En fonction de leur nature et de leur importance, l'explication des écarts devra faire l'objet d'une documentation rigoureuse et d'une revue objective, soit par un manager

[19] Sources :
IIA Australia (2020), *White paper Fraud Risk Indicators*, page 3
IFACI (2017), *Revue internationale des auditeurs et des contrôleurs internes « Audit, risques & contrôle »*, Numéro 9 du 1er trimestre 2017, page 10

opérationnel (1ère ligne de maîtrise), soit par un service de la deuxième ligne de maîtrise (par exemple le service LAF, le contrôle interne, l'assurance qualité).

Ces indicateurs ne devront en aucun cas entraîner un climat de paranoïa ou promouvoir les préjugés, voire des procédés illégaux notamment en matière de protection des données personnelles.

8.3.2 Registre des incidents et registre des plaintes et réclamations

Le registre des incidents survenus au sein de l'institution et le registre des plaintes et réclamations peuvent être une source d'information utile dans la détection de potentiels actes abusifs ou frauduleux existants. Ainsi, l'analyse du registre des incidents peut mettre en lumière des erreurs ou des anomalies répétitives, pouvant être des indicateurs d'abus et de fraudes. Dans le même ordre d'idées, le registre des plaintes et réclamations peut permettre d'identifier des anomalies rapportées par des parties prenantes externes ou tous autres tiers.

En effet, ces registres permettent de recenser (1ère et/ou 2ème ligne de maîtrise) et de centraliser (un autre service de la 2ème ligne de maîtrise) les incidents, les plaintes et les réclamations. En fonction du contexte organisationnel de chaque institution, un registre centralisé respectif sera régulièrement tenu à jour par un acteur de la deuxième ligne de maîtrise alors qu'il est analysé par un autre service de la deuxième ligne de maîtrise.

8.3.3 Dispositif d'alerte - Whistleblowing

La mise en place d'un dispositif d'alerte en cas de soupçons ou d'actes d'abus et de fraudes peut également s'avérer efficace dans la détection et dans la prévention des abus et des fraudes. La mise en place d'un dispositif d'alerte est traitée, de manière plus détaillée, au chapitre 9.

8.4 Surveillance périodique

Les mesures de détection doivent faire l'objet d'une évaluation périodique afin de juger de leur pertinence, de leur implémentation et de leur efficacité. Ces évaluations, qui permettent également de détecter des actes abusifs ou frauduleux, incluent des évaluations objectives par la deuxième ligne de maîtrise, des revues croisées entre pairs, des auto-évaluations et/ou le cas échéant, des missions d'audit interne (Chapitre 11).

Rôles et responsabilités clés

- La première ligne de maîtrise, en concertation avec le service LAF, recense les scénarios d'abus et de fraudes sur base desquels sont déterminés les contrôles détectifs à mettre en place ;
- La première ligne de maîtrise met en œuvre les contrôles détectifs ;
- Le cas échéant, la première ligne de maîtrise et/ou le service LAF collaborent avec le service informatique (ou tout autre service ou personne pertinente comme par exemple un analyste de données) pour la mise en place de contrôles détectifs automatisés ainsi que de techniques analytiques ;
- Les collaborateurs de l'institution sont attentifs aux signaux d'alarme ;
- La première ligne de maîtrise et des acteurs de la deuxième ligne de maîtrise examinent les signaux d'alarme détectés (et documentent l'analyse des exceptions et des écarts) ;
- La première ligne de maîtrise et/ou la deuxième ligne de maîtrise recensent les incidents, les plaintes et les réclamations ;
- Un autre service de la deuxième ligne de maîtrise centralise les incidents, les plaintes et les réclamations dans le registre respectif et les tiennent à jour ;

Pour en savoir plus

- ACFE (2023), *Anti-Fraud Data Analytics Tests,* Anti-Fraud Data Analytics Tests (acfe.com)
- ACFE, Grant Thornton (2020), Anti-fraud playbook – The best defense is a good offense :
  - Play 5 - Use data to uncover fraud
  - Appendix C - Implementation checklists
- ACFE (2017), In-House Fraud Investigation Teams – 2017 Benchmarking Report :
  - Chapter 6 - Software used by fraud investigation teams
- COSO, ACFE (2016), Fraud Risk Management Guide :
  - Chapter 3 - Fraud control activities
  - Appendix I-3 - Fraud control activities scorecard
- ACFE, AICPA, IIA (2008), Managing the Business Risk of Fraud – A Practical Guide :
  - Section 4 - Fraud detection
  - Appendix G - Fraud detection scorecard
- IIA (2021), OECD Global Anti-corruption & Integrity Forum, Webinar on Accountability, Actions and Assurance in Fighting Fraud
- IIA (2009), Global Technology Audit Guide (GTAG) 13 – Fraud Prevention and Detection in an Automated World
- IFACI (2015), Dispositifs de maîtrise des risques de fraude à l'assurance, à la retraite complémentaire et à l'action sociale, Cahier de la Recherche :
  - Partie 2 - Prévenir et détecter la fraude au travers de scénarios
- IFACI (2013), La cartographie des risques, Cahier de la Recherche :
  - Partie 4 - Suivi permanent des risques

9 DISPOSITIF D'ALERTE

9.1 Généralités

Les signalements constituent l'une des méthodes les plus efficaces pour détecter les cas avérés d'abus et de fraudes au sein d'une entité[20]. Dans ce contexte, la mise en place d'un dispositif d'alerte en cas de soupçons ou d'actes d'abus ou de fraudes s'avère être un élément essentiel du dispositif LAF.

Un dispositif d'alerte permet de signaler, de manière orale ou écrite, des informations sur des faits potentiels pouvant sérieusement affecter l'activité de l'institution ou engager gravement sa responsabilité. Il peut s'agir par exemple d'une hotline téléphonique, d'une adresse email générique ou d'une plateforme de signalement en ligne.

La mise en place d'un dispositif d'alerte spécifique à la lutte contre l'abus et la fraude s'inscrit dans le cadre de la Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union (ci-après dénommée la *« Loi »*). Suivant cette Loi, *« les entités juridiques des secteurs privé et public »*[21] sont dans l'obligation d'établir des *« canaux et des procédures pour le signalement interne et leur suivi »*[22]. Ces signalements visent un large périmètre de violations du droit national et européen[23], dont entre autres les abus et les fraudes. Le présent guide se concentre sur le risque d'abus et de fraudes, de sorte qu'il sera référé uniquement à la mise en place d'un dispositif d'alerte dans ce contexte spécifique.

Le présent chapitre vise à exposer les grandes lignes d'un dispositif d'alerte spécifique à la lutte contre l'abus et la fraude afin de permettre aux institutions de faciliter la mise en place d'un tel dispositif.

Cependant, préalablement à l'introduction d'un dispositif d'alerte, la concertation avec le délégué à la protection des données est à prévoir afin d'assurer la conformité du dispositif au Règlement général sur la protection des données.

9.1.1 Devoir de signalement

À l'instar du code de conduite qui impose aux parties prenantes internes de l'institution de signaler un comportement contraire aux valeurs de l'institution, la politique LAF a pour but d'instaurer un devoir de signalement spécifique à la lutte contre l'abus et la fraude. Ainsi, les parties prenantes internes de l'institution sont tenues de signaler tout soupçon raisonnable[24] ou acte d'abus et de fraude au sein de l'institution. Ces signalements peuvent viser d'autres parties prenantes internes, des parties prenantes externes ou tous autres tiers.

9.1.2 Définition et objectifs

Le dispositif d'alerte peut être défini comme un canal ou une procédure permettant aux travailleurs d'une entité et à d'autres personnes qui sont en contact avec cette entité de signaler des informations, y compris des soupçons raisonnables, concernant des violations effectives ou potentielles, qui se sont produites ou sont très susceptibles de se produire en relation avec l'organisation et concernant des tentatives de dissimulation de telles violations.

La mise en place d'un dispositif d'alerte a pour objectifs de faciliter le signalement d'un acte pour lequel il existe des soupçons raisonnables[25] d'abus ou de fraude, de permettre à l'institution de réagir rapidement afin de mitiger les risques et, le cas échéant, de prendre les mesures nécessaires pour y remédier.

[20] ACFE (2020), *Report to the Nations, 2020 Global Study on Occupational Fraud and Abuse. Government Edition*

[21] Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, article 6

[22] Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, article 6

[23] Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, article 3

[24] Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, article 3

[25] Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, article 3

Ainsi, le dispositif d'alerte peut se révéler efficace aussi bien dans la prévention de l'abus et de la fraude, en tant que moyen de dissuasion au passage à l'acte, que dans la détection de l'abus et de la fraude.

9.1.3 Accessibilité

Le dispositif d'alerte doit être accessible à l'ensemble des parties prenantes internes de l'institution mais peut également être ouvert aux parties prenantes externes ou à tous autres tiers. En effet, selon l'Association of Certified Fraud Examiners (ACFE), un tiers des alertes proviendrait d'acteurs externes[26]. Il est donc pertinent pour l'institution de mettre en place des canaux de signalement appropriés leur permettant de rapporter les actes répréhensibles dont ils auraient connaissance. Dans l'hypothèse où l'institution déciderait d'ouvrir le dispositif d'alerte aux acteurs externes à l'institution, il sera possible de prévoir des canaux de signalement différents pour ces derniers (Point 9.2.2.).

9.1.4 Communication et sensibilisation

La mise en place d'un dispositif d'alerte nécessitera une communication adéquate auprès de l'ensemble des parties prenantes et de tous autres tiers de l'institution. Cette communication permettra de les sensibiliser (Points 7.1. et 7.4.) au devoir de signalement qui leur incombe en cas de détection ou de soupçon d'abus ou de fraudes.

En effet, de nombreux cas d'abus et de fraudes sont connus ou suspectés par le personnel d'une entité et le défi pour celle-ci est d'encourager les collaborateurs à s'exprimer dans leur propre intérêt. La loyauté envers des collègues ou la famille, le désintérêt, l'admiration envers l'auteur potentiel d'un abus ou d'une fraude, la peur des conséquences ou bien encore des soupçons plutôt que des preuves concrètes, sont les raisons les plus courantes pour lesquelles un potentiel *« lanceur d'alerte »*[27] s'abstient d'effectuer un signalement[28].

Enfin, les parties prenantes internes devront être sensibilisées à la nécessaire séparation des rôles et des responsabilités dans le processus de signalement. Ainsi, s'il appartient aux parties prenantes internes de signaler de bonne foi et au plus vite tout soupçon raisonnable, elles ne devront pas se lancer de leur propre initiative dans des enquêtes avant (ni même après) avoir effectué un signalement. En effet, les compétences en matière de lutte contre l'abus et la fraude ne s'improvisent pas et un retard dans le signalement pourrait engendrer un risque considérable pour l'institution. D'une part, l'auteur de l'abus ou de la fraude pourrait poursuivre même intensifier ses activités sans être démasqué, et d'autre part, si ce dernier s'aperçoit qu'il a éveillé les soupçons de ses collègues, il pourrait tenter de dissimuler ses actes ou même de détruire les traces et preuves de sa culpabilité[29]. La Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union indique à ce sujet qu'il est *« essentiel que les informations pertinentes parviennent rapidement à ceux qui sont les plus proches de la source du problème, les plus aptes à enquêter et qui disposent des pouvoirs nécessaires pour y remédier, si possible »*[30].

9.2 Procédure et modalités de signalement

9.2.1 Procédures et processus de signalement

Au regard de son contexte organisationnel, l'institution devra établir des procédures internes appropriées pour notamment le signalement des faits, la réception, l'analyse de la recevabilité, le traitement, la documentation, le suivi et l'archivage des signalements (Chapitre 10).

Dans ce contexte, le processus de signalement devra être précisément documenté dans une procédure et communiqué aux parties prenantes de l'institution. La documentation devra porter notamment sur le périmètre et l'accessibilité du dispositif, les étapes du processus de signalement, les personnes ou les services auxquels signaler les faits, les modalités selon lesquelles les alertes seront adressées et traitées (par exemple les canaux de signalement à utiliser, le formalisme à respecter par le lanceur d'alerte et l'institution, l'anonymisation et l'archivage

[26] ACFE (2020), *Report to the Nations, 2020 Global Study on Occupational Fraud and Abuse. Government Edition*

[27] Les mots « lanceur d'alerte » et « auteur du signalement » sont des synonymes

[28] CGMA (2012), *Report Fraud risk management - A guide to good practice*

[29] IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*

[30] Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, page 25

des signalements), les mesures de protection et de confidentialité (Point 9.3.) ainsi que les sanctions éventuelles en cas de tentative de dissuasion, d'entrave au devoir de signalement ou de signalement abusif.

Par ailleurs, la Loi précise, dans son article 7, les éléments que les entités devront impérativement inclure dans leurs procédures de signalement interne et de suivi[31].

L'annexe 10 fournit des extraits d'exemples de procédures et de processus de signalement.

9.2.2 Canaux de signalement

Un signalement peut être effectué via un canal interne ou externe (par exemple une hotline téléphonique, une adresse mail générique ou une plateforme de signalement en ligne interne ou externe (Annexe 11)). Néanmoins, la Loi impose aux *« entités juridiques des secteurs privé et public »*[32] d'établir *« des canaux et des procédures pour le signalement interne et leur suivi »*[33]. Elle précise que ces canaux doivent permettre *« d'effectuer des signalements par écrit ou oralement ou les deux dans une des trois langues administratives (…). Il est possible d'effectuer des signalements oralement par téléphone ou via d'autres systèmes de messagerie vocale et, sur demande de l'auteur de signalement, par le biais d'une rencontre en personne dans un délai raisonnable »* [34].

De plus, tout comme pour les signalements de faits contraires au code de conduite, les parties prenantes internes devront toujours disposer et être informées de la possibilité de signaler directement des soupçons ou actes d'abus et de fraudes à leur(s) supérieur(s) hiérarchique(s) et/ou à *« une personne ou service impartial compétent pour assurer le suivi des signalements »*[35].

En cas d'utilisation d'une hotline téléphonique interne (ouverte à toutes les parties prenantes), la réception de l'alerte pourra se faire par une personne ou un service désigné(e), qui la redirigera ensuite vers la personne et/ou le service désigné(e) comme responsable du suivi et du traitement (Chapitre 10). Il en va de même lorsqu'un collaborateur de l'institution privilégie le fait d'en référer directement à son supérieur hiérarchique. Ce dernier se chargera alors de transmettre le signalement au responsable concerné pour suivi et traitement.

Chaque institution peut également opter pour l'externalisation de la réception des signalements. Dans ce contexte, quel que soit le choix de l'institution, la Loi précise entre autres que les canaux pour la réception des signalements internes doivent être *« conçus, établis et gérés d'une manière sécurisée »*[36] afin de garantir *« la confidentialité de l'auteur de signalement et de tout tiers mentionné dans le signalement (…) »*[37] (Point 9.3.).

Ainsi, il appartiendra à chaque institution de concevoir les canaux de signalement qui lui sembleront les plus adaptés à sa culture et à sa structure organisationnelle.

9.2.3 Contenu et documentation

Il appartient à l'institution d'établir une procédure de signalement pour définir entre autres les informations à transmettre dans le cadre d'un signalement afin de garantir sa recevabilité. Dans ce contexte, un modèle-type de fiche de signalement pourra être élaboré par l'institution, de sorte à ce que les lanceurs d'alerte soient guidés dans l'information qu'ils transmettent et que le signalement soit considéré comme recevable. La mise en place d'un dispositif d'alerte multilingue encourage et facilite la décision de donner l'alerte[38].

---

[31] Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, article 7

[32] Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, article 6

[33] Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, article 6

[34] Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, article 7

[35] Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, article 7

[36] Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, article 7

[37] Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, article 7

[38] ACFE, AICPA, IIA (2008), *Managing the Business Risk of Fraud: A Practical Guide*

En outre, il sera également demandé aux lanceurs d'alerte et à l'institution de respecter un certain formalisme lors d'un signalement.

En particulier, les lanceurs d'alerte devront :

- Indiquer l'identité et les fonctions de la personne visée par un signalement ;
- Décrire de manière détaillée les faits signalés ;
- Fournir toutes informations ou documents (courriers, emails, rapports comptables, etc.) à l'origine de l'acte ou du soupçon.

La Loi précise les éléments que les entités devront inclure dans leurs procédures de signalement interne et de suivi[39] et indique entre autres que les entités devront (si le signalement n'est pas anonyme) :

- Adresser un accusé de réception *« à l'auteur du signalement dans un délai de 7 jours à compter de la réception du signalement* »[40] et
- Fournir un retour d'informations dans « *un délai raisonnable (…), n'excédant pas trois mois à compter de l'accusé de réception du signalement ou, à défaut d'accusé de réception envoyé à l'auteur du signalement, trois mois à compter de l'expiration de la période de sept jours suivant le signalement* » [41] sur les suites du signalement.

Aucune alerte ne devra être laissée sans réponse au risque de décourager les lanceurs d'alerte à signaler d'autres soupçons ou actes éventuels et, de manière plus générale, de discréditer le dispositif LAF.

9.2.4 Anonymisation des signalements

La Loi indique que les entités juridiques des secteurs privé et public acceptent les signalements anonymes et en assurent le suivi[42].

Les organismes internationaux tels que l'Association of Certified Fraud Examiners, l'American Institute of Certified Accountants (AICPA) et l'Institut des auditeurs internes considèrent que le fait de garantir l'anonymat aux lanceurs d'alerte est un élément crucial pour encourager le signalement d'un soupçon de fraude[43].

Toutefois, le risque d'accusations malicieuses et/ou d'abus et de délations en cas de signalement anonyme ne doit pas être sous-estimé, de sorte qu'il soit nécessaire d'indiquer dans la procédure de signalement que les signalements anonymes seront traités avec grande prudence. De plus, les signalements anonymes seront plus difficiles à traiter par l'institution et le lanceur d'alerte ne pourra pas bénéficier d'un réel suivi sur le signalement qu'il a fait.

De même, la Commission nationale pour la protection des données (CNPD), bien que consciente de la nécessité d'autoriser les signalements anonymes afin de ne pas passer à côté d'alertes provenant de personnes n'étant pas disposées à révéler leur identité, estime que ces cas de figure devraient rester exceptionnels[44]. La CNPD énonce dans le même document un ensemble de difficultés liées aux signalements anonymes, à savoir :

- Le traitement du signalement est compliqué par l'impossibilité de poser des questions complémentaires au lanceur d'alerte ;
- La protection du lanceur d'alerte (Point 9.3.2.) est difficile en cas d'identité non révélée ;
- Le lanceur d'alerte qui souhaite à tout prix rester anonyme pourrait être accusé à tort de délation ;

[39] Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, article 7

[40] Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, article 7

[41] Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, article 7

[42] Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, article 4

[43] ACFE, AICPA, IIA (2008), *Managing the Business Risk of Fraud: A Practical Guide*, page 35

[44] CNPD Groupe de travail « ARTICLE 29 » sur la protection des données (2006), *Avis 1/2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière*

- Le contexte pourrait encourager les signalements malveillants et malintentionnés ;
- Un climat d'anxiété pourrait se développer au sein de l'organisation - les collaborateurs pourraient avoir peur d'être accusés à tout moment par un lanceur d'alerte anonyme.

Par conséquent, la CNPD recommande de concevoir les dispositifs d'alerte de manière à *« ne pas encourager la perception des signalements anonymes comme étant la règle habituelle »*[45] et, le cas échéant, à traiter les signalements anonymes avec une *« précaution particulière »* [46].

9.3 Protection, confidentialité et indépendance du traitement

9.3.1 Protection des données

Que le signalement soit fait via un canal interne ou externe, la Loi prévoit un devoir de confidentialité aux entités des secteurs privé et public. Ainsi, elle impose la protection de l'identité de l'auteur du signalement en interdisant sa divulgation *« sans son consentement exprès (…) à toute personne autre que les membres du personnel autorisés compétents pour recevoir des signalements ou pour en assurer le suivi »*[47] .

La CNPD indique également que pour encourager l'utilisation du dispositif d'alerte, il est essentiel que la confidentialité de l'identité du lanceur d'alerte et de son signalement soit assurée[48]. Toutes les informations transmises par le lanceur d'alerte devront faire l'objet d'un traitement strictement confidentiel. Le respect de la confidentialité des données permettra à l'institution de prévenir d'éventuelles fuites d'informations et de garder le contrôle de la communication (Chapitre 12).

En pratique, lors d'un signalement, l'institution devra veiller à ce que tout traitement de données à caractère personnel soit effectué dans le respect du Règlement général sur la protection des données.

Par ailleurs, la Directive (UE) 2019/1937 indique que « *les signalements ne sont pas conservés plus longtemps qu'il n'est nécessaire et proportionné de le faire pour respecter les exigences imposées par la présente directive ou d'autres exigences imposées par le droit de l'Union ou le droit national* »[49].

9.3.2 Protection des lanceurs d'alerte

Les signalements recueillis par l'institution doivent être analysés dans un cadre strictement confidentiel et sécurisé afin de garantir la confidentialité de l'identité des lanceurs d'alerte et leur assurer une protection efficace contre les représailles. La Loi a pour objectif d'encadrer juridiquement la protection des lanceurs d'alerte en assurant à ces derniers un cadre sécuritaire et de confiance facilitant davantage le signalement d'actes répréhensibles. Ainsi, la protection des lanceurs d'alerte doit être une préoccupation fondamentale pour l'institution. Que le mode de signalement choisi garantisse ou non l'anonymat, l'institution devra protéger les lanceurs d'alerte contre tout type de représailles et ce, même si les faits rapportés se révèlent inexacts ou ne donnent lieu à aucune suite.

L'institution devra en effet appliquer le principe de tolérance zéro face à tout acte ou menace de représailles à l'encontre d'un lanceur d'alerte, qu'il porte atteinte par exemple à l'accès à la formation, à la rémunération, aux perspectives de carrière, à la répartition des tâches au quotidien ou au bien-être au travail en général. La protection des lanceurs d'alerte contre des représailles est d'autant plus importante que la confidentialité n'élimine pas entièrement le risque que l'identité du lanceur d'alerte soit découverte ou devinée. Il appartiendra donc à

[45] CNPD Groupe de travail « ARTICLE 29 » sur la protection des données (2006), *Avis 1/2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière*, page 12

[46] CNPD Groupe de travail « ARTICLE 29 » sur la protection des données (2006), *Avis 1/2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière*, page 12

[47] Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, article 22

[48] CNPD Groupe de travail « ARTICLE 29 » sur la protection des données (2006), *Avis 1/2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière*

[49] Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, article 18

l'institution de monitorer l'apparition d'éventuels signaux de représailles en se tenant informée auprès du lanceur d'alerte[50].

Enfin, la CNPD recommande d'informer les collaborateurs de l'entité qu'en cas de soupçon signalé mais non avéré, ils ne pourront pas être sanctionnés tant qu'ils ont été de bonne foi. Par contre, l'utilisation abusive du dispositif d'alerte entraîne des sanctions ou des poursuites[51].

9.3.3 Protection des personnes visées par une alerte

L'institution devra mettre en place des mesures de protection pour les personnes visées par une alerte, de manière à leur garantir entre autres le respect de la présomption d'innocence, le droit à un recours effectif et à un procès équitable, les droits de la défense, y compris le droit d'être entendu, le droit d'accéder à leur dossier et la protection de leur vie privée.

La CNPD souligne que les dispositifs d'alerte *« font courir un risque très grave de stigmatisation et de victimisation »*[52] aux personnes mises en cause lors d'un signalement. En particulier, ces dernières devront être informées rapidement de la collecte et du traitement des données personnelles les concernant et disposeront de droits d'accès, de rectification et d'effacement par rapport à ces données en cas d'erreurs ou d'absence de mise à jour dans leurs données. La CNPD précise néanmoins que s'il existe un risque sérieux de destruction des preuves, la notification aux personnes mises en cause de la collecte de données les concernant pourra être retardée[53].

Ainsi, l'institution devra mettre en place un dispositif permettant de respecter les droits des personnes visées par une alerte et de garantir la confidentialité de leurs données, afin de protéger leur image et leur réputation dans l'hypothèse où elles seraient indûment soupçonnées d'abus ou de fraude ou victimes d'accusations calomnieuses[54].

9.3.4 Indépendance du traitement

Le choix des personnes ou services désigné(e)s comme responsables de la réception et du suivi des signalements doit permettre d'assurer l'indépendance du traitement des signalements et l'absence de conflits d'intérêts. En fonction des canaux de signalement choisis, l'institution devra désigner le ou les service(s) responsable(s) disposant d'un degré d'indépendance suffisant, soumis aux exigences de confidentialité, et rapportant à l'organe de gouvernance.

En cas de dispositif d'alerte interne :

- Plusieurs personnes (mais en nombre limité) devraient être habilitées à réceptionner et traiter les signalements ;
- Ces personnes devraient disposer des compétences adéquates et seront soumises aux exigences en termes de confidentialité.

[50] ACFE, AICPA, IIA (2008), *Managing the Business Risk of Fraud: A Practical Guide*

[51] CNPD Groupe de travail « ARTICLE 29 » sur la protection des données (2006), *Avis 1/2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière*

[52] CNPD Groupe de travail « ARTICLE 29 » sur la protection des données (2006*), Avis 1/2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière*, page 7

[53] CNPD Groupe de travail « ARTICLE 29 » sur la protection des données (2006*), Avis 1/2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière*

[54] IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*

Rôles et responsabilités clés

- Les parties prenantes internes sont conscientes du devoir de signalement qui leur incombe et, le cas échéant, signalent de bonne foi et au plus vite tout acte et/ou soupçon raisonnable d'abus ou de fraudes ;
- Le service LAF, en concertation avec le délégué à la protection des données, met à disposition des parties prenantes internes et/ou des parties prenantes externes ou tous autres tiers, un dispositif d'alerte conforme aux exigences du Règlement général sur la protection des données ;
- Le service LAF s'assure de la communication et de la sensibilisation autour du dispositif d'alerte ;
- Le service LAF rédige des procédures internes pour le signalement des faits, la réception, l'analyse de la recevabilité, le traitement, de documentation, le suivi et l'archivage des signalements ;
- Une personne ou un service désigné(e) (ou un prestataire externe, si l'institution a fait le choix de l'externalisation), réceptionne les signalements, puis les redirige vers la personne et/ou le service désigné(e) comme responsable du suivi et du traitement (Point 10.3.1.) ;
- Le service LAF s'assure que la protection et la confidentialité des données des lanceurs d'alerte et des personnes visées par une alerte soient garanties en toutes circonstances (Point 10.2.).

Pour en savoir plus

- Directive 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union
- Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union :
  - Chapitre 2 - Des signalements internes
  - Chapitre 3 - Office des signalements
  - Chapitre 4 - Des signalements externes et suivi
  - Chapitre 5 - Dispositions applicables aux signalements internes et externes
  - Chapitre 6 - Divulgations publiques
  - Chapitre 7 - Mesures de protection
- Loi du 17 août 2018 sur l'archivage
- Ministère de la Justice (2023) *Lanceurs d'alerte*, https://mj.gouvernement.lu/fr/dossiers/2023/lanceurs-d-alerte.html
- ACFE, IIA (2023), Building a best-in-class whistleblower hotline program
- ACFE (2020), Report to the Nations, 2020 Global Study on Occupational Fraud and Abuse. Government Edition
- ACFE, Grant Thornton (2020), Anti-fraud playbook – The best defense is a good offense :
  - Play 7 - Lay the groundwork for investigations
  - Appendix C - Implementation checklists
- ACFE, AICPA, IIA (2008), Managing the Business Risk of Fraud - A Practical Guide :
  - Section 4 - Fraud Detection
- CGMA (2012), Report Fraud risk management - A guide to good practice :
  - Appendix 8 - Roles and responsibilities : Chart 1 – Reporting fraud

10 TRAITEMENT ET INVESTIGATION D'UN SOUPÇON D'ABUS OU DE FRAUDES

Lorsqu'un signalement est jugé recevable, les soupçons d'abus et de fraudes internes et externes sont traités selon un cheminement et une procédure précise. Le traitement correspond au processus d'analyse et de résolution d'un soupçon d'abus ou de fraudes, allant de la réception du signalement jusqu'à la clôture du dossier. Le traitement des soupçons a pour but d'apporter une réponse adéquate et proportionnée aux soupçons signalés et, le cas échéant, de protéger rapidement les intérêts de l'institution. En ce sens, l'investigation n'est qu'une étape à part entière du traitement et n'est pas systématiquement requise. Dans la suite du guide, le service LAF est considéré comme le service en charge du traitement des soupçons d'abus et de fraudes.

10.1 Prérequis pour mener une investigation

10.1.1 Procédure de traitement et d'investigation d'un soupçon d'abus et de fraudes

Pour répondre efficacement et en temps voulu à un soupçon d'abus ou de fraudes, l'institution doit se doter au préalable d'une procédure de traitement et d'investigation des soupçons d'abus et de fraudes. Cette procédure décrit les actions à mener par l'institution lorsqu'un soupçon émerge afin qu'une réponse appropriée puisse être fournie. De plus, disposer d'une telle procédure permet de garantir une certaine cohérence et harmonisation dans le traitement des signalements.

L'investigation, lorsqu'elle s'avère nécessaire, est une étape majeure du traitement d'un soupçon d'abus et de fraudes. Elle a pour objectif de collecter des informations orales ou écrites afin de reconstituer les faits et leur chronologie, de déterminer les responsabilités et de mesurer les impacts éventuels[55].

Ainsi, la procédure de traitement et d'investigation à établir par l'institution, détaille les étapes à suivre et définit les modalités de documentation et de gestion de l'information au cours du processus de traitement d'un soupçon d'abus et de fraudes qui permettront d'orienter la prise de décision. En effet, une méthodologie cohérente et formelle permet de gérer les risques et de réduire les pertes éventuelles[56].

Une procédure de traitement et d'investigation doit contenir entre autres les informations suivantes :

- La définition des principales phases constituant le traitement d'un signalement ;
- La définition des rôles et responsabilités aux différentes phases du traitement d'un signalement ;
- Les flux de remontées d'informations à chaque phase du traitement. Les modalités de reporting auprès de l'organe de gouvernance dépendront de ses attentes, ainsi que de la gravité des allégations. En fonction de la criticité des risques, le président peut effectuer un suivi rapproché conformément aux modalités définies au préalable. Des seuils de matérialité peuvent notamment être définis à cet effet (par exemple le président est informé de chaque étape du traitement si les enjeux financiers dépassent un montant défini) ;
- Les délais de remontée des informations ;
- Les dispositions légales et règlementaires qui encadrent le traitement du signalement (confidentialité, protection des lanceurs d'alertes, protection de la réputation des suspects, etc.) ;
- La définition des étapes de l'investigation si elle a lieu d'être ;
- Les modalités de documentation et de gestion de l'information au cours du processus de traitement et de l'investigation ;
- Les modalités de gestion de la communication interne et externe tout au long du traitement ;
- Les cas selon lesquels la mise en place d'une cellule de gestion de crise sera nécessaire, son organisation et les modalités de saisie ;
- Les procédures en cas de litige et les sanctions applicables en cas d'abus ou de fraude avéré(e).

Tandis que la politique LAF a vocation à être diffusée auprès de l'ensemble des parties prenantes internes dans un objectif de sensibilisation, la procédure de traitement et d'investigation devra être distribuée uniquement aux

[55] ACFE (2022), *ACFE Fraud Examiners Manual, Chapter Planning and conducting a fraud examination*
[56] ACFE, AICPA, IIA (2008), *Managing the Business Risk of Fraud: A Practical Guide*

personnes concernées, notamment à celles qui feront partie de l'équipe chargée de l'investigation et le cas échéant, de la cellule de gestion de crise. Par ailleurs, la politique LAF doit préciser qu'il sera attendu de l'ensemble des parties prenantes internes qu'elles fournissent toutes les données ou informations utiles demandées par le service LAF, l'équipe chargée de l'investigation ou par la cellule de gestion de crise lors du traitement d'un soupçon d'abus ou de fraudes. En effet, l'équipe chargée de l'investigation doit disposer d'un accès libre et rapide à toutes les informations nécessaires à la réalisation de ses enquêtes.

Avant de lancer une investigation, il sera nécessaire de connaître le cadre légal et règlementaire, à savoir les juridictions compétentes et la législation applicable (par exemple le droit pénal, le droit du travail, le Code administratif de la fonction publique).

10.1.2 Cellule de gestion de crise

Il est opportun de disposer d'une cellule de gestion de crise préalablement définie et pouvant être mobilisée rapidement pour gérer la crise associée au soupçon d'abus ou de fraudes signalé. La cellule de gestion de crise n'est mobilisée que dans des situations exceptionnelles, lorsque les soupçons signalés sont considérés comme alarmants et leurs conséquences potentielles (par exemple financières et réputationnelles) comme graves. Disposer d'une cellule de gestion de crise permet également de capitaliser sur l'expérience acquise lors de gestion de crises précédentes pour mieux réagir face à un soupçon et de prendre les bonnes décisions.

Les modalités de saisie de la cellule de gestion de crise doivent être prévues dans la procédure de traitement et d'investigation, qui précisera notamment :

- Par qui la cellule de gestion de crise pourra être saisie - Le service LAF propose au président de saisir la cellule de gestion de crise lorsque le cas à traiter le justifie. Le président dispose de la prérogative pour décider de mobiliser ou non la cellule de gestion de crise ;
- Les seuils de matérialité à partir desquels la cellule de gestion de crise sera saisie - La cellule de gestion de crise est saisie lorsque les conséquences financières associées aux soupçons dépassent un certain montant ou engendrent des conséquences réputationnelles graves ;
- À quelle phase du traitement la cellule de gestion de crise pourra être saisie - Le service LAF propose de saisir la cellule de gestion de crise à la fin de la phase de pré-investigation, lorsque les éléments rassemblés attestent de la gravité des allégations. Cependant, cela peut être fait à toute autre phase du traitement, dès que le service LAF soupçonne une situation grave.

Lorsqu'elle est mobilisée, la cellule de gestion de crise devient le garant de la confidentialité des informations et est chargée de[57] :

- Garder le contrôle et la maîtrise sur la communication interne et externe ;
- Assurer le bon déroulement des procédures légales et/ou disciplinaires ;
- Assurer la remontée des informations à chaque étape de l'investigation ;
- Solliciter les intervenants externes en fonction des besoins de l'investigation.

Il est à noter que si la cellule de gestion de crise n'est pas mobilisée, c'est le service LAF qui détient les prérogatives énumérées et qui est le garant de la confidentialité des informations.

La composition de la cellule de gestion de crise dépendra notamment de la taille de l'institution, de ses activités et des risques identifiés. Généralement, cet organe se compose du président, du responsable du service LAF, des collaborateurs du service juridique, du contrôle interne et/ou de l'audit interne si existant. D'autres services tels que le service ressources humaines, le service informatique/de la sécurité de l'information, le service communication ou des départements et/ou services opérationnels (*« cœur de métier »* et *« support »*) pourront être représentés soit de manière permanente, soit de manière ponctuelle en fonction des besoins de l'investigation. De par sa composition, la cellule de gestion de crise dispose d'un niveau d'autorité élevé pour réagir rapidement et adéquatement en cas de crise[58].

[57] IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*, pages 37 et 38
[58] IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*

Selon les cas, des experts externes (par exemple des experts en investigation de la fraude ou des avocats) pourront également être mandatés afin de soutenir les activités de la cellule de gestion de crise. Leur niveau d'implication et leurs rôles au sein de l'investigation devront être clairement définis et justifiés.

Toutes les personnes faisant partie de la cellule de gestion de crise doivent être désignées et informées de leurs rôles et responsabilités avant le lancement d'une enquête approfondie.

10.1.3 Base de données sur les cas d'abus et de fraudes traités précédemment

La mise en place d'une base de données sur les cas d'abus et de fraudes, qui recense et documente les cas précédemment traités, peut grandement faciliter le traitement des soupçons d'abus ou de fraudes. En effet, les descriptifs des procédés et mécanismes abusifs et frauduleux, les défaillances du dispositif de gestion des risques et de contrôle interne éventuellement détectées, les mesures correctives prises, les sanctions infligées ainsi que les jugements rendus antérieurement, peuvent orienter le traitement et la prise de décision. En ce sens, la base de données sur les cas d'abus et de fraudes peut constituer un *« benchmark »* pour le traitement des nouveaux signalements et soupçons[59]. Cette base de données sur les cas précédemment traités ne contient aucune donnée personnelle, dans la mesure où elle n'a vocation qu'à recenser les scénarios d'abus et de fraudes et de capitaliser sur l'expérience dans leur traitement. Son objectif n'est pas de tenir un registre des personnes mises en cause (Annexe 12).

Au sein de l'institution, il incomberait au service LAF (deuxième ligne de maîtrise) d'alimenter et de tenir à jour cette base de données.

10.2 Principes régissant la conduite des investigations

10.2.1 Confidentialité

L'équipe chargée de l'investigation veille à traiter les informations et les données qui lui sont confiées dans la réalisation de ses missions, dans la plus stricte confidentialité. L'ensemble des ressources mobilisées au cours de l'enquête, la cellule de gestion de crise y incluse, doit signer une clause de confidentialité. De plus, l'identité des personnes ayant collaboré à l'enquête sera gardée secrète et leur protection contre toute forme de représailles sera assurée. L'équipe d'investigation veillera à traiter les données collectées dans le respect du Règlement général sur la protection des données.

La préservation de la confidentialité tout au long de l'enquête est cruciale pour que l'institution garde la main sur d'éventuelles fuites d'informations mais également pour respecter le droit à la présomption d'innocence des suspects et préserver leur réputation dans l'hypothèse où leur culpabilité s'avèrerait non démontrée[60] (Chapitre 9).

10.2.2 Protection des informations

Des mécanismes nécessaires pour prévenir tout vol, altération ou destruction d'informations en rapport avec l'incident faisant l'objet de l'enquête doivent être instaurés. La protection de l'intégrité des informations a pour objectif de s'assurer que les données nécessaires à l'investigation, une fois identifiées, puissent être collectées sans subir d'altération ou de destruction volontaire. Ainsi, la protection des informations permet de réduire le risque que les suspects tentent de dissimuler les preuves de leurs actes et ainsi compliquer, même faire échouer l'enquête. Pour assurer la préservation des informations et éviter tout risque de corruption des données, l'équipe d'investigation s'engage à garantir la sécurisation des processus de partage, de transmission et de sauvegarde des informations[61]. Elle prend également des mesures appropriées pour que les informations et données ne soient divulguées qu'aux membres de l'équipe d'investigation ou aux personnes dûment autorisées à en être informées.

À cet effet, un environnement informatique spécifique peut être créé afin d'y stocker toutes les données nécessaires à la conduite de l'investigation et à l'établissement de la preuve d'abus ou de fraude. Ces données peuvent être des emails, des conversations (*« chats »*), des données présentes sur les serveurs de l'institution ou des documents papiers scannés. Cet environnement, auquel seule l'équipe d'investigation a accès, fera l'objet de contrôles réguliers visant à vérifier l'intégrité des données et à prouver l'authenticité des pièces.

[59] IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*
[60] IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*
[61] CGMA (2012), *Report Fraud risk management - A guide to good practice*

Si les besoins de l'enquête le justifient, le suspect pourra entre autres être suspendu de l'exercice de ses fonctions, dans le respect du Code administratif de la fonction publique et/ou du droit du travail applicable. Cela sera notamment le cas lorsqu'il existe un risque réel et important que le suspect manipule des données, qu'il exerce une pression sur d'éventuels témoins ou qu'il cède à toute forme d'influence qui pourrait venir entraver le bon déroulement de l'investigation.

10.2.3 Impartialité et objectivité

L'équipe chargée de l'enquête mène ses investigations de manière indépendante et ne devra agir ni sous la direction ni sous la pression exercée par un (chef de) département, un (chef de) service ou l'organe de gouvernance de l'institution. Chaque cas sera investigué en toute impartialité et objectivité, sans laisser place aux opinions personnelles ou aux jugements de valeurs. Les principes d'égalité de traitement, de droit à l'erreur et de présomption d'innocence pour les suspects devront être respectés tout au long de l'enquête.

10.3 Processus de traitement d'un soupçon d'abus et de fraudes

10.3.1 Phase de signalement

Comme détaillé au chapitre 9, quelle que soit la source de la remontée d'un soupçon d'abus ou de fraudes internes ou externes – via une hotline téléphonique, une plateforme de signalement en ligne ou une adresse email générique, via un signalement direct à une personne ou un service désigné(e), via les activités de contrôle et de monitoring, etc. – l'institution doit disposer d'une procédure interne documentant les différentes phases du processus de traitement d'un soupçon d'abus et de fraudes.

Lors de la phase de signalement, une personne ou un service désigné(e) (ou un prestataire externe, si l'institution a fait le choix de l'externalisation) réceptionne le signalement, puis le redirige vers le service LAF, qui évaluera alors sa recevabilité.

Chaque institution définira ses propres critères de recevabilité.

Si le signalement est jugé recevable, le service LAF décide, conformément à la procédure de traitement et d'investigation d'un soupçon d'abus et de fraudes, de lancer la phase de découverte.

10.3.2 Phase de découverte

La procédure (Point 10.1.1.) précise également les premières informations à collecter par le service LAF lors de la phase de découverte. En principe, il s'agit d'informations sur la provenance du signalement, la nature des faits ainsi que l'identité et les fonctions du ou des suspects. Sur base des informations à sa disposition, le service LAF consulte d'autres services (par exemple le service ressources humaines, le service juridique)[62] pour juger de la fiabilité et de la pertinence des faits signalés. Si le signalement n'est pas anonyme, il peut à ce stade déjà être opportun de s'entretenir avec le lanceur d'alerte afin de récolter des informations supplémentaires.

La phase de découverte est clôturée par une succincte première identification et évaluation des risques potentiels et réels compte tenu des informations collectées. Si la criticité des risques réels ou potentiels le justifie, le service LAF consulte, sans délais, le président et/ou l'organe de gouvernance, qui décident des mesures d'urgence devant s'imposer (par exemple en matière de préservation des données et de communication (Chapitre 12)). A défaut, le service LAF peut décider soit de clôturer le dossier, soit de lancer une pré-investigation.

10.3.3 Phase de pré-investigation

La phase de pré-investigation vise à analyser et à compléter les informations collectées lors de la phase de découverte pour pouvoir, par la suite, évaluer la consistance et l'envergure du soupçon d'abus et de fraudes. Cette phase est menée par le service LAF ou par l'équipe chargée de l'investigation et consiste, selon l'IFACI[63] à documenter formellement les informations suivantes :

- Les faits retenus ;

[62] ACFE, AICPA, IIA (2008), *Managing the Business Risk of Fraud: A Practical Guide*
[63] IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*, page 45

- Les risques identifiés ainsi que leur probabilité de survenance et leurs impacts ;
- Les mécanismes et scénarios utilisés par le ou les potentiels auteurs d'abus ou de fraudes pour perpétrer ses/leurs actes ;
- L'identité du ou des potentiels auteurs d'abus ou de fraudes ainsi que de complices potentiels internes ou externes à l'organisation ;
- L'identité des témoins, au sein de l'organisation ou en dehors ;
- Les éventuelles incompréhensions de certains faits et motifs (« *zones d'ombre* »).

Ces informations peuvent être documentées de manière schématique, au moyen de tableaux ou fiches de synthèse (Annexe 13), voire de logigrammes représentant le scénario d'abus ou de fraudes. Ces supports sont actualisés au fil de la collecte des informations nécessaires à la pré-investigation.

Lorsque suffisamment d'informations factuelles ont été rassemblées et documentées afin d'apprécier le bien-fondé, la consistance et l'envergure du soupçon, le service LAF formule ses conclusions et ses propositions sur la phase de pré-investigation. En fonction de la gravité du soupçon et conformément aux modalités de remontée des informations définies dans la procédure de traitement et d'investigation :

- Un document formalisé est présenté au président et/ou à l'organe de gouvernance. Le service LAF peut proposer au président de saisir et de mobiliser d'urgence la cellule de gestion de crise et/ou de mettre en place des plans d'actions et/ou de lancer la phase d'investigation ;
- Le service LAF peut lancer la phase d'investigation sans passer nécessairement par le président et/ou l'organe de gouvernance.

10.3.4 Phase d'investigation

10.3.4.1 Objectifs et techniques analytiques de l'investigation

Les principaux objectifs de l'investigation sont les suivants[64] :

- Identifier le ou les auteurs d'abus ou de fraudes et les mécanismes et scénarios qu'ils ont mis en place ;
- Rassembler les éléments factuels permettant de prouver l'existence de l'abus ou de la fraude ;
- Identifier les faiblesses dans le dispositif de gestion des risques et de contrôle interne y compris dans les procédures internes ainsi que les systèmes d'information impactés afin de mettre en place des contrôles appropriés et/ou des mesures correctives ;
- Estimer l'ampleur du préjudice (par exemple financier et/ou réputationnel) subi par l'institution, le cas échéant en déterminant si le scénario d'abus ou de fraudes a été utilisé par d'autres fraudeurs au sein ou en dehors de l'institution ;
- Si possible, recouvrer les fonds perdus.

Afin de récolter un maximum de preuves et de mettre en évidence les actes abusifs ou frauduleux, l'enquête peut se concentrer sur[65] :

- Une analyse des processus opérationnels concernés et des contrôles mis en place ou manquants. A titre d'exemple, l'enquête peut se concentrer sur les modalités de séparation des tâches, sur les processus d'autorisation et de validation des paiements, sur les droits d'accès à certains systèmes d'information ou bases de données ;
- Des recherches documentaires (des factures, extraits de comptes, bons de livraison, documentation de procédures, emails, communications avec des tiers, relevés des heures pointées, etc.) ;

[64] IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*, page 51

[65] Sources :
ACFE, AICPA, IIA (2008), *Managing the Business Risk of Fraud: A Practical Guide*
IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*

- Des outils technologiques tels que le *data mining* pour une analyse des preuves à disposition, le *computer forensics* pour recouvrer des historiques ou des données effacé(e)s ou encore d'autres plateformes pour effectuer des recherches sur un grand nombre de données non structurées ;
- Une analyse plus approfondie sur les suspects (expérience professionnelle, attitude au bureau, ressenti des collègues, etc.) ;
- Des entretiens avec les lanceurs d'alerte, les collaborateurs (supérieurs hiérarchiques ou collègues) ou des acteurs externes (fournisseurs, assurés, autres tiers, etc.) afin de mieux comprendre ou appréhender la situation. Chaque entretien doit être soigneusement préparé et planifié et la chronologie doit être minutieusement pensée ;
- Si le risque est bien maîtrisé, des entretiens avec le suspect, afin de déterminer les raisons du passage à l'acte et d'identifier les facteurs déclenchants (Chapitre 4).

Ces activités sont menées dans le respect du Code administratif de la fonction publique et des règles applicables en matière de droit du travail et de protection des données personnelles.

La documentation rigoureuse et détaillée de toutes les tâches réalisées dans le cadre des travaux d'investigation est primordiale. L'équipe d'investigation (Point 10.3.4.2.) sera donc chargée de documenter les demandes d'accès aux données ou informations, les données ou informations collectées, les personnes sollicitées pour ces demandes, les comptes-rendus des entretiens réalisés, et les analyses et commentaires qui en découlent[66] (Point 10.3.4.4.).

L'équipe d'investigation fait régulièrement rapport de l'avancement de l'enquête selon les modalités définies dans la procédure de traitement et d'investigation d'un soupçon d'abus et de fraudes. En fonction des cas, l'équipe d'investigation rapporte à l'organe de gouvernance, voire à la cellule de gestion de crise.

10.3.4.2 Élaboration d'un plan d'investigation

S'il est décidé d'entamer une investigation à proprement parler, un plan d'investigation devra être rédigé afin d'encadrer les opérations liées à l'enquête. Ce plan d'investigation se base sur les résultats de la phase de pré-investigation et définit :

1) Les ressources formant l'équipe d'investigation et leurs rôles et responsabilités respectifs

En fonction de la nature du soupçon et des besoins de l'enquête, l'équipe d'investigation, généralement nommée par le service LAF (en fonction des cas, en concertation avec le président), pourra être composée des personnes suivantes[67] :

- Le service LAF, pour capitaliser sur ses connaissances en matière de scénarios d'abus et de fraudes, de risques et de procédures juridiques à suivre ;
- Le responsable du département et/ou service concerné par les faits rapportés. En fonction de l'organisation interne de l'institution, des référents en gestion des risques pourraient être nommés dans chaque département et/ou service dans ce cas, le référent concerné pourrait faire partie de l'équipe d'investigation ;
- Un expert métier du processus concerné ;
- Le service informatique pour l'extraction de données ou l'accès à des logiciels et/ou bases de données ;
- Le contrôle interne ou le cas échéant l'audit interne, pour bénéficier de leur expérience en matière de gestion des risques et de contrôle interne ;
- Un ou plusieurs membres des services financiers et comptables ;
- Un consultant externe disposant de compétences spécifiques en matière d'investigation d'abus et de fraudes (un examinateur de fraude certifié, un cabinet d'expertise forensic, etc.) ;
- Un expert juridique afin de garantir le respect des procédures et la conformité légale de l'enquête (juristes, avocats, etc.).

[66] ACFE, AICPA, IIA (2008), *Managing the Business Risk of Fraud: A Practical Guide*

[67] ACFE, AICPA, IIA (2008), *Managing the Business Risk of Fraud: A Practical Guide*, page 41

Une personne doit être nommée responsable de l'équipe chargée de l'investigation et le service LAF ou alternativement, la cellule de gestion de crise si elle est mobilisée, s'assurera que toutes les personnes sollicitées pour les besoins de l'enquête ne sont pas en situation de conflits d'intérêts, respectivement n'ont pas de liens de familiarité avec les auteurs présumés de l'abus ou de la fraude.

2) Les travaux à réaliser et leurs objectifs

Détailler, planifier et prioriser les tâches à réaliser dans le cadre des travaux d'investigation est un élément essentiel à la conduite d'une investigation rigoureuse et efficiente[68]. Les tâches sont allouées aux membres de l'équipe d'investigation en fonction des compétences qu'elles requièrent. À ce stade les données à collecter sont définies en fonction des objectifs de l'investigation.

3) Les flux de reporting sur l'avancée des travaux et des résultats y afférents

Les modalités et les flux de reporting sont définis dans le respect de la procédure de traitement et d'investigation d'un soupçon d'abus et de fraudes. Les éléments suivants doivent notamment être déterminés[69] :

- La nature des informations à remonter ;
- La forme du reporting ;
- Les délais et échéances pour la remontée des informations ;
- La fréquence du reporting ;
- Les destinataires du reporting, généralement l'organe de gouvernance.

Les reportings à prévoir sont par exemple :

- Le reporting de l'équipe d'investigation à l'organe de gouvernance sur l'avancement des travaux d'investigation. La fréquence de ce reporting dépendra notamment de la gravité du soupçon ;
- Le cas échéant, le reporting de l'équipe d'investigation à la cellule de gestion de crise sur l'avancement des travaux d'investigation.

4) Les mesures conservatoires à prendre

Afin d'éviter que l'abus ou la fraude ne continue à être perpétré(e) ou que le scénario d'abus ou de fraudes ne soit répliqué à des situations/processus analogues, des mesures conservatoires peuvent être prises avant la phase d'investigation. Ces mesures ont pour but de minimiser les conséquences de l'abus ou la fraude sur l'organisation et de protéger ses biens, ses ressources ainsi que son image. A titre d'exemple, l'institution pourra envisager de sécuriser les accès à ses locaux ou de restreindre les accès à certains systèmes d'information ou dossiers papier. Le cas échéant, s'il existe un risque avéré que le suspect perpétue ses actes ou tente d'influencer l'investigation, ce dernier pourra être entre autres suspendu de l'exercice de ses fonctions, dans le respect du Code administratif de la fonction publique et du droit du travail.

5) Les exigences en termes de confidentialité qui accompagnent l'investigation

Le sujet de la confidentialité, un des principes régissant la conduite des investigations, est détaillé au point 10.2.1.

10.3.4.3 Réalisation des travaux d'investigation

L'équipe d'investigation mène les travaux d'investigation tels que définis dans le plan d'investigation. L'équipe d'investigation veille aussi à rapporter sur l'avancée des travaux selon les flux de reporting préalablement définis dans le plan d'investigation.

[68] ACFE, AICPA, IIA (2008), *Managing the Business Risk of Fraud: A Practical Guide*

[69] IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*

10.3.4.4 Documentation des travaux d'investigation

L'équipe d'investigation veille à documenter, de manière rigoureuse, les activités et travaux qu'elle mène dans le cadre de l'investigation. Cette documentation servira de support à la rédaction du rapport final. Les éléments suivants sont concernés[70] :

- Les demandes de documents, données électroniques ou autres types d'informations, émises par l'équipe d'investigation ;
- Les documents, données électroniques ou autres types d'informations recueillies ;
- Les comptes-rendus ou mémorandums d'entretiens réalisés ;
- Les analyses et résultats d'analyses relatives aux documents, données électroniques, interviews ou autres types d'informations.

Une documentation consciencieuse est importante dans la mesure où les éléments factuels collectés pourraient servir de preuves dans un contexte de procédures pénales ou civiles[71].

10.3.5 Phase de clôture

Les résultats de l'investigation sont compilés dans un rapport final, une revue indépendante, qui étaye les allégations d'abus ou de fraudes par des faits documentés. Les mécanismes et scénarios d'abus ou de fraudes identifiés sont exposés, ainsi que les causes si elles ont pu être identifiées. L'ampleur du préjudice par exemple financier et/ou réputationnel pour l'institution est également évaluée. Ce rapport est transmis à l'organe de gouvernance en conformité avec la procédure de traitement et d'investigation d'un soupçon d'abus et de fraudes définie au préalable. Les conclusions de l'investigation doivent permettre un traitement adéquat de l'incident et l'équipe d'investigation peut émettre une proposition sur les sanctions à prévoir. Le rapport d'investigation final permet au service LAF, voire à l'équipe d'investigation de :

- Déterminer les mesures correctives en concertation avec les différents services ;
- Prévoir la mise en œuvre de ces mesures ;
- Planifier le suivi par exemple par le service LAF et/ou le contrôle interne.

De même, ce rapport permet au service LAF d'alimenter et de tenir à jour la base de données sur les cas d'abus et de fraudes précédemment traités.

10.4 Sanctions

En fonction des résultats de l'enquête menée par l'équipe d'investigation et de la gravité des faits, différentes sanctions pourront être appliquées à l'encontre du ou des auteurs d'abus et de fraudes. Il appartient généralement au président et/ou à l'organe de gouvernance de décider des sanctions à prévoir sur base des suggestions faites par l'équipe d'investigation dans son rapport final. Les sanctions seront décidées et appliquées au regard du cadre légal et règlementaire applicable à l'institution et de ses procédures internes.

10.4.1 Sanctions disciplinaires

Tout manquement à ses devoirs et toute infraction aux lois et aux règlements en vigueur expose le collaborateur à une sanction disciplinaire et à une éventuelle sanction pénale[72].

10.4.2 Procédures pénales

En cas de faits commis par des parties prenantes et/ou tous autres tiers et que la gravité de l'incident le justifie, l'institution se réfère aux autorités judiciaires compétentes (notamment le Parquet général) pour entamer des

[70] ACFE, AICPA, IIA (2008), *Managing the Business Risk of Fraud: A Practical Guide*, page 43

[71] IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*

[72] Portail de la Fonction publique :
Manquement aux devoirs, https://fonction-publique.public.lu/fr/carriere/manquement-devoirs.html

poursuites pénales à l'encontre de la personne concernée. Ces poursuites ont pour but de sanctionner de manière appropriée le non-respect des lois et règlements en vigueur.

Comme indiqué au chapitre 3, la fraude, sous forme d'escroquerie et de tromperie, constitue, au Luxembourg, un délit passible d'une peine d'emprisonnement de quatre mois à cinq ans et d'une amende allant de 251 à 30.000 euros[73]. L'abus de confiance, constitue aussi un délit passible d'une peine d'emprisonnement d'un mois à cinq ans et d'une amende allant de 251 à 5.000 euros[74].

Selon l'article 451 du Code de la sécurité sociale, ceux qui ont frauduleusement amené les institutions de sécurité sociale à fournir des prestations, une pension, des secours ou d'autres avantages qui n'étaient pas dus ou n'étaient dus qu'en partie, sont punis d'un emprisonnement d'un mois à cinq ans et d'une amende de deux cent cinquante et un euros à quinze mille euros à moins qu'une peine plus forte ne résulte d'une autre disposition légale. De même, la tentative de ce délit sera punie d'un emprisonnement de huit jours à deux ans et d'une amende de deux cent cinquante et un euros à dix mille euros. De plus, les coupables pourront être placés, pour un terme de deux à cinq ans, sous la surveillance spéciale de la police et condamnés à l'interdiction de tout ou partie des droits énumérés à l'article 31 du Code pénal, pour un terme de cinq à dix ans.

L'IFACI recommande fortement de recourir à un avocat pour bénéficier de conseils sur la constitution du dossier pénal et d'une assistance technique tout au long de la procédure[75]. D'ailleurs, un élément important à prendre en compte en cas de saisine des autorités judiciaires est la recevabilité des preuves. Toutes les données collectées dans le cadre de l'investigation ne constituent pas forcément des preuves à valeur légale en tant que telles. Par exemple, des comptes-rendus d'entretiens ne pourront pas servir à la démonstration de la preuve. Par contre, les données informatiques peuvent être des données cruciales du dossier. L'institution et notamment la cellule de gestion de crise (si mobilisée), met en place les mesures nécessaires à la *« capture, la conservation et l'analyse »*[76] de ces données.

10.4.3 Procédures civiles

Si l'acte abusif ou frauduleux a engendré un dommage financier pour l'institution, cette dernière pourra se constituer partie civile et engager une procédure judiciaire auprès des autorités compétentes afin d'exiger la réparation du préjudice financier subi, auprès du ou des responsable(s) des faits.

10.5 Mesures correctives

Comme mentionné au point 10.3.4., l'investigation permet entre autres d'identifier les faiblesses, dans le dispositif de gestion des risques et de contrôle interne, qui ont favorisé la survenance de l'abus ou de la fraude. Les défaillances recensées, suite à l'investigation, doivent donc être analysées en détail afin de déterminer les mesures correctives à mettre en place pour y remédier et éviter que le scénario d'abus et de fraudes se répète dans le futur.

Les corrections apportées peuvent viser le renforcement des contrôles aussi bien préventifs (par exemple l'amélioration des contenus de formation, le lancement de campagnes de sensibilisation, la revue de la séparation des tâches)[77] que détectifs (par exemple l'analyse de données plus poussée, la mise en place de contrôles supplémentaires). Dans certains cas, les mesures correctives engendrent des remaniements organisationnels[78].

Les mesures correctives sont décrites dans le rapport final d'investigation et dans la base de recensement des cas d'abus et de fraudes traités, tenue par le service LAF. Leur implémentation fait l'objet d'un suivi rigoureux dans le temps. En fonction de la gravité des cas, mais aussi de l'impact de ces mesures, les propositions d'actions correctives seront validées par le président et présentées à l'organe de gouvernance.

[73] Code pénal (2023), Livre II, Titre IX, Chapitre II, articles 496 à 504
[74] Code pénal (2023), Livre II, Titre IX, Chapitre II, articles 491 à 495
[75] IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*
[76] IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*, page 55
[77] ENABEL (2019), *Politique concernant la maîtrise des risques de fraude et de corruption*, page 5
[78] ACFE, AICPA, IIA (2008), *Managing the Business Risk of Fraud: A Practical Guide*

Rôles et responsabilités clés

- Le service LAF élabore une procédure de traitement et d'investigation d'un soupçon d'abus et de fraudes. L'organe de gouvernance valide ladite procédure ;
- Le service LAF tient à jour une base de données sur les cas d'abus et de fraudes ;
- Une personne ou un service désigné(e) (ou un prestataire externe, si l'institution a fait le choix de l'externalisation), réceptionne le signalement puis le redirige vers le service LAF, qui évaluera alors sa recevabilité (phase de signalement) ;
- Le service LAF collecte les premières informations disponibles et effectue une succincte première identification et évaluation des risques potentiels ou réels (phase de découverte) ;
- Le service LAF ou l'équipe chargée de l'investigation mène la phase de pré-investigation et documente ses conclusions et propositions dans un document formalisé ;
- Le service LAF peut proposer au président de saisir et de mobiliser la cellule de gestion de crise ;
- Le service LAF rédige le plan d'investigation (selon les cas, le président est consulté pour nommer l'équipe d'investigation) ;
- L'équipe d'investigation mène la phase d'investigation et documente ses travaux. En fonction des cas, l'équipe d'investigation rapporte à l'organe de gouvernance voire à la cellule de gestion de crise ;
- L'équipe d'investigation s'assure du respect des principes de confidentialité, de protection des informations, d'impartialité et d'objectivité tout au long de l'investigation ;
- L'équipe d'investigation rédige un rapport final d'investigation (phase de clôture) ;
- Sur proposition de l'équipe d'investigation, respectivement du service juridique et/ou sur conseil d'un avocat, le président et/ou l'organe de gouvernance décident des procédures civiles et/ou disciplinaires à enclencher dans le respect du cadre légal et règlementaire applicable à l'institution et de ses procédures internes ;
- Le service juridique (ou le cabinet d'avocats mandaté par l'institution) constitue le dossier pénal et/ou civil ;
- Le service LAF en concertation avec le contrôle interne respectivement l'audit interne et les départements et/ou services, déterminent les mesures correctives à mettre en place ;
- Les différents départements et services mettent en place des mesures correctives : le suivi pourra être réalisé par le service LAF et/ou le contrôle interne en fonction du contexte organisationnel et des choix de chaque institution ;

Au cas où une cellule de gestion de crise est saisie :

- La cellule de gestion de crise garantit la confidentialité des informations ;
- La cellule de gestion de crise s'assure que la communication interne et externe est maîtrisée ;
- La cellule de gestion de crise s'assure du bon déroulement des procédures légales et/ou disciplinaires et de la remontée des informations à chaque étape de l'investigation ;
- La cellule de gestion de crise sollicite des intervenants externes en fonction des besoins de l'investigation.

Pour en savoir plus

- ACFE, IIA (2023), Building a best-in-class whistleblower hotline program
- ACFE (2022), ACFE Fraud Examiners Manual :
  - Chapter Planning and conducting a fraud examination
- ACFE, Grant Thornton (2020), Anti-fraud playbook – The best defense is a good offense :
  - Play 7 - Lay the groundwork for investigations
  - Play 8 - Conduct investigations
  - Appendix C - Implementation checklists
- ACFE (2017), In-House Fraud Investigation Teams – 2017 Benchmarking Report
- ACFE, AICPA, IIA (2008), Managing the Business Risk of Fraud - A Practical Guide :
  - Section 5 - Fraud investigation and corrective action
- CGMA (2012), Report Fraud risk management – A guide to good practice :
  - Appendix 7 - Outline fraud response plan
  - Appendix 8 - Example of a fraud response plan
- COSO, ACFE (2016), Fraud Risk Management Guide :
  - Chapter 4 - Fraud investigation and corrective action
  - Appendix I-4 - Fraud investigation and corrective action scorecard
- Durham County Council (2018), *Fraud response plan*
- IFACI (2010), La fraude – Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche :
  - Partie 4 - Réagir face à un soupçon de fraude ou traiter un cas avéré
  - Partie 6 - Capitaliser l'expérience à partir des cas avérés
  - Annexe 5 - Fiches

11 MONITORING : ÉVALUATION DE L'EFFICACITÉ DU DISPOSITIF DE LUTTE CONTRE L'ABUS ET LA FRAUDE

Le dispositif LAF, établi et mis en œuvre par l'institution, doit faire l'objet d'une évaluation permanente et périodique de son efficacité. Ce monitoring s'insère dans le cadre du dispositif de gestion des risques et de contrôle interne de l'institution. De ce fait, il doit couvrir l'ensemble des aspects ayant trait au dispositif LAF, à savoir : la gouvernance, la prévention, la détection, le dispositif d'alerte, le traitement et l'investigation, le monitoring ainsi que la communication et la coordination avec les différents intervenants.

Préalablement à l'évaluation de l'efficacité du dispositif LAF, un état des lieux devra être réalisé en procédant à une analyse de l'existant (situation *« As is »*) et à un diagnostic du degré de maturité du dispositif afin de définir les actions à mettre en place pour atteindre les objectifs attendus (le *« To be »*). Cette approche permettra également d'implémenter de nouveaux éléments visant à lutter contre l'abus et la fraude ou de compléter les mesures existantes.

Des outils et documents disponibles en libre accès peuvent être utiles à la réalisation de l'analyse de l'existant et audit diagnostic.

À cet effet, le COSO et l'ACFE mettent à disposition des fiches d'évaluation (*« Scorecards »*) portant sur la gouvernance du risque d'abus et de fraudes, l'évaluation dudit risque, les activités de contrôles y relatives, l'investigation ainsi que les actions correctives et le monitoring de la gestion du risque d'abus et de fraudes.

Une grille de diagnostic préalable à la réalisation d'un état des lieux du dispositif LAF est fournie à l'annexe 14. L'annexe 15 illustre une grille de diagnostic pour l'évaluation de la maturité du dispositif LAF.

Comme alternative à la grille de diagnostic, une checklist peut également être utilisée pour réaliser un état des lieux du dispositif LAF. Un exemple de checklist pour le diagnostic des mesures de prévention de la fraude est fourni à l'annexe 16.

11.1 Surveillance permanente

Pour évaluer l'efficacité du dispositif LAF, l'institution doit prévoir des évaluations continues à réaliser par :

- Les managers opérationnels de la première ligne de maîtrise (personnel d'encadrement des activités « *cœur de métier* » et « *support* »). Dans ce contexte, ils peuvent être assistés par des acteurs de la deuxième ligne de maîtrise tels que le service LAF ou le contrôle interne ;
- Le président (et/ou un collaborateur désigné suivant les dispositions de l'article 397 alinéa 3 du CSS).

Ces évaluations permettent, le cas échéant, de détecter des problèmes et un suivi avec les collaborateurs concernés s'imposent pour déterminer les mesures correctives ou autres initiatives à mettre en place.[79].

À titre d'exemples, la surveillance permanente peut se traduire par :

- La mise en place de tableaux de bord et le suivi d'indicateurs ;
- La définition de systématiques de suivi et de reporting ;
- La mise en place de contrôles récurrents ou en continu (requêtes informatiques, rapports d'exception, etc.) afin d'identifier des indicateurs d'abus et de fraudes : Points 8.2. et 8.3. ;
- Le suivi de l'efficacité des plans d'actions décidés (Introduction du chapitre 11, informant sur l'analyse de l'existant) ;
- Le suivi des plaintes et des réclamations : Point 8.3.2. ;
- Le suivi des incidents : Point 8.3.2.

[79] IFACI, PWC (2013), COSO Référentiel intégré de contrôle interne – Principes de mise en œuvre et de pilotage

11.1.1 Mise en place de tableaux de bord et suivi d'indicateurs

L'analyse et le diagnostic du dispositif LAF précités pourront être réalisés par le service LAF ou par d'autres acteurs de la deuxième ligne de maîtrise, tels que le contrôle interne. Ils permettront notamment d'identifier de potentielles faiblesses et des points d'amélioration, de prioriser les actions à mener[80] et de définir les indicateurs à suivre[81].

Les indicateurs peuvent être de deux types à savoir ; les indicateurs de suivi ou de résultats et les indicateurs de performance.

Les indicateurs de suivi ou de résultats, purement descriptifs, attestent de la réalisation d'une action (la rédaction d'une politique LAF, la rédaction d'un code de conduite, des actions de sensibilisation, le nombre de cas d'abus et de fraudes traités et clôturés par année, etc.).

Les indicateurs de performance mesurent quant à eux l'efficacité des actions menées par rapport à l'objectif défini (le montant des pertes recouvrées, le montant des pertes subies par rapport au montant des pertes attendues, le nombre de jours nécessaires pour clôturer une investigation, le pourcentage de cas ayant mené à des sanctions disciplinaires, le pourcentage de cas ayant mené à des actions judiciaires, etc.).

Ainsi, dans le cadre des campagnes de sensibilisation des collaborateurs de l'institution aux risques d'abus et de fraudes (Point 7.4.), le plan d'action pourra par exemple inclure la rédaction et la promotion d'un code de conduite au moyen de communications internes. De même, l'apposition de pancartes, la distribution de flyers et l'organisation de formations peut contribuer à la sensibilisation aux risques d'abus et de fraudes. Les indicateurs de suivi ou de résultats indiqueront si toutes ces actions ont bien été menées. En revanche, les indicateurs de performance détermineront si l'objectif de sensibilisation a bien été atteint, par exemple en examinant les réponses à un quiz proposé aux participants aux formations.

Les indicateurs de performance sont associés à un taux de recouvrement des pertes plus important que les indicateurs de suivi[82]. Ainsi, l'utilisation d'indicateurs tels que le montant des pertes recouvrées et le pourcentage de cas ayant mené à des actions judiciaires serait, par exemple, plus utile au renforcement du dispositif LAF que le suivi du nombre de cas traités et clôturés d'année en année.

De plus, les indicateurs doivent être accompagnés de cibles, qui sont à déterminer par le service responsable, comme par exemple[83] :

- Un taux de recouvrement des indus frauduleux augmentant de nième % chaque année ;
- Un taux de couverture des contrôles sur un processus spécifique de nième %.

Ces actions et indicateurs devraient, à moyen terme, être considérés lors de l'établissement et de la mise à jour annuelle de la planification triennale des institutions et faire l'objet d'un suivi régulier.

11.1.2 Systématiques de suivi et de reporting

Des systématiques de suivi et de reporting devront être définies. La nature des informations rapportées, leur granularité et la fréquence des communications dépendront du destinataire du reporting et de ses attentes. Ainsi, un reporting trimestriel (par exemple sous forme de tableaux de bord) portant sur les activités du service LAF, le suivi des actions ainsi que sur les indicateurs, pourra être mis en place à destination du président et des collaborateurs qui l'assistent conformément à l'article 397 alinéa 3 du CSS. Ces derniers, ensemble avec le CA jouent un rôle important dans le monitoring des activités et la surveillance des risques d'abus et de fraudes.

Le reporting au CA pourra être réalisé de manière plus synthétique, avec une fréquence semestrielle ou annuelle par exemple.

---

[80] IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*

[81] AISS (2019), *Lignes directrices de l'AISS - Erreur, évasion et fraude dans les systèmes de sécurité sociale*. Ligne directrice 6 - Établir des objectifs et indicateurs en matière d'EEF

[82] ACFE (2017)*, In-House Fraud Investigation Teams : 2017 Benchmarking Report*

[83] AMELI (2018), *Convention d'objectifs et de gestion entre l'État et la Cnam 2018* > 2022, page 92

Ces systématiques de reporting, leur contenu et leur forme seront à définir et à documenter en tenant compte des attentes de l'organe de gouvernance.

De plus, le suivi des actions à mettre en place et des objectifs à atteindre en termes de lutte contre les abus et les fraudes devrait, à moyen terme, faire partie intégrante du rapport annuel informant sur la manière dont fonctionne le contrôle interne tel que prévu à l'article 408bis alinéa 3 du Code de la sécurité sociale.

De même, il pourrait être utile d'y dédier un chapitre dans le rapport d'activité publié annuellement par l'institution. Certains indicateurs, notamment de performance, pourraient, par ce moyen, être communiqués à l'extérieur dans un objectif de prévention et de dissuasion auprès des parties prenantes externes ou de tous autres tiers. Les pertes financières évitées grâce à la mise en place d'un dispositif LAF sont souvent communiquées pour témoigner de son efficacité. Des exemples de communication externe sur les résultats du programme de lutte contre l'abus et la fraude sont disponibles en ligne[84].

11.2 Surveillance périodique

L'institution doit prévoir des évaluations périodiques afin de s'assurer que le dispositif LAF fonctionne comme conçu. Ces dernières peuvent être réalisées par la fonction d'audit interne ou via d'autres approches en matière d'évaluation périodique.

11.2.1 Evaluations réalisées par l'audit interne

L'audit interne[85], au sens de l'IIA et en tant que troisième ligne de maîtrise, doit, lors de chaque mission d'assurance, définir dans son programme de travail, des procédures d'audit permettant d'identifier et d'évaluer le risque de fraude ainsi que la manière dont l'organisation gère ce risque[86]. Ainsi, par exemple, les contrôles mis en place dans le cadre du dispositif LAF peuvent faire l'objet d'une appréciation par l'audit interne.

Par ailleurs, l'audit interne peut être amené à évaluer de manière périodique, indépendante et objective, l'efficacité du dispositif LAF. Pour se faire, l'audit interne doit inclure au préalable cette mission d'assurance dans son plan d'audit interne.

À défaut de disposer d'un service d'audit interne, il est possible de faire appel à un autre service de l'institution, appartenant à la deuxième ligne de maîtrise, qui réalisera alors une évaluation de l'efficacité du dispositif LAF. Toutefois, il convient de rappeler que les acteurs de la deuxième ligne de maîtrise (comme le contrôle interne) disposent d'un degré d'indépendance et d'objectivité moindre que celui de l'audit interne.

Dans le cadre des évaluations périodiques du dispositif LAF, le recours à un prestataire externe (auditeur externe réalisant des missions d'assurance et de conseil) pourrait également être envisagé.

11.2.2 Autres approches en matière d'évaluation périodique

Une évaluation périodique du dispositif LAF s'avère nécessaire afin de juger de sa pertinence, de son implémentation et de son efficacité.

Les évaluations périodiques du dispositif LAF pourront notamment être réalisées par :

- Les services de la deuxième ligne de maîtrise (service LAF, gestion des risques, contrôle interne, assurance qualité, etc.). En effet, en fonction des objectifs poursuivis et de la maturité de l'institution au contrôle interne et à la lutte contre les abus et les fraudes, ils pourront soit :
    - Réaliser des évaluations objectives eux-mêmes lors d'ateliers avec la première ligne de maîtrise ;
    - Fournir des checklists d'auto-évaluation aux managers opérationnels de la première ligne de maîtrise et leur apporter une assistance méthodologique. Ces derniers devront alors compléter les checklists et faire remonter leurs résultats aux services de la deuxième ligne de maîtrise.

[84] AMELI (2019), *Bilan 2018 des actions de lutte contre la fraude et actions de contrôles*

[85] Le Code de la sécurité sociale (2023) ne prévoit pas de fonction d'audit interne. Toutefois l'exposé des motifs du projet de loi n° 7004 précise que « En effet, la mise en place d'une gestion des risques implique l'organisation du contrôle interne complété, le cas échéant, par une fonction d'audit interne, adaptée au niveau de maturité en matière de bonne gouvernance et à la taille de l'institution de sécurité sociale concernée. »

[86] IIA (2019), Prise de *position Fraude et Audit interne : Fournir une assurance sur les contrôles anti-fraude est indispensable pour garantir leur efficacité*

Lors des campagnes de sensibilisation aux risques d'abus et de fraudes (Point 7.4.), des checklists d'auto-évaluation pourront être distribuées aux managers opérationnels de la première ligne de maîtrise afin qu'ils puissent les utiliser, s'ils le souhaitent.

- Un collaborateur d'un autre service (1ère ligne de maîtrise), via des évaluations croisées entre pairs (*« peer reviews »*) ;
- Le manager opérationnel du service concerné (1ère ligne de maîtrise), via des auto-évaluations ayant pour but d'évaluer la mise en place et le fonctionnement du dispositif LAF relatif à son domaine d'activité.

Il convient de noter que ces évaluations devront être coordonnées entre les différents acteurs de la première et de la deuxième lignes de maîtrise afin d'éviter des redondances inutiles[87].

Rôles et responsabilités clés

- La première ligne de maîtrise, en collaboration avec le service LAF et d'autres acteurs de la deuxième ligne de maîtrise, comme le contrôle interne, réalisent un état des lieux du dispositif LAF en procédant à une analyse de l'existant (situation *« As is »)* et à un diagnostic du degré de maturité du dispositif, afin de définir les actions à mettre en place pour atteindre les objectifs attendus (le *« To be »*). Ces actions sont à valider par le président de l'institution ;
- Les managers opérationnels (personnel d'encadrement de la 1ère ligne de maîtrise) et le président (et/ou le collaborateur désigné suivant les dispositions de l'article 397 alinéa 3 du CSS) mettent en place des évaluations continues pour évaluer l'efficacité du dispositif LAF (surveillance permanente) ;
- Le service LAF (ou le contrôle interne) garantit que les systématiques de reporting (en lien avec les abus et les fraudes) soient respectées et en assure le suivi (surveillance permanente) ;
- L'audit interne considère le risque de fraude dans ses missions d'assurance et peut être amené à évaluer de manière périodique, indépendante et objective, l'efficacité du dispositif LAF et les contrôles mis en place à cette fin. En l'absence d'une telle fonction, un prestataire externe peut être mandaté ou un service de la deuxième ligne de maîtrise (comme le contrôle interne) peut en être chargé. Toutefois, il convient de rappeler que la deuxième ligne de maîtrise dispose d'un degré d'indépendance et d'objectivité moindre que celui de l'audit interne ou du prestataire externe (surveillance périodique) ;
- Les services de la deuxième ligne de maîtrise pourront également réaliser des évaluations périodiques. En fonction des objectifs poursuivis et de la maturité de l'institution au contrôle interne et à la lutte contre les abus et les fraudes, ils pourront soit :
  - Réaliser des évaluations objectives eux-mêmes lors d'ateliers avec la première ligne de maîtrise ;
  - Fournir des checklists d'auto-évaluation aux managers opérationnels de la première ligne de maîtrise et leur apporter une assistance méthodologique. Ces derniers devront alors compléter les checklists et faire remonter leurs résultats aux services de la deuxième ligne de maîtrise ;
- Un collaborateur d'un autre service (1ère ligne de maîtrise) réalise des évaluations croisées entre pairs (surveillance périodique) ;
- Les managers opérationnels (personnel d'encadrement de la 1ère ligne de maîtrise) réalisent des auto-évaluations ayant pour but d'évaluer la mise en place et le fonctionnement du dispositif LAF dans leur domaine d'activité (surveillance périodique).

[87] IFACI, PWC (2013), *COSO Référentiel intégré de contrôle interne – Principes de mise en œuvre et de pilotage*

Pour en savoir plus

- ACFE, COSO, (2023) Fraud Risk Management Scorecards :

Fraud Risk Tools (acfe.com)

  - Principle 1 - Fraud risk governance
  - Principle 2 - Fraud risk assessment
  - Principle 3 - Fraud control activities
  - Principle 4 - Fraud investigation and corrective action
  - Principle 5 - Fraud risk management monitoring

- ACFE, Grant Thornton (2020), Anti-fraud playbook – The best defense is a good offense :
  - Play 9 - Monitor your progress
  - Play 10 - Report on your progress
  - Appendix A - Enterprise Anti-Fraud Maturity Assessment Model
  - Appendix C - Implementation checklists
- COSO, ACFE (2016), Fraud Risk Management Guide :
  - Chapter 5 - Fraud risk management monitoring activities
  - Appendix I-5 - Fraud risk management monitoring scorecard
- IFACI, PWC (2013), COSO Référentiel intégré de contrôle interne – Principes de mise en œuvre et de pilotage
- IFACI (2011), Des clés pour la mise en œuvre et l'optimisation du contrôle interne, Cahier de la Recherche
- IFACI (2005), L'auto-évaluation du contrôle interne, Cahier de la Recherche
- IIA (2019), Prise de position Fraude et Audit interne : Fournir une assurance sur les contrôles anti-fraude est indispensable pour garantir leur efficacité

12 COMMUNICATION

La communication est un aspect essentiel pour assurer l'efficacité d'un dispositif LAF. En effet, elle permet notamment de :

- Sensibiliser les collaborateurs aux risques d'abus et de fraudes et développer leur esprit critique ;
- Informer les collaborateurs des procédures en place dans le cadre de la lutte contre l'abus et la fraude (y inclus les modalités de signalement en cas de soupçons) ;
- Renforcer le volet préventif, en informant sur les sanctions encourues ;
- Faciliter les échanges et les remontées d'informations entre tous les acteurs (y inclus les systématiques de reporting vers le président et/ou l'organe de gouvernance) ;
- Faciliter la coordination entre tous les acteurs du dispositif LAF faisant partie de la première, deuxième et, si existant, de la troisième ligne de maîtrise.

Le lancement de campagnes de communication internes et externes permet d'une part, de rappeler aux parties prenantes ou à tous autres tiers, les lois, les règlementations et les règles en vigueur et d'autre part, de les informer sur les risques encourus en cas de leur non-respect. Ces campagnes de communication sont considérées comme une mesure de prévention aux risques d'abus et de fraudes[88].

De même, la diffusion systématique d'informations sur les résultats de la lutte contre l'abus et la fraude, tant en interne qu'en externe, peut avoir un effet dissuasif sur le comportement abusif ou frauduleux, favoriser la conformité et renforcer la réputation de l'institution.

Une bonne communication institutionnelle sera également primordiale en cas de crise. En effet, garder la maîtrise sur la communication en temps de crise est indispensable au maintien de la confiance du public, à la préservation de la réputation de l'institution et à sa continuité opérationnelle[89]. Un dispositif de communication de crise doit être prévu afin que l'institution puisse communiquer de manière *« cohérente, précise et adaptée »*[90] et en temps voulu. Le service communication (ou relations publiques) devra contrôler les informations divulguées à l'extérieur, de sorte à protéger l'intégrité de l'institution. De ce fait, un représentant du service communication pourra faire partie de la cellule de gestion de crise (Point 10.1.2.).

En ce qui concerne la relation avec les médias, il devra être clairement communiqué que seul le service communication (ou relations publiques) et l'organe de gouvernance sont habilités à répondre aux questions en rapport avec la lutte contre l'abus et la fraude pour le compte de l'institution. En effet, la divulgation d'informations relatives à un soupçon d'abus et de fraudes par l'intermédiaire des médias peut mettre en danger la réputation et la crédibilité de l'institution. Toute demande d'informations par des journalistes ou d'autres personnes sera transmise directement au service communication (ou relations publiques). De même, sur les médias sociaux, les parties prenantes internes de l'institution seront tenues, conformément au code de conduite, de ne pas répondre ou émettre de commentaires à propos du dispositif LAF de l'institution.

En cas de poursuites judiciaires, le service communication sera amené à suivre de près le procès et à vérifier que des éventuelles fuites dans la presse ne mettent pas en péril les intérêts de l'institution[91]. En cas de sanctions disciplinaires, les informations communiquées en interne devront être scrupuleusement maîtrisées afin de préserver la confidentialité des informations et le droit à la vie privée.

[88] Sources :
ACFE, Grant Thornton (2020), *Anti-fraud playbook - The best defense is a good offense*
AMELI du Tarn (2011), *L'Assurance Maladie du Tarn lutte contre les abus et les fraudes*. Dossier de presse

[89] AISS (2022), *Lignes directrices de l'AISS - Communication des administrations de sécurité sociale*. Ligne directrice 11, Gestion et communication de crise

[90] AISS (2022), *Lignes directrices de l'AISS - Communication des administrations de sécurité sociale*. Ligne directrice 11, Gestion et communication de crise page 20

[91] IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*

13 ANNEXES

Annexe 1 – Exemples de facteurs déclenchants[92]

Des *opportunités* d'abus ou de fraudes peuvent se présenter lorsque le dispositif de contrôle interne d'une organisation est défaillant. Cette défaillance peut être matérialisée par les exemples suivants :

- Les contrôles sont manquants ou mal conçus ;
- Une séparation des tâches adéquate n'a pas été mise en place ;
- La répartition des rôles et responsabilités entre les collaborateurs et les dirigeants manque de clarté et n'est pas documentée ;
- La répartition des pouvoirs est tellement déséquilibrée qu'il existe des possibilités, en particulier pour les dirigeants, de contourner les contrôles ;
- Le niveau de confiance élevé envers un collaborateur ou un responsable hiérarchique lui permet de contourner ou d'outrepasser les règles et les contrôles existants ;
- Aucune diligence n'est effectuée lors du recrutement d'un nouveau collaborateur ;
- Les procédures d'autorisations des transactions sont absentes ;
- Le principe de double signature pour les engagements et paiements de dépenses est absent ;
- Aucune réconciliation entre les comptes annuels et les actifs physiques n'est effectuée ;
- Aucune réconciliation bancaire n'est effectuée ;
- Aucun dispositif de revue indépendante n'est prévu ;
- Aucune procédure de gestion et de monitoring des accès informatiques n'est en place ;
- Les logs des accès et des actions utilisateurs dans les systèmes d'information ne sont pas tracés ;
- Plusieurs collaborateurs partagent un accès administrateur pour modifier les données de traitement des paiements et les informations bancaires ;
- Le fichier maître des bénéficiaires/fournisseurs peut être mis à jour par tous les collaborateurs et le système ne garde aucun historique des modifications ;
- La supervision, formation ou communication concernant les règles de bonne conduite professionnelle et les conséquences en cas de violations sont absentes ;
- Les transactions sont complexes et peu de collaborateurs les maîtrisent (compétences) ;
- Etc.

Les *incitations/pressions* à l'abus ou à la fraude se réfèrent par exemple, aux situations suivantes :

- L'organisation fixe des objectifs trop exigeants et instaure une pression sur les collaborateurs et les dirigeants pour qu'ils les atteignent ;
- L'organisation établit des systèmes de rémunération, largement basés sur les résultats individuels, en particulier dans des environnements compétitifs et dans des contextes économiques difficiles ;
- Le collaborateur a un grand besoin de reconnaissance ;
- Le collaborateur a des difficultés financières ou un attrait particulier pour l'argent ;
- Le collaborateur fait face à des difficultés personnelles (par exemple problèmes familiaux ou d'addiction) ;

[92] Sources :
IIA Australia (2020*), White paper Fraud Risk Indicators*, pages 3 et 4
IIA (2017), *CRIPP - Lignes directrices complémentaires, Guide pratique sur la planification de la mission : Evaluation des risques de fraude*, pages 5, 6 et 23
IFACI (2017), *Revue internationale des auditeurs et des contrôleurs internes « Audit, risques & contrôle »*, Numéro 9 du 1er trimestre 2017, page 10
IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*, pages 17 et 18

- Le collaborateur a des liens de familiarité avec les fournisseurs, les assurés, etc. ;
- La personne désire avoir du pouvoir, de l'influence ou l'estime de sa famille, de ses collègues ou de la direction (par exemple les pirates informatiques qui fraudent avec l'intention de faire état de leurs capacités plutôt que de causer des dommages) ;
- Certains collaborateurs s'inquiètent de l'avancement professionnel limité et/ou craignent de perdre leur emploi ;
- Etc.

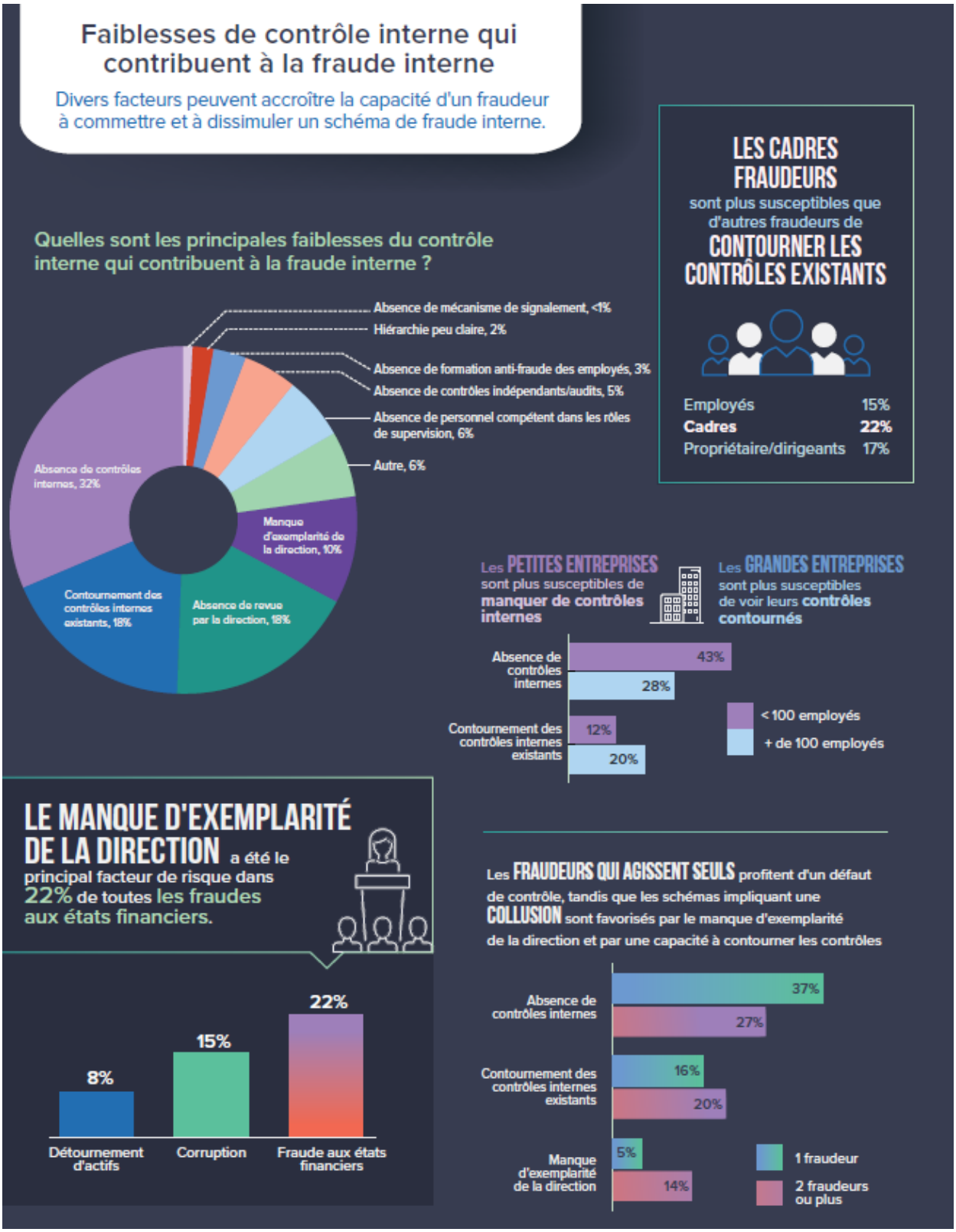
Enfin, la *rationalisation* de l'acte d'abus ou de fraude peut s'exprimer de différentes manières, dont notamment par une auto-justification rationnelle (inventée, convaincante ou plausible) fondée sur des arguments tels que par exemple :

- Une promotion manquée ;
- Une rémunération trop basse par rapport aux efforts consentis ;
- L'impression ou la croyance que « *tout le monde fait pareil* » ;
- L'impression qu'un comportement inapproprié semble être monnaie courante et fait partie de la culture de l'organisation ;
- La croyance que les politiques et procédures internes n'ont aucun sens et ne sont donc, de facto, pas applicables à soi-même ;
- La croyance que « *ce n'est pas grave* » car l'action est si insignifiante que personne ne la remarquera et/ou s'en souciera ;
- La croyance que les actions sont temporaires et que les actifs financiers ou physiques seront remboursés, respectivement rendus plus tard à l'organisation ;
- La perception de favoritisme ou de négligence par rapport à d'autres collaborateurs ;
- La perception que le management affiche un comportement négatif au plus haut niveau ;
- Etc.

La rationalisation sera d'autant plus impactée si la culture éthique de l'organisation n'encourage pas la bonne conduite ni l'exemplarité des dirigeants (« *Tone at the top* »).

Annexe 2 – Principales faiblesses dans un dispositif de contrôle interne

A) Faiblesses de contrôle interne (tous secteurs confondus)[93]



[93] ACFE (2020), *Report to the Nations. 2020 Étude mondiale sur la fraude interne et les abus professionnels*, page 36

B) Faiblesses de contrôle interne (secteur public)[94]

[94] ACFE (2020), *Report to the Nations. 2020 Global Study on Occupational Fraud and Abuse. Government Edition*, page 14

Annexe 3 – Exemples de rôles et responsabilités dans un dispositif LAF

A) Sample Fraud Policy Responsibility Matrix du COSO et ACFE[95]

Sample Fraud Policy Responsibility Matrix

This sample matrix can be used as a tool to summarize and visualize the fraud risk governance responsibilities that have been defined for the organization. Entries shown are for example only.

Action Required	Board	Exec. Mgmt.	Mid / Line Mgmt.	Risk Mgmt.	Legal	Internal Audit	Fin / Acctg.	FIU* / Corp. Security	HR / Employee Relations	PR	IT	BU** / Line Personnel
1. Fraud Risk Management Oversight	P											
2. Code of Conduct / Fraud Control Policy		P										
3. Fraud Prevention Controls (Process Level)		P	SR	S	S	S	S	S	S	S	S	S
4. Fraud Risk Assessment		P	S	S	S	S	S	S	S	S	S	S
5. Fraud Detection Controls (Process Level)		P	SR	S	S	S	S	S	S	S		S
6. Fraud Education / Training and Awareness		S			S	S		P	SR			
7. Hotline / Ethics Line					P	S		S	S			
8. Reporting of Concerns / Complaints/ Violations	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR
9. Evaluation of Reported Incidents					P	S		SR	S		S	
10. Fraud / Misconduct Investigations	S				SR	S		P	S		S	

[95] COSO, ACFE (2016), *Fraud Risk Management Guide*, page 90

11. Whistleblower Follow-Up					SR			P				
12. Referral to Law Enforcement					S			P				
13. Regulatory Self-Disclosure	S	P			SR							
14. Civil Litigation					P			S				
15. Asset recovery								P				
16. Monitor Recoveries							P	S				
17. Disciplinary Action			SR		S				SR			
18. Remediation / Corrective Action		S	SR	S	S	SR	S	SR	S		S	
19. Fraud Prevention / Detection Recommendations	S	S	S	S	S	SR	S	SR	S	S	S	S
20. Publicity / Press Releases		S			S					P		
21. Proactive Fraud Auditing						P	S					
22. Internal Controls Review						P						
23. Case Analysis						S		P				
24. Fraud Risk Reporting		P	S	S	S	S	S	SR	S		S	
25. Fraud Risk Management Framework Assessment		SR				P						

P (Primary Responsibility) **S** (Secondary Responsibility) **SR** (Shared Responsibility)
***FIU** (Fraud Investigation Unit) ****BU** (Business Unit)

B) Sample Fraud Policy Decision Matrix de l'ACFE, l'AICPA et l'IIA[96]

SAMPLE FRAUD POLICY DECISION MATRIX

NOTE: This matrix can be used as a tool to summarize and visualize the responsibilities that have been defined for the organization. This is not a standard for "who" should have "what" responsibilities.

Action Required	Investigation Unit	Internal Auditing	Finance Acctg.	Exec Mgmt.	Line Mgmt.	Risk Mgmt.	PR	Employee Relations	Legal
1. Controls to Prevent Fraud	S	S	S	P	SR	S	S	S	S
2. Incident Reporting	P	S	S	S	S	S	S	S	S
3. Investigation of Fraud	P	S						S	S
4. Referrals to Law Enforcement	P								S
5. Recovery of Monies Due to Fraud	P								
6. Recommendations to Prevent Fraud	SR	SR	S	S	S	S	S	S	S
7. Internal Control Reviews		P							
8. Handle Cases of a Sensitive Nature	P	S		S		S		S	S
9. Publicity/Press Releases	S	S					P		
10. Civil Litigation	S	S							P
11. Corrective Action/ Recommendations to Prevent Recurrences	SR	SR		S	SR	S			S
12. Monitor Recoveries	S		P						
13. Proactive Fraud Auditing	S	P							
14. Fraud Education/ Training	P	S			S		S		
15. Risk Analysis of Areas of Vulnerability	S	S				P			
16. Case Analysis	P	S							
17. Hotline	P	S							
18. Ethics Line	S	S							P

P (Primary Responsibility) **S (Secondary Responsibility)** **SR (Shared Responsibility)**

[96] ACFE, AICPA, IIA (2008), *Managing the Business Risk of Fraud: A Practical Guide*, page 54

Annexe 4 – Exemples de risques d'abus et de fraudes dans les activités cœur de métier et support[97]

A) Activités cœur de métier

	Intitulé du risque
Fraudes et abus internes	Abus d'arrêts de travail ;
	Abus de pouvoir ;
	Acceptation de cadeaux illicites ;
	Acceptation de pots de vin et dessous de table ;
	Attribution de prestations fictives par un collaborateur ;
	Communication de fausses informations (internes/externes) ;
	Comptabilisation de fausses créances et remboursements ;
	Conflits d'intérêts (par exemple assurés, prestataires de soins, pensionnés, etc.) ;
	Corruption active ou passive ;
	Création de fausses instructions de paiements ;
	Création de mémoires d'honoraires fictifs ;
	Création interne d'un faux dossier (par exemple individu, carrière, demande de liquidation) ;
	Détournement de financement d'activités sociales ;
	Détournement de paiements ;
	Détournement par annulation de créances ;
	Dissimulation de paiements entrants ;
	Divulgation d'informations confidentielles ;
	Double paiement / erreur de paiement ;
	Ententes ;
	Falsification de documents ;
	Falsification de documents en vue d'obtenir une autorisation de paiement ;
	Falsification de signatures ;
	Fausse saisie sur allocation / pension / indemnité ;
	Fausses déclarations intentionnelles ;
	Favoritisme vis-à-vis d'un assuré, prestataire de soins, pensionné, etc. ;
	Majoration de prestations ;
	Malveillance informatique (par exemple virus, destruction de fichiers, piratage) ;
	Malversations ;
	Modification du bénéficiaire d'une prestation ;
	Modification frauduleuse des accès et profils utilisateurs dans les systèmes d'information ;
	Modification frauduleuse des coordonnées de paiement dans un dossier existant (par exemple assurés, pensionnés, bénéficiaires d'allocations) ;
	Non-versement intégral des prestations ;
	Omissions intentionnelles (par exemple non-paiement d'une prestation)
	Prestations sur ou sous-évaluées ;
	Remboursements frauduleux multiples ;
	Remboursements indus sur le compte bancaire d'un proche ;
	Usurpation de compte / d'identité ;
	Utilisation abusive d'informations confidentielles ;
	Utilisation abusive des actifs physiques mis à disposition dans le cadre des activités professionnelles ;

[97] Sources :
ACFE (2020), *Report to the Nations. 2020 Global Study on Occupational Fraud and Abuse*
IIA (2017), *CRIPP - Lignes directrices complémentaires, Guide pratique sur la planification de la mission : Évaluation des risques de fraude*
IFACI (2015), *Dispositifs de maîtrise des risques de fraude à l'assurance, à la retraite complémentaire et à l'action sociale, Cahier de la Recherche*
IFACI (2013), *La cartographie des risques, Cahier de la Recherche*
IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*
Assurance maladie Alsace (2017), Lutte contre les abus et les fraudes à l'Assurance Maladie en Alsace : les résultats pour l'année 2016, Conférence de presse, 19 mai 2017
Assurance maladie Alsace (2016), *Lutte contre les abus et les fraudes à l'Assurance Maladie en Alsace : les résultats pour l'année 2015, Dossier de presse du 23 mai 2016*
CGMA (2012), *Report Fraud risk management - A guide to good practice*

	Utilisation du profil d'un autre utilisateur pour réaliser des transactions frauduleuses dans les systèmes d'information (usurpation d'identité) ;
	Utilisation non autorisée d'actifs physiques ;
	Vol d'actifs financiers (par exemple caisse, chèques)
	Vol d'actifs physiques ;
	Vol de données ;
	Vol de mots de passe pour effectuer des transactions dans les systèmes de paiements ;
	Etc.
Fraudes et abus externes	Abus d'arrêts de travail ;
	Abus de consommation de médicaments ou de soins ;
	Abus de consultations médicales ;
	Abus de pouvoir (ou de position dominante) ;
	Abus de prescription d'arrêts de travail ;
	Abus de prescription de médicaments ;
	Attribution de cadeaux illicites ;
	Blanchiment d'argent ;
	Communication de fausses informations (internes/externes) ;
	Conflits d'intérêts ;
	Consultation répétée et non justifiée de plusieurs professionnels de santé du même domaine de spécialité ;
	Corruption active ou passive de collaborateurs ;
	Création de mémoires d'honoraires fictifs ;
	Création de salariés fictifs afin de bénéficier d'avantages indus ;
	Création d'ordonnances médicales fictives ;
	Déclaration d'un faux accident de travail ;
	Détournement de financement d'activités sociales ;
	Détournement du mécanisme de tiers payant ;
	Détournement par annulation de créances ;
	Divulgation d'informations confidentielles ;
	Double facturation / erreur de facturation ;
	Ententes ;
	Exercice d'une activité non autorisée rémunérée ou bénévole pendant un arrêt maladie indemnisé ;
	Facturation répétée d'actes non nécessités ;
	Facturation répétée de produits non délivrés ;
	Falsification d'ordonnances médicales ;
	Falsification de codifications utilisées pour les actes de prescriptions ou de factures (par exemple optiques ou dentaires) ;
	Falsification de documents ;
	Falsification de la durée de l'arrêt de travail prescrit ;
	Falsification de signatures ;
	Fausse déclaration concernant la dépendance après un décès ;
	Fausse déclaration de personnes à charge ;
	Fausse déclaration de salaires ;
	Fausse facturation par un professionnel de santé, établissement de soins, transporteur de patients, etc. ;
	Fausses déclarations intentionnelles ;
	Favoritisme vis-à-vis d'un assuré, prestataire de soins, pensionné, etc. ;
	Fraude à la réversion ;
	Fraude au président ;
	Fraude aux aides sociales individuelles ;
	Fraude aux prestations d'indemnité journalière et d'incapacité ;
	Fraude aux prestations de soins de santé ;
	Fraude sur la situation familiale ;
	Malveillance informatique (par exemple virus, destruction de fichiers, piratage) ;
	Modification frauduleuse des accès et profils utilisateurs dans les systèmes d'information ;
	Modification frauduleuse des coordonnées de paiement (usurpation de compte) ;

	Non-déclaration d'un changement de situation (par exemple remariage, enfants ne faisant plus partie du ménage) ;
	Non-respect des consignes tarifaires ;
	Non-respect des règles de facturation ;
	Omissions intentionnelles (par exemple rétention d'informations) ;
	Poursuite illégitime de prestations d'un bénéficiaire décédé ;
	Prescription d'un arrêt maladie non justifié par l'état de santé du patient ;
	Prescription d'un médicament préférentiel en raison d'un accord tacite avec une entreprise pharmaceutique ;
	Prescription de médicaments non nécessités et justifiés ;
	Prestations sur ou sous-évaluées ;
	Surfacturation des séjours (établissements de soins) ;
	Usurpation de compte / d'identité ;
	Utilisation abusive d'informations confidentielles ;
	Utilisation frauduleuse de la carte de sécurité sociale d'une autre personne (usurpation d'identité) ;
	Versement de pots de vin et dessous de table ;
	Vol d'actifs financiers (par exemple caisse, chèques) ;
	Vol de données ;
	Vol de mots de passe ;
	Etc.

B) Activités de support

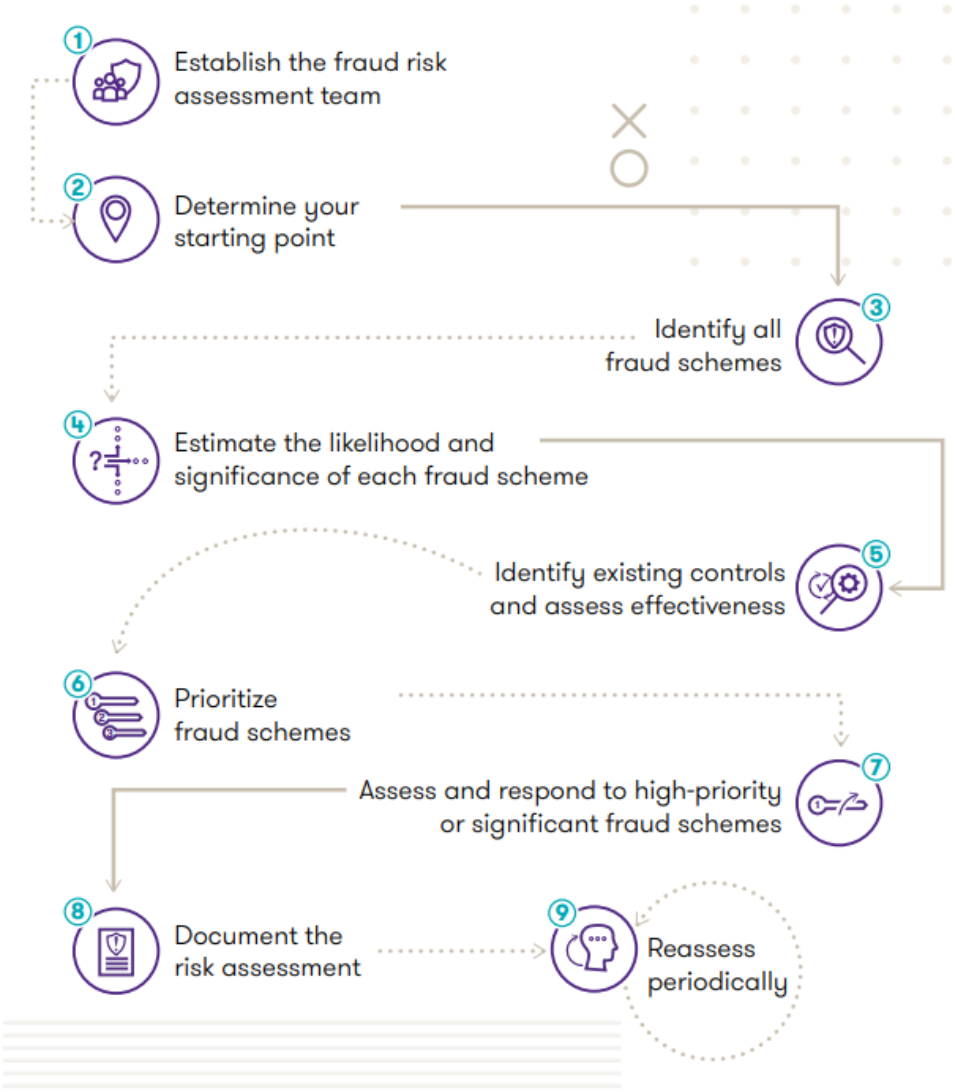
	Intitulé du risque
Fraudes et abus internes	Abus d'arrêts de travail ;
	Abus de pouvoir ;
	Acceptation de cadeaux illicites ;
	Acceptation de pots de vin et dessous de table ;
	Achats disproportionnés par rapport aux besoins ;
	Achats et réceptions non autorisés ;
	Achats fictifs ;
	Achats personnels ;
	Altération des bons de commandes ;
	Annulation de créances ;
	Appropriation d'actifs physiques ;
	Attribution de prestations fictives par un collaborateur ;
	Communication de fausses informations (internes/externes) ;
	Communication de fausses références professionnelles ;
	Comptabilisation de fausses créances et remboursements ;
	Conflits d'intérêts (processus achats, recrutement, etc.) ;
	Corruption active ou passive ;
	Création d'employés fictifs (fantômes) ;
	Création de fausses factures ;
	Création de fausses instructions de paiements ;
	Création de fournisseurs fictifs ;
	Création interne de faux dossiers ;
	Décalage ou omissions d'enregistrements comptables ;
	Demande de paiement pour de fausses factures de fournisseurs fictifs ou fournisseurs existants ;
	Destruction malveillante de biens ;
	Détournement de créances ;
	Détournement de paiements entrants ;
	Détournement de salaires ;
	Détournement par annulation de créances ;
	Dissimulation de paiements entrants ;
	Dissimulation de passifs ou de dépenses ;
	Divulgation d'informations confidentielles ;
	Double paiement / erreur de paiement ;
	Encaissements non comptabilisés ;
	Endossement frauduleux de chèques ;
	Ententes (par exemple fournisseurs) ;
	Falsification de documents (par exemple factures, notes de crédit, contrats) ;
	Falsification de documents en vue d'obtenir une autorisation de paiement ;
	Falsification de signatures ;
	Falsification des états financiers ;
	Falsification des heures supplémentaires ;
	Fausses classifications de frais ;
	Fausses déclarations intentionnelles ;
	Fausses évaluations d'actifs ;
	Fausses notes de frais ;
	Favoritisme vis-à-vis d'un fournisseur ;
	Frais fictifs ;
	Malveillance informatique (par exemple virus, destruction de fichiers, piratage) ;
	Malversations ;
	Manipulation des appels d'offres ;

	Modification de salaires / points indiciaires dans le logiciel de paie ;
	Modification du bénéficiaire d'une prestation ;
	Modification frauduleuse des accès et profils utilisateurs dans les systèmes d'information ;
	Modification frauduleuse des coordonnées de paiement dans un dossier existant (par exemple fournisseurs, employés) ;
	Omissions intentionnelles (par exemple manipulation des appels d'offres, non-paiement d'une biennale) ;
	Prestations de biens et services sur ou sous-évaluées ;
	Remboursements frauduleux multiples ;
	Remboursements indus sur le compte bancaire d'un proche ;
	Report d'échéances de créances ;
	Sur ou sous-évaluation d'actifs ou de recettes ;
	Sur-évaluation de frais ;
	Usurpation de compte / d'identité ;
	Utilisation abusive d'informations confidentielles ;
	Utilisation abusive des actifs physiques mis à disposition dans le cadre des activités professionnelles ;
	Utilisation du profil d'un autre utilisateur pour réaliser des transactions frauduleuses dans les systèmes d'information (usurpation d'identité) ;
	Utilisation non autorisée d'actifs physiques ;
	Vol d'actifs financiers (par exemple caisse) ;
	Vol d'actifs physiques ;
	Vol de données ;
	Vol de mots de passe pour effectuer des transactions dans les systèmes de paiements ;
	Vol de stocks ;
	Etc.
Fraudes et abus externes	Abus de pouvoir (ou de position dominante) ;
	Altération des bons de livraison ;
	Attribution de cadeaux illicites ;
	Blanchiment d'argent ;
	Communication de fausses informations (internes/externes) ;
	Communication de fausses références professionnelles ;
	Conflits d'intérêts (par exemple processus achats, recrutement) ;
	Corruption active ou passive de collaborateurs ;
	Création de fausses factures ;
	Divulgation d'informations confidentielles ;
	Double facturation / erreur de facturation ;
	Facturation frauduleuse de prestations / travaux ;
	Facturation répétée de prestations de service non délivrées ;
	Falsification de documents ;
	Falsification de documents en vue d'obtenir une autorisation de Paiement ;
	Falsification de prix ;
	Falsification de signatures ;
	Fausses déclarations (par exemple dossier d'appels d'offres) ;
	Fausses déclarations intentionnelles ;
	Favoritisme ;
	Fraude au président ;
	Malveillance informatique (par exemple virus, destruction de fichiers, piratage) ;
	Modification frauduleuse des accès et profils utilisateurs dans les systèmes d'information ;
	Modification frauduleuse des coordonnées de paiement (usurpation de compte) ;
	Non-respect des règles de facturation ;
	Omissions intentionnelles (par exemple rétention d'informations) ;
	Prestations sur ou sous-évaluées ;
	Usurpation de compte / d'identité ;
	Utilisation abusive d'informations confidentielles ;
	Ventes non autorisées ;
	Versement de pots de vin et dessous de table ;

	Vol d’actifs financiers ;
	Vol d’actifs physiques ;
	Vol de données ;
	Vol de mots de passe pour effectuer des transactions dans les systèmes de paiements ;
	Etc.

Annexe 5 – Étapes pour l'identification et l'évaluation des risques d'abus et de fraudes[98]

FIG. 6 Steps of a Fraud Risk Assessment



[98] ACFE, Grant Thornton (2020), *Anti-fraud playbook - The best defense is a good offense*, pages 19 et 20

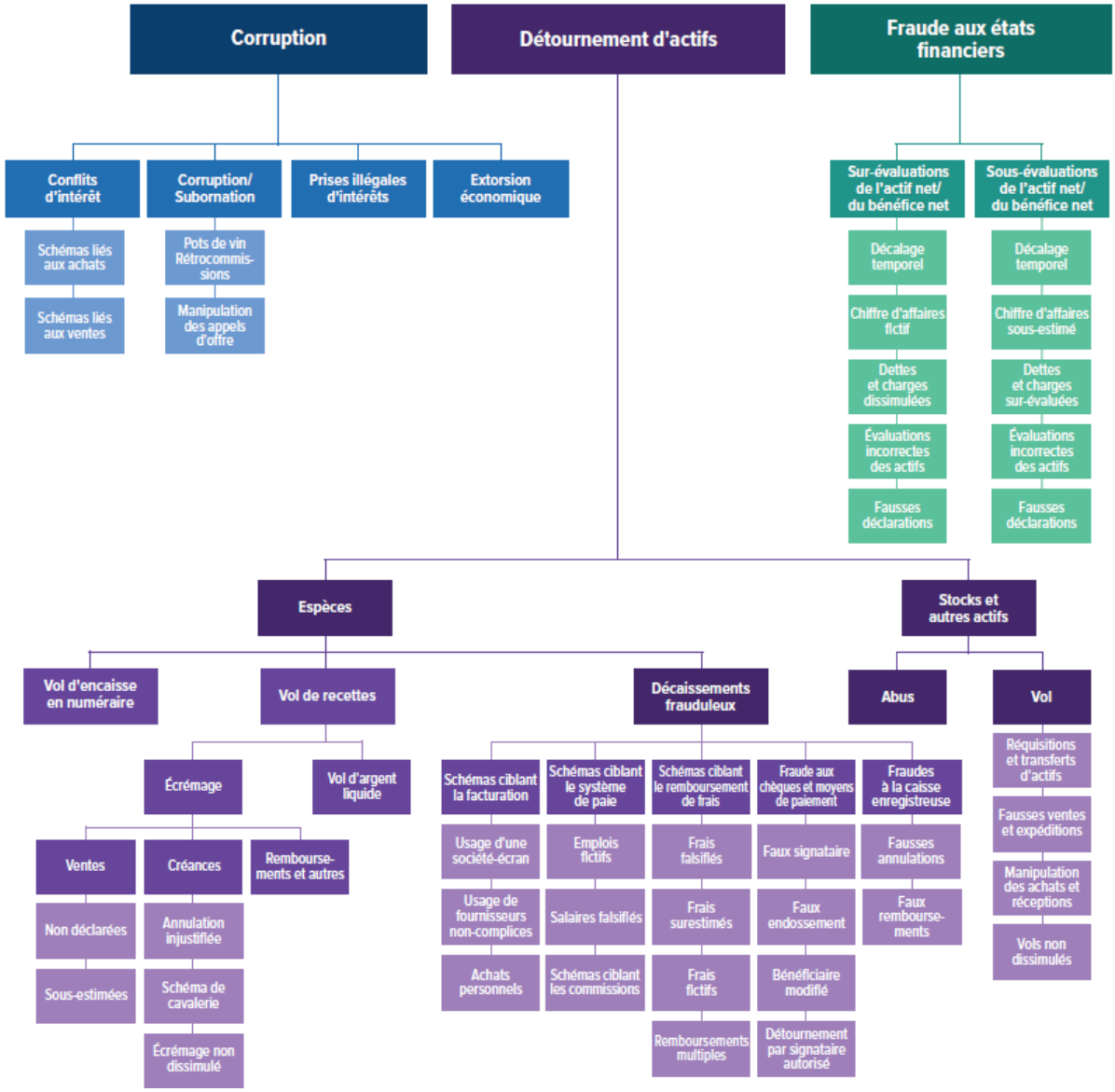
The following table outlines several of the Guide's points of focus related to the fraud risk assessment principle.[5] The points of focus detailed in this table *do not* include those that apply to the identification of fraud risks. (For other points of focus related to fraud risk assessment, see Play 3.) You will also find key questions and a checklist, intended to help your organization conduct a comprehensive fraud risk assessment, in line with the Guide's leading practices and guidance.[6]

Points of focus	Key questions
• Involves appropriate levels of management • Estimates the likelihood and significance of risks identified • Identifies existing fraud control activities and assesses their effectiveness • Determines how to respond to risks • Uses data analytics techniques for fraud risk assessment and fraud risk responses • Performs periodic reassessments and assesses changes to fraud risk • Documents the risk assessment	• Who will be on your fraud risk assessment team? What are their roles and responsibilities? • Where do you want to start your fraud risk assessment? • Does your organization leverage a likelihood and impact scale for other risk assessment efforts that you can leverage for assessing fraud risk? If not, how do you plan to develop those scales? • How will you educate stakeholders on the fraud risk assessment process to ensure understanding of key terms and procedures? • How will you document and evaluate existing fraud controls throughout the assessment process? • What factors should you consider when prioritizing fraud risks? Will this be based solely on likelihood and impact scores, or will other information be considered? • How will you respond to high-priority risks identified? How can you leverage your roadmap and strategy (see Play 1) to inform this process? • How often will you perform a fraud risk assessment? What changes will initiate a reassessment?

Annexe 6 – Exemples de catégorisations des risques d'abus et de fraudes

A) Classification des fraudes internes et abus professionnels (l'arbre de la fraude) de l'Association of Certified Fraud Examiners[99]

FIG. 3 **Classification des fraudes internes et abus professionnels (*l'arbre de la fraude*)**[3]



[99] ACFE (2020), *Report to the Nations. 2020 Étude mondiale sur la fraude interne et les abus professionnels*, page 11

B) Catégorisation des risques de fraudes de l'Institut français de l'audit et du contrôle internes (IFACI)[100]

Niveau 1	Famille	Définition Risques Niveau 1	Niveau 2	Risques Niveau 2	Définition Risque de Niveau 2	Niveau 3	Risques Niveau 3	Définition Risques Niveau 3
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R306	Fraude interne	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne	R30601	Activité non autorisée - Dissimulation volontaire de position	Dissimulation volontaire de position
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R306	Fraude interne	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne	R30602	Activité non autorisée - Transactions non notifiées	Transactions intentionnellement non notifiées
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R306	Fraude interne	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne	R30603	Activité non autorisée - Abus de pouvoir	Abus de pouvoir, activité intentionnelle non autorisée
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R306	Fraude interne	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne	R30604	Activité non autorisée - Fausses déclarations	Fausses déclarations intentionnelles
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R306	Fraude interne	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne	R30606	Vol et fraude - Vol / détournement de fonds	Vol / détournement de fonds
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R306	Fraude interne	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne	R30607	Vol et fraude - Vol / détournement de biens	Vol / détournement de biens
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R306	Fraude interne	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne	R30608	Vol et fraude - Contrefaçon de documents	Contrefaçon de documents
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou	R306	Fraude interne	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une	R30609	Vol et fraude - Usurpation de compte / d'identité	Usurpation de compte / d'identité
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R306	Fraude interne	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne	R30610	Vol et fraude - Fraude fiscale	Fraude fiscale / évasion délibérée

[100] Extraits issus de :
IFACI (2013), *La cartographie des risques, Cahier de la Recherche*, pages 98 à 103

Niveau 1	Famille	Définition Risques Niveau 1	Niveau 2	Risques Niveau 2	Définition Risque de Niveau 2	Niveau 3	Risques Niveau 3	Définition Risques Niveau 3
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R306	Fraude interne	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne	R30605	Vol et fraude - Autre	Autres fraudes internes
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R306	Fraude interne	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne	R30611	Vol et fraude - Délits d'initiés	Non-respect des règles en matière d'opérations financières personnelles / délits d'initiés
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R306	Fraude interne	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne	R30612	Vol et fraude - Cadeaux et invitations	Non-respect des règles déontologiques relatives aux cadeaux et aux invitations
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R306	Fraude interne	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne	R30613	Sécurité des systèmes - Malveillance informatique	Malveillance informatique (virus, destruction de fichiers, piratages, etc.)
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R306	Fraude interne	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne	R30614	Sécurité des systèmes - Données	Vol et divulgation de données
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R306	Fraude interne	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne	R30615	Vol et fraude - Abus de biens sociaux	Risque de faire usage sciemment de biens, du crédit de la société, ou des pouvoirs possédés par des dirigeants sociaux (droits reconnus par la Loi ou les statuts aux dirigeants sociaux) contraire aux intérêts de la société et dans un intérêt personnel, intérêt du dirigeant social, des membres de sa famille, de ses proches
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R307	Fraude externe	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles par une tierce partie	R30701	Vol et fraude - Fausses déclarations	Fausses déclarations intentionnelles
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R307	Fraude externe	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles par une tierce partie	R30702	Vol et fraude - Contrefaçon de documents	Contrefaçon de documents
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R307	Fraude externe	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles par une tierce partie	R30703	Vol et fraude - Vol	Vol

Niveau 1	Famille	Définition Risques Niveau 1	Niveau 2	Risques Niveau 2	Définition Risque de Niveau 2	Niveau 3	Risques Niveau 3	Définition Risques Niveau 3
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R307	Fraude externe	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles par une tierce partie	R30704	Vol et fraude - Autre	Autres fraudes externes
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R307	Fraude externe	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles par une tierce partie	R30705	Vol et fraude - Usurpation de compte / d'identité	Usurpation de compte / d'identité
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R307	Fraude externe	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles par une tierce partie	R30706	Sécurité des systèmes - Malveillance informatique	Malveillance informatique (virus, destruction de fichiers, piratages, etc.)
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R307	Fraude externe	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles par une tierce partie	R30707	Sécurité des systèmes - Données	Vol et divulgation de données
R3	Opérationnels	Risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs	R307	Fraude externe	Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'infractions à la législation ou aux règles par une tierce partie	R30708	Risques de corruption	Risques de corruption active ou passive de membres du personnel, de commerciaux mandataires, salariés ou indépendants (courtiers)

Annexe 7 – Bonnes pratiques en matière de formation anti-fraude[101]

As you develop your targeted and role-based anti-fraud training program, consider the best practices shown in Figure 8:

FIG. 8 Training Best Practices

[101] ACFE, Grant Thornton (2020), *Anti-fraud playbook - The best defense is a good offense*, page 27

Annexe 8 – Exemples de contrôles anti-fraude[102]

[102] IIA (2021), *OECD Global Anti-corruption & Integrity Forum, Webinar on Accountability, Actions and Assurance in Fighting Fraud*, page 6

Annexe 9 – Exemples de techniques analytiques

A) Outils et techniques analytiques suggérés par CGMA[103]

Identifying anomalies

Background reading

- It is important to keep up to date with fraud trends and issues through the press, technical journals, books and the internet.

Risk assessment

- Undertake a fraud risk assessment and design specific tests to detect the significant potential frauds identified through the risk assessment. Act on irregularities which raise concern.

Benchmarking

- Comparisons of one financial period with another; or the performance of one cost centre, or business unit, with another; or of overall business performance with industry standards, can all highlight anomalies worthy of further investigation.

Systems analysis

- It is important to examine the systems in place and identify any weaknesses that could be opportunities for the fraudster.

Ratio analysis

- Can be used to identify any abnormal trends or patterns.

Mathematical modelling

- Using the 'sort' tool on a spreadsheet can help to identify patterns in expenditure etc. There are also specialist mathematical models such as Benford's Law, a formula which can help identify irregularities in accounts. Database modelling can also be used.

Specialist software

- Such as audit tools for data matching analysis can prove very useful. Other tools allow for analysis such as real time transaction assessment, targeted post-transactional review, or strategic analysis of management accounts.

Exception reporting

- Many systems can generate automatic reports for results that fall outside predetermined threshold values (exceptions), enabling immediate identification of results deviating from the norm. Emails or text alerts can be sent directly to appropriate managers to follow up.

[103] CGMA (2012), *Report Fraud risk management - A guide to good practice*, page 17

B) Contrôles détectifs suggérés par l'IIA en matière de fraude[104]

GTAG — Fraud Detection Using Data Analysis

Type of Fraud	Tests Used to Discover This Fraud
Fictitious vendors	• Run checks to uncover post office boxes used as addresses and to find any matches between vendor and employee addresses and/or phone numbers. • Be alert for vendors with similar sounding names or more than one vendor with the same address and phone number.
Altered invoices	• Search for duplicates. • Check for invoice amounts that do not match contracts or purchase order amounts.
Fixed bidding	• Summarize contract amount by vendor, and compare vendor summaries for several years to determine whether a single vendor is winning most bids. • Calculate days between close for bids and contract submission date by vendor to see whether the last bidder consistently wins the contract.
Goods not received	• Search for purchase quantities that do not agree with contract quantities. • Check whether inventory levels are changing in relation to supposed delivery of goods.
Duplicate invoices	• Review for duplicate invoice numbers, duplicate dates, and duplicate invoice amounts.
Inflated prices	• Compare prices across vendors to see whether prices from a particular vendor are unreasonably high.
Excess quantities purchased	• Review for unexplained increases in inventory. • Determine whether purchase quantities of raw materials are appropriate for production level. • Check to see whether increases in quantities ordered compare similarly to previous contracts or years or compare to other plants.
Duplicate payments	• Search for identical invoice numbers and payment amounts. • Check for recurring requests for refunds for invoices paid twice.
Carbon copies	• Search for duplicates within all company checks cashed. • Conduct a second search for gaps in check numbers.
Duplicate serial numbers	• Determine whether high-value equipment a company already owns is being repurchased by checking for duplicate serial numbers and for the involvement of the same personnel in both purchasing and shipping processes.
Payroll fraud	• Check whether a terminated employee is still on payroll by comparing the date of termination with the pay period covered by the paycheck, and extract all pay transactions for departure date less than the date of the current pay period.
Accounts payable	• Find transactions that do not match contract amounts by linking accounts payable files to contract and inventory files and examining contract date, price, ordered quantity, inventory receipt quantity, invoice quantity, and payment amount by contract.

[104] IIA (2009), *Global Technology Audit Guide (GTAG) 13 - Fraud Prevention and Detection in an Automated World*, page 10

Annexe 10 – Exemples de procédures et de processus de signalement

A) CGMA (2012), Report Fraud Risk Management - A guide to good practice[105]

Appendix 4

Sample whistle-blowing policy.

Introduction

This whistle-blowing policy provides a procedure which enables employees to raise concerns about what is happening at work, particularly where those concerns relates to unlawful conduct, financial malpractice or dangers to the public or the environment. The objective of this policy is to ensure that concerns are raised and dealt with at an early stage and in an appropriate manner.

This organisation is committed to its whistle-blowing policy. If an employee raises a genuine concern under this policy, he or she will not be at risk of losing their job, nor will they suffer any form of detriment as a result. As long as the employee is acting in good faith and in accordance with this policy, it does not matter if he or she is mistaken.

How the whistle-blowing policy differs from the grievance procedure

This policy does not apply to raising grievances about an employee's personal situation. These types of concern are covered by the organisation's grievance procedure. The whistle-blowing policy is primarily concerned with situations where the interests of others or the organisation are at risk. It may be difficult to decide whether a particular concern should be raised under the whistle-blowing policy or under the grievance procedure or both. If an employee has any doubt as to the correct route to follow, this organisation encourages the concern to be raised under this policy and will decide how the concern should be dealt with.

Protecting the employee

This organisation will not tolerate harassment or victimisation of anyone raising a genuine concern under the whistle-blowing policy. If an employee requests that their identity be protected, all possible steps will be taken to prevent the employee's identity becoming known. If the situation arises where it is not possible to resolve the concern without revealing the employee's identity (eg if the employee's evidence is needed in a court of law), the best way to proceed with the matter will be discussed with the employee. Employees may submit reports anonymously, but should be aware that doing so, it will be more difficult for the organisation to investigate them, to protect the employee and to give the employee feedback.

How the matter will be handled

Once an employee has informed the organisation of his or her concern, these will be examined and the organisation will assess what action should be taken. This may involve an internal enquiry or a more formal investigation. The employee will be advised who is handling the matter, how they can contact him/her and whether any further assistance may be needed. If the employee has any personal interest in the matter, this should be declared at the outset. If the employee's concern falls more properly within the grievance procedure, then they will be advised of this.

[105] CGMA (2012), *Report Fraud Risk Management - A guide to good practice*, pages 29 et 30

How to raise a concern internally

Step 1

If an employee has a concern about malpractice, he or she should consider raising it initially with their line manager. This may be done orally or in writing. An employee should specify from the outset if they wish the matter to be treated in confidence so that appropriate arrangements can be made.

Alternatively, employees can call the 24 hour whistle-blowing telephone hotline. This service is strictly confidential and callers will not be asked to give their name if they do not wish to do so.

Step 2

If these channels have been followed and the employee still has concerns, or feels that they are unable to raise the issue with their line manager, for whatever reason, they should address their concerns to their head of department, the head of human resources or the chief internal auditor [OR INSERT OTHER APPROPRIATE NOMINATED POINTS OF CONTACT HERE].

Anonymous reports

These may be made verbally to the 24 hour whistle-blowing telephone hotline or in writing to [INSERT NOMINATED POINT OF CONTACT SUCH AS HEAD OF HUMAN RESOURCES OR CHIEF INTERNAL AUDITOR].
The submission should be clearly marked 'Confidential: anonymous employee submission'.

Independent advice

If an employee is unsure whether to use this procedure, to report the matter externally to regulators/ law enforcement authorities or simply wants independent advice at any stage, they may contact
[INSERT EXTERNAL CONTACT IF APPLICABLE – IN SOME JURISDICTIONS, THERE ARE ORGANISATIONS WHICH CAN PROVIDE FREE CONFIDENTIAL ADVICE TO EMPLOYEES ABOUT MALPRACTICE AT WORK.]
An employee can also seek advice from a lawyer of their own choice at their own expense.

Matters raised maliciously

Employees who are found to raise a matter maliciously that they know to be false, will be subject to the organisation's disciplinary policy.

B) Groupe Gorgé[106]

2. COMMENT LANCER UNE ALERTE

2.1 PROCEDURE D'ALERTE PAR PALIERS

La Loi Sapin 2 prévoit une **procédure d'alerte graduée, en deux paliers** :

- En premier lieu, le Collaborateur doit porter l'alerte à la connaissance de son supérieur hiérarchique, ou de son employeur, ou utiliser l'adresse mail du/des Référent(s), ou un autre canal de signalement existant au sein de son entreprise ;
- En second lieu, il peut a dresser son alerte à des tiers en cas de non traitement de son alerte dans des délais raisonnables ou d'urgence caractérisée.

> *La protection du lanceur d'alerte salarié du groupe dépend notamment du respect de cette procédure graduée.*

2.1.1 SIGNALEMENT AU REFERENT INTERNE

En sus des autres canaux de signalement susceptibles d'exister au sein de chaque filiale, le lanceur d'alerte adresse son signalement aux Référents internes désignés par le groupe, joignable à l'adresse email suivante :

compliance@groupe-gorge.com

Cette adresse mail n'est consultable que par les Référents de Groupe Gorgé[5].

Avant de lancer une alerte, chaque Collaborateur pourra – s'il le souhaite – s'adresser à son supérieur hiérarchique ou à toute personne visée dans les points de contact du Code de conduite anti-corruption du groupe ou de sa filiale, ce dernier ayant pour devoir de l'orienter et le conseiller.

2.1.2 SECOND PALIER D'ALERTE

a) A défaut de traitement de son alerte dans un délai raisonnable, le Collaborateur pourra saisir les autorités administratives, judiciaires ou un ordre professionnel ;
b) A défaut de traitement dans un délai de 3 mois du signalement par l'un des organismes saisis, le signalement pourra être rendu public.
c) En cas de danger grave et imminent ou en présence d'un risque de dommages irréversibles (sur la santé, l'environnement, etc), le signalement peut être adressé directement à l'autorité judiciaire, à l'autorité administrative ou aux ordres professionnels. Il peut également être rendu public.

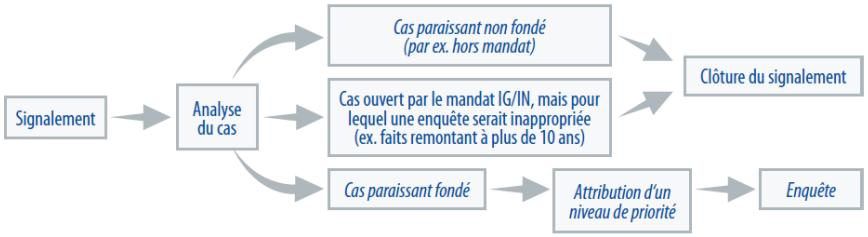
[106] Groupe Gorgé (2019), *Dispositif d'alerte interne,* pages 5 et 6

C) Banque européenne d'investissement

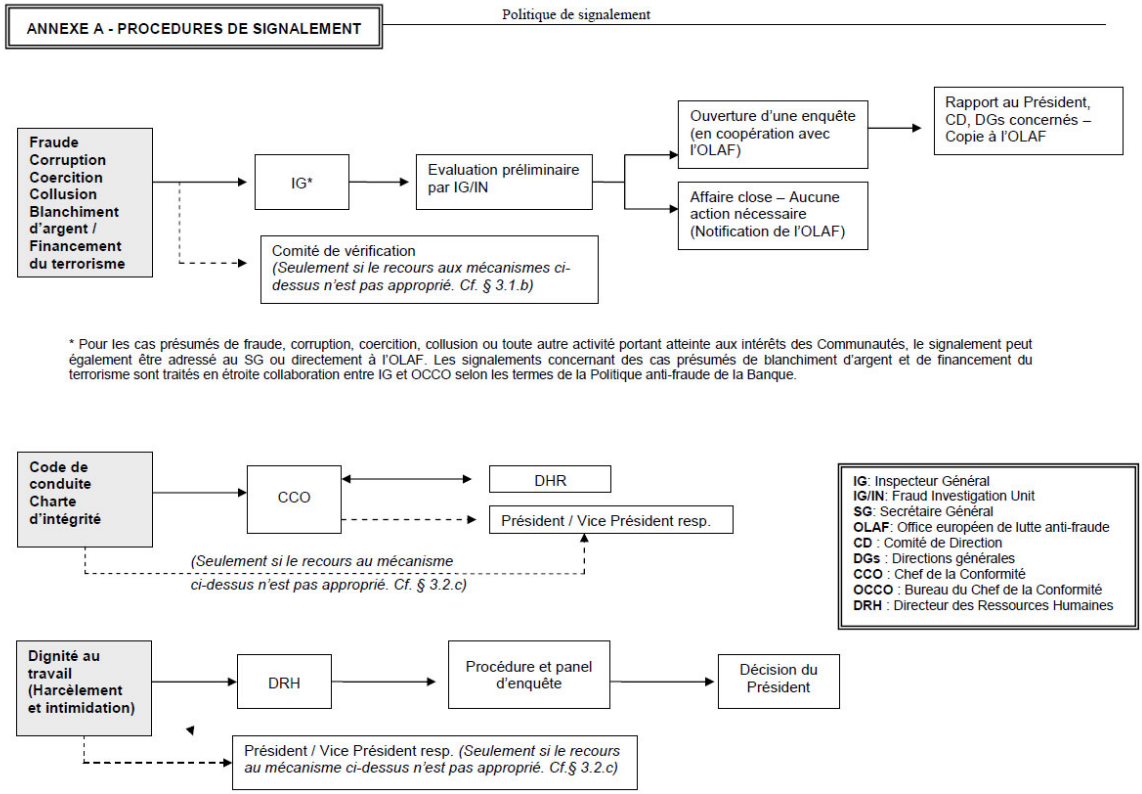
Exemple 1[107]

Analyse des cas faisant l'objet d'un signalement et enquêtes

Avant qu'une enquête soit ouverte, chaque signalement est **analysé** afin de déterminer sa crédibilité et sa source et décider si le cas relève du mandat d'IG/IN et si l'ouverture d'une enquête est la mesure la plus appropriée. Afin d'assurer que les **ressources** allouées aux enquêtes sont utilisées de la manière la plus efficace et la plus efficiente possible, un niveau de priorité est attribué à chaque cas.



Exemple 2[108]



Exemple 3[109]

(C) Procédure de signalement

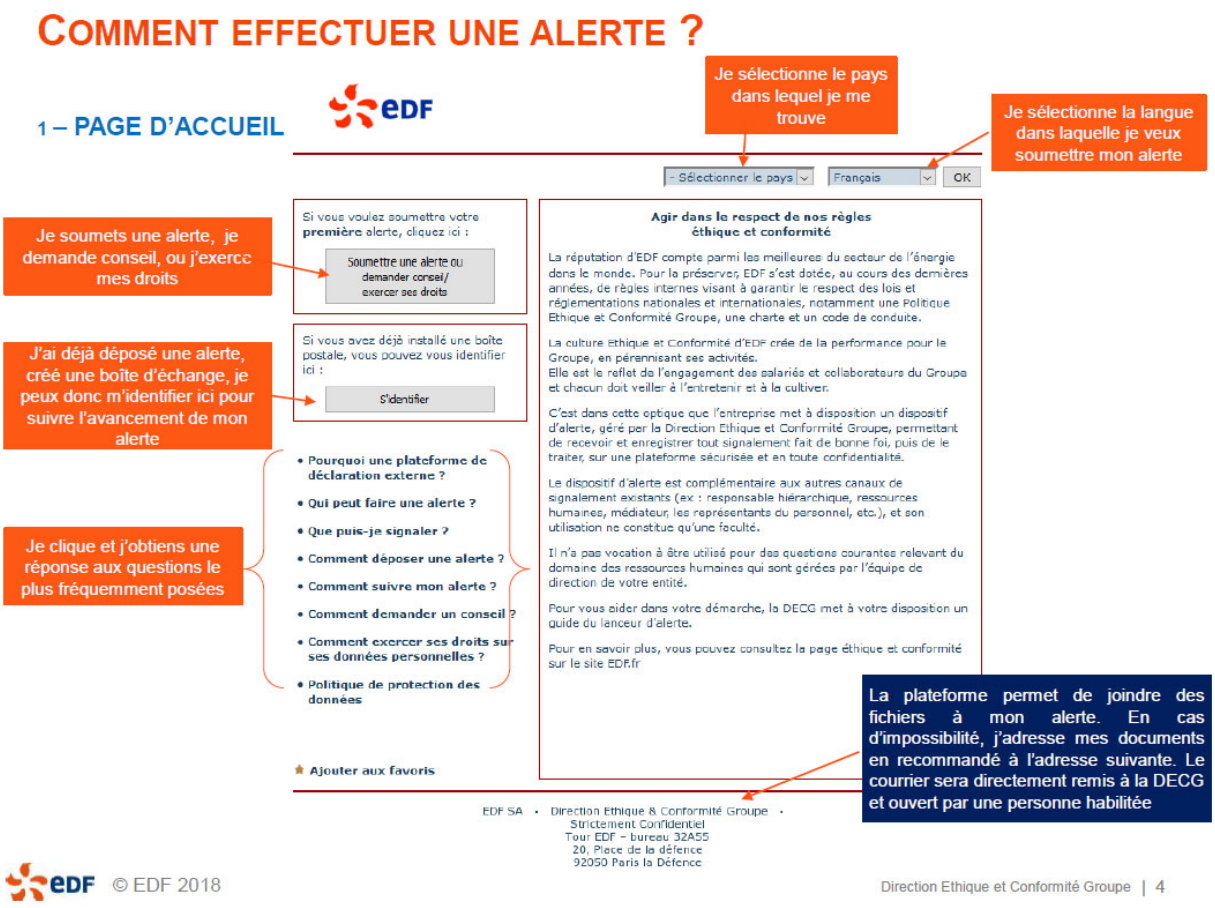
41. En vertu de la politique en vigueur, tous les cas présumés de manœuvre interdite constatés par des agents de la BEI, des contreparties, des partenaires en affaires, des membres du public (y compris des membres de la société civile) ou des tiers associés à ses projets doivent être signalés à la division Enquête sur les fraudes de la BEI qui accusera réception du signalement qui peut être transmis :
    - par courrier[17] ;
    - par courriel adressé à : investigations@eib.org
    - au moyen du formulaire en ligne disponible sur le site Web de la BEI[18] ;
    - par téléphone : +352 4379-87441 ou bien
    - par fax (+352 4379 64 000).[19]

[107] BEI (2017), *Lutte contre la fraude et la corruption dans le cadre des opérations dans la BEI*, page 3

[108] BEI (2009), *Politique de signalement*, page 9.

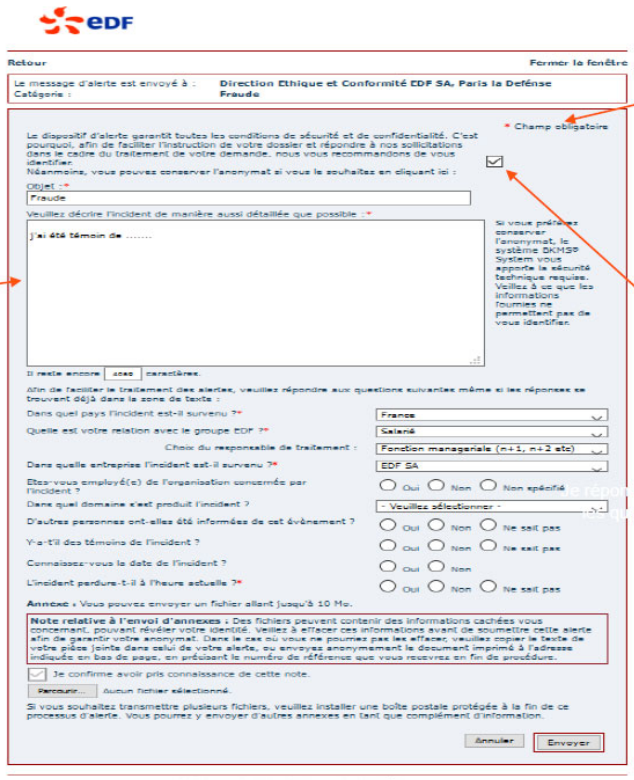
[109] BEI (2013), *Politique antifraude de la BEI*, page 10

Annexe 11 – Exemple d'un canal de signalement[110]



[110] EDF (2018), *Dispositif d'alerte éthique et conformité. Tutoriel d'utilisation « Comment saisir une alerte ou une demande dans le Dispositif »*

4 – DESCRIPTION DE L'ALERTE (1/2)

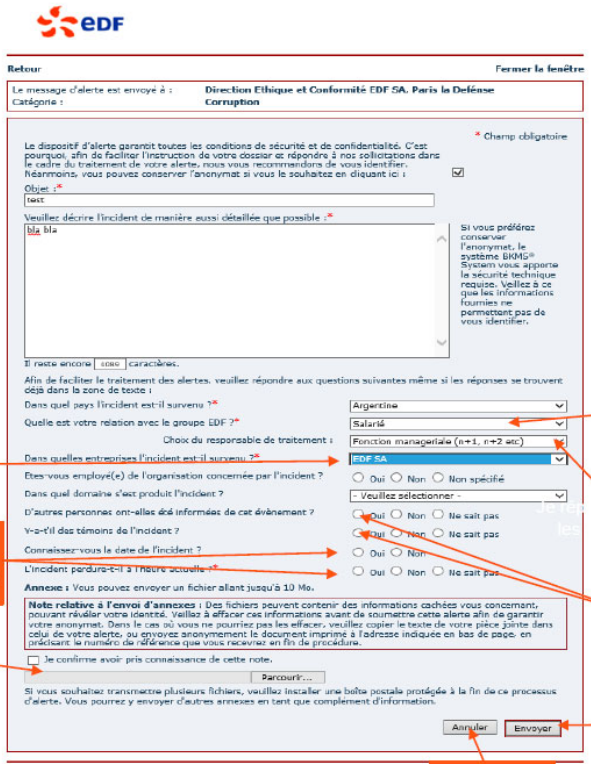


Les champs avec * doivent obligatoirement être complétés

Je décris de bonne foi les faits que je souhaite signaler

Le dispositif d'alerte garantit toutes les conditions de sécurité et de confidentialité. C'est pourquoi, afin de faciliter l'instruction de mon dossier il est recommandé de m'identifier.
Si je souhaite toutefois garder l'anonymat, je coche cette case. La DECG pourra demander la levée de l'anonymat si la poursuite du traitement est rendue impossible par cet anonymat

4 – DESCRIPTION DE L'ALERTE (2/2)



J'indique ici mon lien avec l'entreprise (salarié, intérimaire, stagiaire, externe, etc)

Je précise dans quelle entreprise a eu lieu l'incident

Si je suis un collaborateur de l'entreprise, j'indique ma préférence sur la fonction qui sera chargée du traitement de mon alerte

Si je le peux, je précise la date de l'incident ou la période pendant laquelle il est intervenu et je précise s'il dure encore

Si je peux, je précise si d'autres personnes ont été informées ou témoins de l'incident

Je peux joindre ici un fichier

Je clique sur « envoyer » pour enregistrer mon alerte

Je peux annuler mon alerte

Annexe 12 – Exemple de documentation des cas d'abus et de fraudes détectés[111]

Fraud Investigations and Corrective Actions Taken											
Case Tracking Number	Description of Allegation	Source	Date Received	Resolution Responsibility Assigned To:	Date Investigation Completed	Recommended Disposition	Recommendations Reported To:	Date Reported	Resolution Decisions Reached	Date Matter Closed	Was Source Informed of Outcome?

[111] ACFE (2023), *Fraud risk management tool :* https://www.acfe.com/fraud-resources/fraud-risk-tools---coso/tools

Annexe 13 – Exemples de feuille et de fiche d'analyse du soupçon de fraude

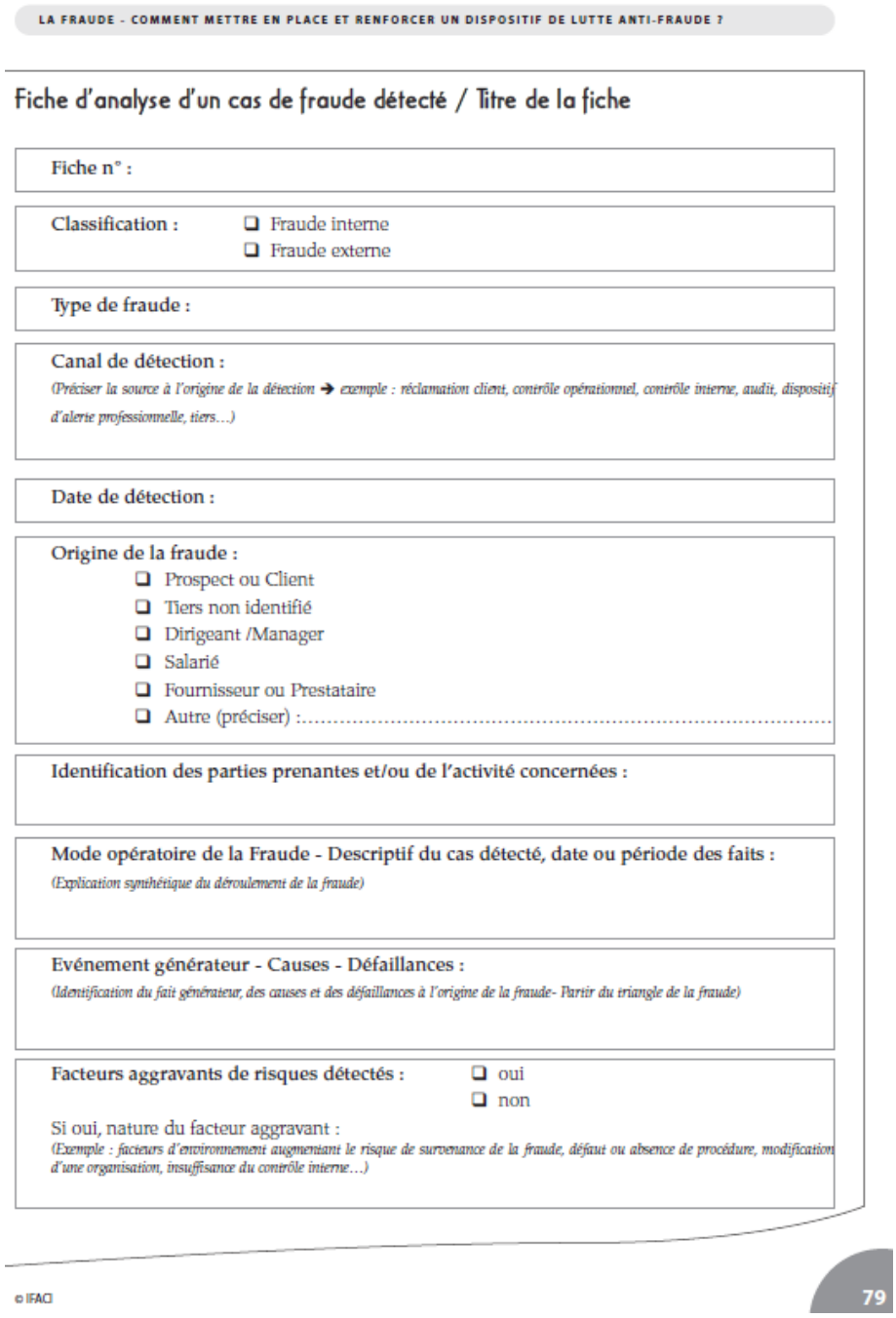
A) Feuille d'analyse du soupçon de fraude en phase de pré-investigation[112]

Feuille d'analyse du soupçon de fraude en phase de pré-investigation :

Principaux constats et analyse concernant le soupçon de fraude	• Commentaires détaillés sur la nature de la découverte. • Analyse du soupçon de fraude. • Analyse du processus. • Date, historique, évaluation de la matérialité, analyse de la cohérence des faits, etc. • Identifier les parties prenantes (initialiser un logigramme).
Identification des points non éclaircis	• Identification des « zones d'ombres ». • Incompréhension de certains faits et motifs.
Mesure des risques, des enjeux et des conséquences	• Identifications des risques majeurs. • Identification des risques mineurs (ils peuvent révéler des failles à maîtriser ; la répétition de l'incident peut en faire des risques majeurs). • Premières évaluations du ou des préjudices.
Identification des motivations des éventuels fraudeurs	• Identifier les liens entre les personnes. • Comprendre le rôle de chacun.
Principales actions proposées ou déjà mises en œuvre par rapport à ce soupçon de fraude	• Actions mises en œuvre en urgence pour neutraliser les risques perçus. • Actions proposées pour mise en œuvre ultérieure.
Evaluation de la consistance d'un soupçon de fraude	• Résultat de la simulation du soupçon de fraude. • Premières conclusions. • Premiers axes de recherche à mettre en place pour compléter les informations sur le soupçon de fraude. • Identification des besoins.

[112] IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*, pages 44 et 45

B) Fiche d'analyse d'un cas de fraude détecté[113]



LA FRAUDE - COMMENT METTRE EN PLACE ET RENFORCER UN DISPOSITIF DE LUTTE ANTI-FRAUDE ?

Fiche d'analyse d'un cas de fraude détecté / Titre de la fiche

Fiche n° :

Classification : ❑ Fraude interne ❑ Fraude externe

Type de fraude :

Canal de détection :
(Préciser la source à l'origine de la détection ➔ exemple : réclamation client, contrôle opérationnel, contrôle interne, audit, dispositif d'alerte professionnelle, tiers…)

Date de détection :

Origine de la fraude :
- ❑ Prospect ou Client
- ❑ Tiers non identifié
- ❑ Dirigeant /Manager
- ❑ Salarié
- ❑ Fournisseur ou Prestataire
- ❑ Autre (préciser) :……

Identification des parties prenantes et/ou de l'activité concernées :

Mode opératoire de la Fraude - Descriptif du cas détecté, date ou période des faits :
(Explication synthétique du déroulement de la fraude)

Evénement générateur - Causes - Défaillances :
(Identification du fait générateur, des causes et des défaillances à l'origine de la fraude- Partir du triangle de la fraude)

Facteurs aggravants de risques détectés : ❑ oui ❑ non

Si oui, nature du facteur aggravant :
(Exemple : facteurs d'environnement augmentant le risque de survenance de la fraude, défaut ou absence de procédure, modification d'une organisation, insuffisance du contrôle interne…)

[113] IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche*, pages 79 à 81

Détermination du « Qui fait quoi » en fonction du point précédent :
➔ 3 axes : détection – prévention – contrôle

1- Actions au niveau opérationnel (1er niveau) :
(Quels peuvent être les travaux et les mesures à mettre en œuvre au niveau opérationnel ?)

2- Actions au niveau du contrôle permanent (2ème niveau) :
(Quels peuvent être les travaux et les mesures à mettre en œuvre au niveau du contrôle permanent ?)

3- Actions au niveau de l'audit (3ème niveau) :
(Quels peuvent être les travaux de l'audit, en vue de s'assurer sinon de l'absence de fraude, du moins de l'existence d'un contrôle interne robuste diminuant le risque de fraude ?)

4- Actions par d'autres intervenants (A préciser) :
(selon le niveau de compétences et d'expertise requis)

Suivi des actions *(Contrôle permanent et/ou Audit selon le cas)* :

Nom du rédacteur :

Date :
Signature :

Catégorie de fraude[1] **:**

- ❑ Conflits d'intérêts
- ❑ Commissions frauduleuses
- ❑ Cadeaux illicites
- ❑ Extorsions de fonds
- ❑ Informations financières frauduleuses
- ❑ Informations non financières frauduleuses
- ❑ Détournements d'actifs financiers
- ❑ Détournements d'actifs physiques
- ❑ Autre (préciser) : .....

Echelle d'impact *(Elle doit être cohérente avec d'autres échelles de risques utilisées dans l'organisation)* **:**

- ❑ Mineur
- ❑ Moyen
- ❑ Important
- ❑ Majeur
- ❑ Critique

Nature de l'impact :

- ❑ Pertes financières,
- ❑ Pertes de productivité
- ❑ Pertes commerciales (exemple nombre de clients affectés)
- ❑ Préjudice humain
- ❑ Préjudice réglementaire ou juridique
- ❑ Détérioration de l'image de marque
- ❑ Autre (préciser) : .....

Evaluation financière, si pertinente :

Perte brute : .....

% récupéré : .....

Perte nette : .....

Charges d'investigation : .....

Mesures correctrices envisagées : *(Exemple : modification d'un processus, actualisation du dispositif de contrôle a priori et/ou a posteriori, actualisation du dispositif de sécurité, sensibilisation du personnel…)*

- **Mesures préventives :** *vérifier que des actions sont entreprises en cas de fraude détectée (à posteriori) : recouvrement, procédure pénale ; la diffusion et l'utilisation de mode.*
- **Mesures détectives :** *comprenant les mesures classiques de contrôle interne (états d'alerte, analyse de données a posteriori) et aussi les indices qui peuvent être des signaux faibles.*

[1] *Catégories issues de l'arbre de la fraude, partie 1.2, p. 14*

Annexe 14 – Grille de diagnostic préalable : État des lieux du dispositif LAF[114]

Etat des lieux du dispositif anti-fraude : Que doit-on analyser en amont de toute action ?

	Incontournables	Pratiques observables	Criticité			Commentaires & illustrations
			Contributive	Souhaitable	Indispensable	
1	Une capacité d'anticipation et des responsabilités clairement définies au niveau de l'organisation ?					**Les rôles et responsabilités sont définis de manière appropriée par rapport à chaque organisation.** **L'organisation est proactive.** **Elle n'est pas uniquement en réaction par rapport à des cas avérés de fraude.**
		Un recensement des acteurs internes à mobiliser et une explication de leurs rôles respectifs dans le cadre du dispositif de lutte contre la fraude	X			Par exemple : métier, direction financière, direction juridique, resources humaines, système d'information, communication, etc.
		Une définition claire et partagée des rôles et des responsabilités des fonctions de contrôle interne par rapport à lutte contre la fraude	X			Selon les organisations, il peut s'agir de l'audit interne, de la direction de contrôle interne/contrôle permanent, de la conformité, de la direction des risques, de la sécurité financière, d'un service de lutte contre la fraude, etc.
		Des rôles pré-définis en matière de sensibilisation et de formation des collaborateurs	X			Un cadre général de réflexion qui intègre la formation de tous les acteurs.
		Une culture de décisions explicites et formalisées		X		La fraude n'est plus un sujet tabou.
		L'identification préalable des intervenants externes		X		Par exemple : les tutelles, les régulateurs, les CAC, l'équipe d'investigation externe, les assureurs, les autorités de police ou de justice.
		Un engagement officiel et visible de la direction générale concernant la lutte contre la fraude			X	Référence de documents ou minutes d'événements significatifs.
		Une structure hiérarchique organisée et connue de tous			X	Les gestionnaires sur le terrain savent à qui s'adresser et comment gérer les soupçons ou les cas avérés de fraude.

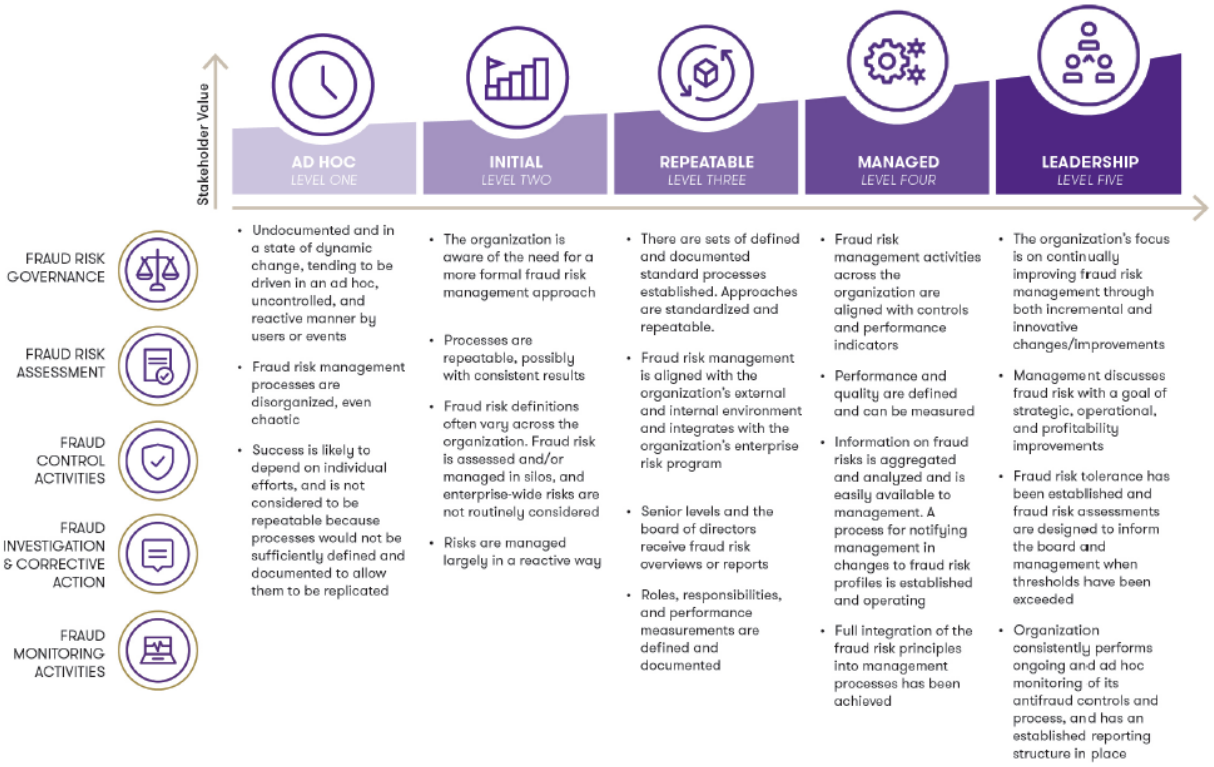
	Incontournables	Pratiques observables	Criticité			Commentaires & illustrations
			Contributive	Souhaitable	Indispensable	
2	Des organes de gouvernance impliqués et informés ?					**Le risque de fraude est suivi par les instances de direction et de gouvernance.**
		Le recours à une cellule de crise pour traiter des cas rencontrés est validé par les organes dirigeants.	X			Des scénarii de gestion de crise existent.
		Un comité spécialisé du conseil d'administration surveille le dispositif anti-fraude.	X			L'organe de gouvernance s'est saisi du risque de fraude et demande des informations sur ce sujet.
		Un membre du comité exécutif anime un comité éthique.	X			L'organisation a mené une réflexion sur l'éthique et s'est doté de moyens spécifiques.
		La gestion du risque de fraude est à l'ordre du jour des réunions du comité d'audit.		X		L'organe de gouvernance s'est saisi du risque de fraude et demande des informations sur ce sujet.
		La direction générale sponsorise la politique de lutte contre le rique de fraude.			X	Le directeur général ou l'un des membres du comité de direction a un mandat spécifique pour gérer le risque de fraude.
		Les opérationnels s'engagent à faire remonter tous les cas de fraude à leur hiérarchie.			X	Un élément important de la politique de gestion du risque de fraude dans le respect de la réglementation sur les données personnelles.

[114] IFACI (2010), *La fraude - Comment mettre en place et renforcer un dispositif de lutte anti-fraude ? Cahier de la Recherche,* Annexe 1, pages 84 à 94

	Incontournables	Pratiques observables	Criticité			Commentaires & illustrations
			Contributive	Souhaitable	Indispensable	
3	**Une politique anti-fraude formalisée est mise en œuvre ?** *(suite)*	Un reporting actualisé du traitement des cas en cours permet d'assurer un suivi, de construire une base de connaissance et d'alimenter des actions de prévention ou de détection.		X		Une cellule centrale est opératoire sur l'analyse des fraudes.
		Une politique anti-fraude est formalisée.			X	La gestion du risque de fraude peut comprendre notamment les définitions et conséquences, les principes et engagements de l'organisation, les rôles et responsabilités, les sanctions.
		La politique anti-fraude s'appuie sur une charte d'éthique ou un code de déontologie.			X	Le respect de la réputation des personnes et du droit sous-tend toutes les démarches entreprises, à chacune des étapes.
		Les principes de la politique et les procédures sont clairement accessibles à tous.			X	Cette diffusion s'appuie sur une communication et des formations internes appropriées.
		Un programme de lutte contre la fraude articulé, évolutif et planifié, est validé annuellement.			X	Ce programme doit être piloté avec la publication d'indicateurs clé d'avancement et d'efficacité, de rapports annuels présentés en Conseil d'administration et Comité d'audit.
		Les fraudes découvertes font l'objet d'une procédure de remontée/ escalade/ reporting formalisée aux instances de contrôle interne ?			X	Le respect de la réputation des personnes et du droit sous-tend toutes les démarches de l'organisation à chacune des étapes.

Annexe 15 – Grille de diagnostic pour l'évaluation de la maturité du dispositif LAF[115]

Appendix A: Enterprise Anti-Fraud Maturity Assessment Model©



[115] ACFE, Grant Thornton (2020), *Anti-fraud playbook – The best defense is a good offense, Annexe A*, page 45

Annexe 16 – Checklist pour le diagnostic des mesures de prévention de la fraude[116]

La manière la plus économique de limiter les pertes liées à la fraude est d'empêcher que celle-ci ne se produise. Cette check-list est conçue pour aider les organisations à effectuer un diagnostic rapide de leurs mesures de prévention de la fraude. Des conseils, des ressources et des outils supplémentaires pour gérer les risques de fraudes au sein de l'organisation sont disponibles sur ACFE.com/fraudrisktools.

1. **Tous les employés de l'organisation bénéficient-ils d'une formation continue à la lutte contre la fraude ?**
   - ❑ Les employés comprennent-ils en quoi consiste une fraude ?
   - ❑ Les coûts de la fraude pour l'entreprise et pour tous ses employés, y compris le manque à gagner, la publicité négative, les pertes d'emploi potentielles et la baisse de moral et de productivité, ont-ils été clairement expliqués à tous les employés ?
   - ❑ Les employés savent-ils où demander conseil lorsqu'ils doivent prendre des décisions dont le caractère éthique est ambigu, et pensent-ils pouvoir s'exprimer librement ?
   - ❑ Une politique de tolérance zéro en matière de fraude a-t-elle été communiquée aux employés, en paroles et en actes ?

2. **Un mécanisme efficace de signalement des fraudes est-il en place ?**
   - ❑ Les employés ont-ils appris comment communiquer leurs préoccupations concernant des actes répréhensibles connus ou potentiels ?
   - ❑ Les employés disposent-ils d'un ou de plusieurs canaux de signalement (comme une ligne d'alerte téléphonique externe, une boîte de messagerie officielle ou un formulaire en ligne) ?
   - ❑ Les employés sont-ils certains qu'ils peuvent signaler une activité suspecte de manière anonyme et/ou confidentielle (lorsque la loi l'autorise) et sans crainte de représailles ?
   - ❑ Les employés ont-ils reçu l'assurance que les signalements d'activités suspectes seront évalués rapidement et de manière approfondie ?
   - ❑ Les politiques et les mécanismes de signalement s'étendent-ils aux fournisseurs, aux clients et aux autres parties externes ?

3. **Pour accroître la perception de détection de fraudes par les employés, les mesures proactives suivantes sont-elles prises et portées à la connaissance des employés ?**
   - ❑ Les éventuels comportements frauduleux sont-ils recherchés avec détermination, plutôt que d'être traités passivement ?
   - ❑ Des audits inopinés de fraude sont-ils effectués, indépendamment des audits réguliers ?
   - ❑ Des techniques d'analyse de données sont-elles utilisées pour rechercher la fraude de manière proactive ? Dans l'affirmative, l'utilisation de ces techniques a-t-elle été portée à la connaissance de toute l'organisation ?
   - ❑ Les cadres examinent-ils activement les contrôles, les processus, les comptes ou les transactions qui relèvent de leur compétence pour s'assurer qu'ils sont conformes aux politiques et attentes de l'entreprise ?

4. **La culture et l'attitude de la direction en termes d'honnêteté et d'intégrité sont-elles exemplaires ?**
   - ❑ Les employés sont-ils périodiquement interrogés pour déterminer dans quelle mesure ils estiment que la direction agit avec honnêteté et intégrité ?
   - ❑ Les objectifs de performance sont-ils réalistes et clairement communiqués ?
   - ❑ Les objectifs de prévention de la fraude ont-ils été intégrés dans les mesures de performance utilisées pour évaluer les cadres et déterminer leurs primes de performance ?
   - ❑ L'organisation a-t-elle établi, mis en œuvre et testé un processus de gestion des risques de fraudes par le conseil d'administration ou d'autres personnes chargées de la gouvernance (par exemple, le comité d'audit) ?

[116] ACFE (2020), *Report to the Nations, Étude mondiale sur la fraude interne et les abus professionnels 2020*, Check-list de prévention de la fraude, pages 1 et 2

5. **Des évaluations des risques de fraude sont-elles effectuées pour identifier et atténuer de manière proactive les vulnérabilités de l'entreprise à la fraude interne et externe ?**

6. **De solides contrôles anti-fraude sont-ils déployés et fonctionnent-ils efficacement, notamment les suivants ?**
   - ❑ Séparation adéquate des tâches incompatibles
   - ❑ Règles de revues et d'autorisations
   - ❑ Mesures de sécurité physique
   - ❑ Rotations des postes
   - ❑ Vacances obligatoires

7. **S'il existe un service d'audit interne, celui-ci dispose-t-il des ressources et de l'autorité nécessaires pour fonctionner efficacement et sans influence indue de la part de la direction ?**

8. **La politique d'embauche comprend-elle les éléments suivants (lorsque la loi le permet) ?**
   - ❑ Vérification des antécédents professionnels
   - ❑ Vérification des antécédents criminels et civils
   - ❑ Contrôle de solvabilité
   - ❑ Dépistage de substances illicites
   - ❑ Vérification du profil académique
   - ❑ Vérification des références

9. **Existe-t-il des programmes d'assistance pour aider les employés aux prises avec des problèmes de toxicomanie, de santé mentale/émotionnelle, de famille ou de finances ?**

10. **Existe-t-il une politique de dialogue au sein de l'organisation qui permet aux employés de parler librement des pressions subies, donnant ainsi à la direction la possibilité d'atténuer ces pressions avant qu'elles ne s'aggravent ?**

11. **Des enquêtes régulières et anonymes sont-elles menées pour évaluer le moral des employés ?**